ABSTRACT ALGEBRA WITH APPLICATIONS

Irwin Kra, State University of New York at Stony Brook
and University of California at Berkeley

Contents

Introduction

This book is closest in spirit to [**7**]. Except for Chapters 7 and 9[1], where the reader will need some results from linear algebra (which are reviewed), this book requires no formal mathematics prerequisites. Readers should, however, posses sufficient mathematical sophistication to appreciate a logical argument and what constitutes a proof. More than enough information on these topics can be found in [**10**].

The reader should be aware of the following features of the book that may not be standard.

- I have cut the book down to a bare minimum. If a reader is interested in a given chapter or it is part of a mathematics course, then every word in it should be read and understood. When requested all the details should be filled in and all exercises and problems done (their content may be needed in subsequent parts of the "main" text).
- At times I use a "familiar" concept before if is formally defined as in Example 1.3.
- I use *italics* for terms defined, either formally in definitions or informally during a proof or discussion.
- Most nontrivial calculations and nontrivial management of sets as well as certain algebraic manipulations are performed using the symbolic manipulation programs MAPLE or MATHEMATICA.
- MAPLE and MATHEMATICA worksheets are included both in the text and on an accompanying disc – this latter format will permit easy program modifications by the reader for further exploration and experimentation. This is not a text book on MAPLE nor on MATHEMATICA. See [**3**] for such a treatise. Rather, these programs are used as tools to learn and do mathematics. I have tried to use only very simple MAPLE and MATHEMATICA programs and routines and to use, whenever possible, commands that are similar to ordinary mathematical expressions and formulae.
- I have tried to keep a reasonable mixture between formal proofs and informality (claims that certain statements are "obvious").

This book is an introduction to abstract algebra. I have particularly tried to pay attention to the needs of future high school mathematics teachers. With this in mind I have chosen applications such as public key cryptography and error correcting codes which use basic algebra as well as a study of polynomials and their roots which is such a big part of precollege mathematics.

Portions of the the material in this book were used as a basis for courses tought at Stony Brook and at Berkeley. The students challenged me with good questions and suggestions. I

[1]The tone and level of mathematical sophistication of these two chapters is considerably different in these two chapters from those in the others. Much more background is expected from the reader interested in these sections.

am very grateful to the students who read the material, corrected errors, and pointed out ways for improving the exposition. Errors, of course, remain and are the responsibility of the author.

Standard Notation and Commonly Used Symbols

A LIST OF SYMBOLS

TERM	MEANING
$\mathbb{Z}$	integers
$\mathbb{Z}_n$	congruence classes of integers modulo n
$\mathbb{Z}_n^*$	the units (invertible elements) in $\mathbb{Z}_n$
$\mathbb{Q}$	rationals
$\mathbb{R}$	reals
$\mathbb{C}$	complex numbers
$\|a\|$	the absolute value of the number a
$\gcd(a_1,\ a_2,\ ...,\ a_n) = (a_1,\ a_2,\ ...,\ a_n)$	the greatest common divisor of the integers a_1, a_2, ..., a_n
$\mathrm{lcm}(a_1,\ a_2,\ ...,\ a_n)$	the least common multiple of the integers a_1, a_2, ..., a_n
$[a]_n$	the congruence class modulo n containing the integer a
$\imath$	a square root of -1
$\Re z$	real part of the complex number z
$\Im z$	imaginary part of the complex number z
$z = x + \imath y$	$x = \Re z$ and $y = \Im z$
$\bar{z}$	conjugate of the complex number z
$r = \|z\|$	absolute value of the complex number z
$\theta = \arg z$	an argument of the complex number z
$z = re^{\imath\theta}$	$r = \|z\|$ and $\theta = \arg z$
$\|R\|$	cardinality of set R
$X_{condition}$	the set of $x \in X$ that satisfy *condition*
$\varphi(n)$	the Euler φ-function evaluated at the positive integer n
$\mathrm{ord}[a]_n$	the order of the congruence class $[a]_n$
$a\|b$	the integer a divides the integer b
red_n	reduction of integers modulo n
$\ker(\theta)$	kernel of homomorphism θ
$\mathrm{Im}(\theta)$	image of homomorphism θ
F^*	the units (invertible elements) in the ring F
$R[x]$	polynomial ring over the commutative ring R
$F(\alpha)$	smallest subfield of $\mathbb{C}$ containing F and α
$F(x)$	the field of rational functions for the field F

STANDARD TERMINOLOGY

TERM	MEANING
LHS	left hand side
elements of sets	usually denoted by lower case letters
sets	usually denoted by upper case letters
RHS	right hand side
iff	if and only if
$\subset$	proper subset
$\subseteq$	subset, may not be proper
$a \in A$	the element a is a member of the set A
$a \notin A$	the element a is not a member of the set A
$\emptyset$	the empty set
$\|A\|$	the cardinality of the set A
$A \cup B$	the union of the sets A and B
$A \cap B$	the intersection of the sets A and B
A^c	the complement of the set A
$A - B$	$A \cap B^c$
$X_{condition}$	the elements of X that satisfy *condition*

CHAPTER 1

The integers

All of us have been dealing with integers from a very young age. They have been studied by mathematicians for thousands of years. Yet much about them is unknown and, in their education, most people though they have consistently used integers have not paid much attention to their basic properties. Only in 2003 was it proven that it does not take too long to decide whether an integer is a prime or not. It is still unknown whether one can factor an integer (into its prime factors) in a reasonably short time; although the belief is that it cannot be done in what is called "polynomial time." It is also surprising, perhaps, that in addition to their obvious role in counting and recording of data, they have deep applications to everyday life. The next to the last section of the chapter descibes a public key encryption system that allows secure communication, (on the INTERNET, for example) that is based on a beautiful theorem of Euler and the fact that it is very hard to factor large integers; the last section contains a small collection of results that I found fascinating – some of them will be needed in subsequent chapters of the book.

1. Introduction

In this chapter, we study properties of the set of *integers*

$$\mathbb{Z} = \{..., -2, -1, 0, 1, 2, 3, ...\}$$

and the subset $\mathbb{N} \subset \mathbb{Z}$ of *natural numbers* or *non-negative integers*

$$\mathbb{N} = \{0, 1, 2, 3, ...\}.$$

We will assume that the reader is familiar with elementary logic, set theoretic notation (reviewed in §1 of Chapter 2), and the basic properties of the *binary relations of addition* $(+)$ and *multiplication* $(\cdot)$ and the *order relation*[1] *less than or equal* $(\leq)$ on the integers. Thus our basic object of study is the quadruple

$$(\mathbb{Z}; +, \cdot, \leq).$$

Three other (but related) order relations are associated to $\leq$: *less than* $<$ (meaning $\leq$ but $\neq$), *greater than or equal* $\geq$ (meaning $\not<$) and *greater than* $>$ (meaning $\geq$ but $\neq$). It is convenient to introduce some more notation. For all $a \in \mathbb{Z}$, we let

$$\mathbb{Z}_{\leq a} = \{b \in \mathbb{Z}; b \leq a\}.$$

The sets $\mathbb{Z}_{<a}$, $\mathbb{Z}_{\geq a}$ and $\mathbb{Z}_{>a}$ are defined in a similar manner. In this notation $\mathbb{N} = \mathbb{Z}_{\geq 0} = \mathbb{Z}_{>-1}$. Although we do not discuss the basic properties of this system, we emphasize one; the next principle. It will be converted in the next section into a property that we will use throughout this book.

[1]Relations are discussed in Chapter 2. As seen in that chapter, the four order relations on the integers are defined in terms of the additive group $(\mathbb{Z}, +)$ and the subset $\mathbb{N} \subset \mathbb{Z}$.

THE WELL ORDERING PRINCIPLE: If $S \subset \mathbb{Z}$ is *bounded from below* (that is, there exists a $b \in \mathbb{Z}$ such that $b \leq s$ for all $s \in S$) and $S \neq \emptyset$ (that is, it contains some elements), then there exists a *least* or *smallest* element[2] in S (that is there exists an $a \in S$ such that $a \leq s$ for all $s \in S$ and if also $b \leq s$ for all $s \in S$, then $a \geq b$); in particular, every nonempty set of nonnegative integers contains a smallest element.

EXERCISES

(1) Show that the least element of a non empty set of integers that is bounded from below is unique.
(2) Formulate the concept of sets of integers being *bounded from above* and translate the WELL ORDERING PRINCIPLE to such sets. Prove the translation.

2. Induction

One of the most powerful tools at our disposal will turn out to be a reformulation of the last principle into one that will be illustrated with simple examples in this section and will be used extensively throughout the book. The well ordering principle is equivalent to

THE INDUCTION PRINCIPLE: Let $a \in \mathbb{Z}$ and assume that for each $n \in \mathbb{Z}_{\geq a}$, we have a statement $P(n)$. If $P(a)$ is true, and if for all $k > a$, $P(k)$ is true whenever $P(k-1)$ is true, then $P(n)$ is true for all $n \in \mathbb{Z}_{\geq a}$.

We begin with an informal example to illustrate the above principle.

Example 1.1. Let us assume that we have infinitely many dominos lined up in a straight line. We are ignoring all kinds of technicalities. For example, exactly what it means to be lined up in a straight line, how we order or number the dominos (say they are numbered 1, 2, 3, ...), the sizes of the dominos (they are all the same), the distances between dominos (they should be small in relation to the sizes of the dominos), etc... . We claim that if we push the first domino so that in falling it hits the second one, then all the dominoes will fall down. The first domino certainly falls down. For induction we assume that the n^{th} domino has fallen down. In doing so, it pushed (hits) the $(n+1)^{st}$ domino causing it also to fall. We conclude that all of the dominos fall down.

In working with the principle of mathematical induction, there is always a collection of statements, usually an infinite number, and we are trying to prove that each statement is true. In the above example the statements are "For each positive integer k, the k^{th} domino falls". Thus we are trying to establish the validity of an infinite collection of statements. The first statement is true, since we push the first domino to fall (and in faling it pushes the second). The induction principle allows us to assume the truth of the n^{th} statement (n is an ARBITRARY positive integer) and requires us to establish the $(n+1)^{st}$ statement. If we do so, we conclude that each statement is true.

WELL ORDERING and INDUCTION are equivalent PRINCIPLES. We show first that WELL ORDERING implies INDUCTION. Let

$$S = \{n \in \mathbb{Z}_{\geq a}; P(n) \text{ is not true}\}.$$

[2]In the language of analysis (calculus) courses and books, the least element of S is its minimum, infimum, or greatest lower bound.

Then obviously $S \subseteq \mathbb{Z}_{\geq a}$. If $S \neq \emptyset$, then by the well ordering principle it would contain a smallest element b. But $b \neq a$ since $a \notin S$. Thus $b > a$ and $b-1 \in \mathbb{Z}_{\geq a}$ but $b-1 \notin S$. Hence $P(b-1)$ is true. The induction hypothesis guarantees that under these circumstances $P(b)$ is also true. Thus b could not belong to S; we have arrived at a contradiction, and the set S must be empty.

To establish the converse that INDUCTION implies WELL ORDERING, assume that $S \subset \mathbb{Z}$, that $S \neq \emptyset$ (let $a \in S$) and that for some $b \in \mathbb{Z}$, $b \leq s$ for all $s \in S$. Assume that S does not contain a least element. Let $P(n)$, $n \in \mathbb{Z}_{\geq (b-1)}$, be the statement that $\mathbb{Z}_{\leq n} \cap S = \emptyset$. Then $P(b-1)$ is true because $S \subset \mathbb{Z}_{\geq b}$. Let $k > (b-1)$. If $P(k-1)$ were true, then so would be $P(k)$ because otherwise k would be a least element of S. So by induction, $\mathbb{Z}_{\leq n} \cap S = \emptyset$ for all $n \in \mathbb{Z}$, $n \geq (b-1)$. But this contradicts that $a \geq b$ and $a \in S$.

The well ordering principle (and hence also the induction principle) is equivalent to

THE STRONG INDUCTION PRINCIPLE: Let $a \in \mathbb{Z}$ and assume that for each $n \in \mathbb{Z}_{\geq a}$, we have a statement $P(n)$. If $P(a)$ is true, and if for all $k > a$, $P(k)$ is true whenever $P(j)$ is true for integers j with $a \leq j \leq (k-1)$, then $P(n)$ is true for all $n \in \mathbb{Z}_{\geq a}$.

We leave it to the reader to verify the equivalence of the two forms of induction.

We proceed to two examples of the use of induction to prove elementary results.

EXAMPLE 1.2. For $n \in \mathbb{Z}_{>0}$, evaluate the sum of the first n positive integers.

PROOF. We are required to evaluate

$$\sum_{i=1}^{n} i = 1 + 2 + ... + n.$$

We first derive a formula for the sum. Notice that the first and last terms add up to $n+1$. So do the second and second from the end, the third and third from the end, etc... . By grouping appropriate terms we have produced $\frac{n}{2}$ groups each adding up to $n+1$ (this statement is correct even for odd n when appropriately interpreted). Thus

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}. \tag{1}$$

For the the second proof of the last formula, let us assume that through some process we have reached the conjecture that (1) is true for each positive integer n. An induction argument can turn the conjecture into a theorem. In this case $P(n)$, for $n = 1, 2, 3, ...$ is the identity or equation (1). The *base case* $n = 1$ is certainly correct. Assume now that $k > 1$ and that the formula holds for $k-1$ (that $P(k-1)$ is true), then

$$\sum_{i=1}^{k} i = \left(\sum_{i=1}^{k-1} i\right) + k = \frac{(k-1)k}{2} + k = \frac{k^2 - k + 2k}{2} = \frac{k^2 + k}{2} = \frac{k(k+1)}{2};$$

that is, the formula for the sum also holds for k ($P(k)$ is true). The induction principle allows us to conclude that (1) holds for all $n \in \mathbb{Z}_{>0}$. □

EXAMPLE 1.3. The product of any three consecutive integers is divisible by 3.

REMARK 1.4. Formally, this problem should appear only after we have discussed divisibility in the next section. We assume the reader remembers from high school mathematics elementary properties of division of integers.

PROOF. We are asked to show that for all $n \in \mathbb{Z}$, $3|n(n+1)(n+2)$. Let us use induction to establish the last assertion for all integers $n \geq -2$. The base case $n = -2$ certainly is true. So let us take $k > -2$, and assume that $3|(k-1)k(k+1)$. We need to show from this assumption that $3|k(k+1)(k+2)$. We compute

$$k(k+1)(k+2) - (k-1)k(k+1) = k(k+1)(k+2-k+1) = 3k(k+1).$$

Certainly $3|3k(k+1)$and hence the induction assumption that $3|(k-1)k(k+1)$ guarantees that $3|k(k+1)(k+2)$ as required since the sum of two integers divisible by 3 is certainly also divisible by 3. We are left to consider the case $n < -2$. Notice that

$$n(n+1)(n+2) = -(-n(-n-1)(-n-2)),$$

and that for any integer a, $3|a$ if and only if[3] $3|(-a)$. Finally observe that $n < 2$ if and only if $-n-2 > 0 \geq -2$. □

EXERCISES

(1) (a) Show that the product of any three consecutive integers is divisible by 6.
    (b) Show that for every positive integer n, $n^5 - n$ is divisible by 5.
    (c) Show that for every positive integer n, $3^{2n} - 1$ is divisible by 8.

(2) Prove that for all positive integers n,

$$1 + 2^2 + 3^2 + ... + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

(3) Do the next worksheet.

(4) This problem gives a different way to determine the function $p(n)$ of the worksheet below and hence a way to establish the formulae for the sum of cubes. As a consequence of the first two items of that worksheet, it is reasonable to conjecture that we have the following identity valid for all $n \in \mathbb{Z}_{>0}$

$$\sum_{i=1}^{n} i^3 = an^4 + bn^3 + cn^2 + dn + e,$$

for some constants a, b, c, d and e. Evaluate these constants by expressing the sum of the first $n+1$ cubes in two different ways; that is, start with

$$\sum_{i=1}^{n+1} i^3 = a(n+1)^4 + b(n+1)^3 + c(n+1)^2 + d(n+1) + e = an^4 + bn^3 + cn^2 + dn + e + (n+1)^3.$$

Justify this last formula and then use it to evaluate the five constants. Use the last calculation as a basis for an induction argument to prove the conjecture (with appropriate values for the 5 constants).

WORKSHEET # 1.

This worksheet provides a leisurely way to arrive at a formula for the sum of cubes of integers. It is also an introduction to the use of MAPLE.

[3]Abbreviated in many displayed equations as iff.

(1) (Sums of integers.) Recall that we proved (in the text) by induction that for all positive integers n,
$$1 + 2 + ... + n = \frac{n(n+1)}{2}.$$
(2) (Sums of squares of integers.) Similarly we proved (in the exercises) by induction that for all positive integers n,
$$1^2 + 2^2 + ... + n^2 = \frac{n(n+1)(2n+1)}{6}.$$
(3) (Sums of cubes of integers.) The aim of this worksheet is to formulate and then prove a similar result for sums of cubes. We follow a leisurely path.
(4) Notice that the sum of the first n positive integers is a quadratic polynomial in n. The sum of the squares of the first n positive integers is a cubic polynomial in n. It is hence reasonable to expect that the sum of the cubes of the first n positive integers is a fourth degree polynomial in n; that is,
$$1^3 + 2^3 + ... + n^3 = an^4 + bn^3 + cn^2 + dn + e, \tag{2}$$
for some constants a, b, c, d and e that do not depend on the variable n. What are the corresponding constants for sums of integers and sums of squares of integers? Can you make some "educated guesses" about what the 5 constants should be?
(5) If we are not to rely on guesswork nor on inspiration, then one of our tasks is to determine the 5 constants. If equation (2) is to hold for all integers n, it certainly should hold for for $n = 1$, 2, 3, 4 and 5, leading us to five equations
$$1 = a + b + c + d + e,$$
$$9 = 16a + 8b + 4c + 2d + e,$$
$$36 = 81a + 27b + 9c + 3d + e,$$
$$100 = 256a + 64b + 16c + 4d + e$$
and
$$225 = 625a + 125b + 25c + 5d + e.$$
(6) If our intuition is right, the above system of linear equations should have a unique solution. Recall from your linear algebra course that a necessary and sufficient condition for the above system of equations to have a unique solution is that the matrix
$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 16 & 8 & 4 & 2 & 1 \\ 81 & 27 & 9 & 3 & 1 \\ 256 & 64 & 16 & 4 & 1 \\ 625 & 125 & 25 & 5 & 1 \end{bmatrix}$$
be nonsingular. One could certainly compute its determinant by hand and show that it is non-zero. Do it using MAPLE or MATHEMATICA. You should get that the determinant equals 288.
(7) Now use MAPLE or MATHEMATICA to solve the system of equations. You should have obtained a polynomial $p(n)$ with rational coefficients. You are trying to prove by induction, because so far we have no guarantee that the equation is correct, that
$$1^3 + 2^3 + ... + n^3 = p(n)$$

for all positive integers n.

Let's make the polynomial look prettier. First write $p(n)$ as $\frac{P(n)}{N}$ where $P(n)$ is a polynomial with integer coefficients and N is a positive integer, chosen as small as possible. Now factor the polynomial $P(n)$. The formula you now need to establish for sums of cubes should appear similar to the ones for sums of integers and sums of squares. Prove by induction that the formula you obtained is true. Thus finishing this exercise.

(8) To get used to work with symbolic manipulation programs you may want, after attempting by yourself the steps outlined above, to consult the MAPLE program following this workshheet that outlines the commands needed to perform the calculations. There is a very nontrivial initial investment of time in learning to use a program of this kind. But, if one needs to do many symbolic calculations, it pays off in the long run.

(9) Were your "educated guesses" about what the values of the 5 constants close to the mark?

(10) Note that MAPLE has a command that evaluates $p(n)$ directly.

(11) Can you formulate and prove a similar result for sums of fourth powers of integers?

MAPLE SESSION #1.

(Most MAPLE warnings were suppressed in this and other printouts.)

```
> a :=
  Matrix([[1,1,1,1,1],[16,8,4,2,1],[81,27,9,3,1],[256,64,16,4,1],[625,12
  5,25,5,1]]);
```

$$a := \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 16 & 8 & 4 & 2 & 1 \\ 81 & 27 & 9 & 3 & 1 \\ 256 & 64 & 16 & 4 & 1 \\ 625 & 125 & 25 & 5 & 1 \end{bmatrix}$$

```
> with(linalg);
  det(a);
```

$$288$$

```
> b := Vector[column]([1,9,36,100,225]);
```

$$b := \begin{bmatrix} 1 \\ 9 \\ 36 \\ 100 \\ 225 \end{bmatrix}$$

```
> linsolve(a,b);
```

$$\left[\frac{1}{4}, \frac{1}{2}, \frac{1}{4}, 0, 0\right]$$

```
> poly := (y^4 +2*y^3 +y^2)/4;
```

$$poly := \frac{1}{4}\,y^4 + \frac{1}{2}\,y^3 + \frac{1}{4}\,y^2$$

```
> p := 4 *poly;
```

$$p := y^4 + 2\,y^3 + y^2$$

```
> factor(p);
```

$$y^2\,(y+1)^2$$

```
> sum(k^3,k=1..n);
```

$$\frac{1}{4}\,(n+1)^4 - \frac{1}{2}\,(n+1)^3 + \frac{1}{4}\,(n+1)^2$$

```
> simplify(%);
```

$$\frac{1}{4}\,n^4 + \frac{1}{2}\,n^3 + \frac{1}{4}\,n^2$$

```
> factor(%);
```

$$\frac{1}{4}\,n^2\,(n+1)^2$$

END OF PROGRAM

We follow this and, as appropriate, most other MAPLE and MATHEMATICA sessions with some explanatory remarks.

(1) The first and third commands of the program enter the 4×4 matrix a and the column vector $b \in \mathbb{R}^4$, respectively.
(2) The second command, introduces the linear algebra package (a technical MAPLE requirement) and computes the determinant of the matrix a.
(3) Since $\det a \neq 0$, the equation $ax = b$ is solvable. The solution is obtained by the fourth command.
(4) The next three commands obtain the polynomial p.
(5) The last three commands use MAPLE commands to directly evaluate the sum of cubes.
(6) Note that MAPLE (the version used here) employs the symbol % to denote the result of its last calculation.

MATHEMATICA SESSION #1

In the interactive MATHEMATICA session (notebook) reproduced below we study sums of 4^{th} powers of integers. Two avenues are explored.

Sum[k^4, {k, 2}]
17
Sum[k^4, {k, n}]
$\frac{1}{30}n(1+n)(1+2n)\,(-1+3n+3n^2)$
% + (n + 1)^4
$(1+n)^4 + \frac{1}{30}n(1+n)(1+2n)\,(-1+3n+3n^2)$
Simplify[%]
$(1+n)^4 + \frac{1}{30}n(1+n)(1+2n)\,(-1+3n+3n^2)$

Expand[%]
$1 + \frac{119n}{30} + 6n^2 + \frac{13n^3}{3} + \frac{3n^4}{2} + \frac{n^5}{5}$
Factor[%]
$\frac{1}{30}(1+n)(2+n)(3+2n)\left(5+9n+3n^2\right)$
f[n_]:=an^5 + b n^4 + cn^3 + dn^2 + en + h
Solve[Coefficient[f[n] + (n + 1)^4, n, 4] ==
Coefficient[f[n + 1], n, 4], a]
$\left\{\left\{a \to \frac{1}{5}\right\}\right\}$
a = 1/5
$\frac{1}{5}$
Solve[Coefficient[f[n] + (n + 1)^4, n, 3] ==
Coefficient[f[n + 1], n, 3], b]
$\left\{\left\{b \to \frac{1}{2}\right\}\right\}$
b = 1/2
$\frac{1}{2}$
Solve[Coefficient[f[n] + (n + 1)^4, n, 2] ==
Coefficient[f[n + 1], n, 2], c]
$\left\{\left\{c \to \frac{1}{3}\right\}\right\}$
c = 1/3
$\frac{1}{3}$
Solve[Coefficient[f[n] + (n + 1)^4, n] ==
Coefficient[f[n + 1], n], d]
$\{\{d \to 0\}\}$
d = 0
0
Solve[Coefficient[f[n] + (n + 1)^4, n, 0] ==
Coefficient[f[n + 1], n, 0], e]
$\left\{\left\{e \to -\frac{1}{30}\right\}\right\}$
e = −1/30
$-\frac{1}{30}$
f[n]
$h - \frac{n}{30} + \frac{n^3}{3} + \frac{n^4}{2} + \frac{n^5}{5}$
Solve[f[1] == 1, h]
$\{\{h \to 0\}\}$
h = 0
0
Factor[f[n]]
$\frac{1}{30}n(1+n)(1+2n)\left(-1+3n+3n^2\right)$
END OF PROGRAM

- The reader should note the diiference in appearance of a MATHEMATICA session from a MAPLE session. As with MAPLE, a command line (which may appear on more than one printed line) is followed usually by the program's response.
- The first program command is practice to familiarize us with the language. The computer's response gives us confidence that we used appropriately the command.

- The second command evaluates symbolically $\sum_{k=1}^{n} k^4 = \frac{1}{30}n(1+n)(1+2n)(-1+3n+3n^2)$.
- Steps 3 through 6 give the induction aqrgument to establish the above formula.
- We begin an exploration of how to arrive at the above formula. From our work on sums of first, second and third powers of integers, it is reasonable to expect that $\sum_{k=1}^{n} k^4$ is a fifth degree polynomial in n.
- Steps 7 through 21 of the program determine this polynomial. The commands use language that is very close to mathematical expressions and the reader should be able to follow it.
- In the above program we equated the coefficients of the zeroth, first, second, third and fourth powers of n in two polynomials of degree 5 to evaluate some undetermined coedfficients. We did not use an equation for fifth powers. Why not?

3. The division algorithm: gcd and lcm

The fact that the non-zero integers are not closed under the binary operation of division, rather than being a problem, presents an opening for all kind of investigations into the deeper properties of integers; some of these have practical implications as we will see later.

DEFINITION 1.5. Let a and $b \in \mathbb{Z}$. We say that *a divides b* or *a is a factor of b* or *b is a multiple of a* (and write $a|b$) if there exists a $q \in \mathbb{Z}$ such that $b = qa$.

REMARK 1.6. Note that for all $a \in \mathbb{Z}$, $a|0$. Thus every integer (including 0) divides 0. But only 0 is a multiple of 0, as expected.

CAUTION 1.7. Do not confuse the symbols $a|b$ and $\frac{a}{b}$. The first states, more or less, that b (which may be 0) can be divided by a to obtain an integer; the second represents the number obtained by dividing a by b (which must be assumed $\neq 0$) which need not be an integer.

PROPOSITION 1.8. *Let a, b, c, β and $\gamma \in \mathbb{Z}$. If $a|b$ and $a|c$, then $a|(\beta b + \gamma c)$.*

PROOF. That $a|b$ and $a|c$ means the existence of integers q_1 and q_2 such that $b = q_1 a$ and $c = q_2 a$. Thus

$$\beta b + \gamma c = \beta q_1 a + \gamma q_2 a = (\beta q_1 + \gamma q_2)a.$$

□

EXAMPLE 1.9. For all $n \in \mathbb{Z}_{>0}$, $13|\left(4^{2n-1} + 3^{n+1}\right)$.

PROOF. The proof is by induction on n. The *starting point*, $n = 1$, is of course trivial. We assume that we have the divisibility condition for $k \geq 1$ and establish it for the *successor* integer $k+1$:

$$4^{2k+1} + 3^{k+2} = 4^2 4^{2k-1} + 4^2 3^{k+1} - 4^2 3^{k+1} + 3 \cdot 3^{k+1} = 16\left(4^{2k-1} + 3^{k+1}\right) - (16-3)3^{k+1};$$

the induction hypothesis tell us that $13|\left(4^{2k-1} + 3^{k+1}\right)$ and since $13|(3-16)$, the last proposition tell us that $13|\left(4^{2k+1} + 3^{k+2}\right)$. □

DEFINITION 1.10. Let $n \in \mathbb{Z}_{\geq 0}$, we define $n!$ (to be read *n-factorial*) by induction as

$$n! = \begin{cases} 1 & \text{for } n = 0 \\ n(n-1)! & \text{for } n > 0 \end{cases},$$

and if $k \in \mathbb{Z}$ with $0 \leq k \leq n$, then we let

$$\left(\begin{array}{c} n \\ k \end{array} \right) = \frac{n!}{k!(n-k)!}$$

(these are called the *binomial coefficients (n choose k)*).

The next result does not depend on divisibility properties and could have been established in the previous section.

THEOREM 1.11 (The binomial theorem). *For all $n \in \mathbb{Z}_{>0}$ and all x and $y \in \mathbb{Z}$,*

$$(x+y)^n = \sum_{i=0}^{n} \left(\begin{array}{c} n \\ i \end{array} \right) x^{n-i} y^i.$$

PROOF. We fix x and y and use induction on n. The base case, $n = 1$, is trivial. Assume that $k \geq 1$ and that we have the result for $n = k$; that is,

$$(x+y)^k = \sum_{i=0}^{k} \left(\begin{array}{c} k \\ i \end{array} \right) x^{k-i} y^i.$$

For the induction argument,

$$(x+y)^{k+1} = (x+y)(x+y)^k = (x+y) \sum_{i=0}^{k} \left(\begin{array}{c} k \\ i \end{array} \right) x^{k-i} y^i = \sum_{i=0}^{k+1} a_i x^{k+1-i} y^i,$$

for some integers a_0, a_1, ..., a_{k+1} that we need to determine. Obviously

$$a_0 = \left(\begin{array}{c} k \\ 0 \end{array} \right) = 1 = \left(\begin{array}{c} k+1 \\ 0 \end{array} \right) \text{ and } a_{k+1} = \left(\begin{array}{c} k \\ k \end{array} \right) = 1 = \left(\begin{array}{c} k+1 \\ k+1 \end{array} \right).$$

For (the interesting cases), $1 \leq i \leq k$,

$$a_i = \left(\begin{array}{c} k \\ i \end{array} \right) + \left(\begin{array}{c} k \\ i-1 \end{array} \right) = \frac{k!}{i!(k-i)!} + \frac{k!}{(i-1)!(k-i+1)!} = k! \frac{(k-i+1)+i}{i!(k+1-i)!} = \frac{(k+1)!}{i!(k+1-i)!}.$$

□

REMARK 1.12. We have never used that x and y are integers. The theorem is valid for general *indeterminate* x and y.

THEOREM 1.13 (The division algorithm). *For all $a \in \mathbb{Z}_{>0}$ and all $b \in \mathbb{Z}_{\geq 0}$, there exist unique integers q and r such that $b = aq + r$ and $0 \leq r < a$.*

PROOF. The proof has two parts.
Existence: If $a > b$, then $q = 0$ and $r = b$. Now assume that $a \leq b$. We let

$$D = \{b - ak; k \in \mathbb{Z}_{\geq 0} \text{ and } b - ak \geq 0\}.$$

The set of non-negative integers D is not empty since it contains b (we use $k = 0$). It is bounded from below (by 0). Hence it contains a least element r; further, $b - aq = r$ for some $q \in \mathbb{Z}_{\geq 0}$. We need to verify that $0 \leq r < a$. Since $r \in D$, $r \geq 0$. If $r \geq a$, then

$$0 \leq r - a = b - a(q+1).$$

We conclude that $r - a \in D$ contradicting the fact that r was a smallest element of D.
Uniqueness: Assume that $b = aq + r$ as in the statement of the theorem and also that

$b = aq_1 + r_1$ for some integers q_1 and r_1 with $0 \leq r_1 < a$. It involves no loss of generality to assume that $r_1 \geq r$. Thus

$$a(q - q_1) = (r_1 - r),$$

and we conclude that $a|(r_1 - r)$. If $r_1 \neq r$, then $0 < r_1 - r < r_1 < a$ and so a cannot divide $(r_1 - r)$. We conclude that $r_1 = r$ and hence also $q_1 = q$. □

EXAMPLE 1.14. For $b = 17$ and $a = 3$, $q = 5$ and $r = 2$.

REMARK 1.15. The last theorem is valid for all $b \in \mathbb{Z}$. We establish the existence part for $b < 0$. By the theorem as stated, there exist unique integers q and r such that

$$-b = aq + r, \quad 0 \leq r < a.$$

Thus

$$b = a(-q) + (-r).$$

If $r = 0$, we are done otherwise we continue with

$$b = a(-q) + (-r) = a(-q - 1) + (a - r).$$

Since $0 < a - r < a$, we have concluded the existence argument. Note that the proof of uniqueness part of the theorem never assumed that b was non-negative. Why is it unnecessary to consider $a \in \mathbb{Z}_{\leq 0}$? If we also want to consider such a, it is convenient to introduce the *absolute value* of $a \in \mathbb{Z}$ defined by

$$|a| = \begin{cases} a & \text{if } a \geq 0 \\ -a & \text{if } a \leq 0 \end{cases}.$$

The division algorithm can now be stated as follows: For all a and $b \in \mathbb{Z}$ with $a \neq 0$, there exist unique integers q and r such that

$$b = aq + r \text{ and } 0 \leq r < |a|.$$

This is the formulation we will use in the sequel.

DEFINITION 1.16. It is useful to introduce two definitions with notation motivated by computer science. Let a and b be integers with $a > 0$. We define the *integral content* or *floor* $\left\lfloor \frac{b}{a} \right\rfloor$ of the rational number $\frac{b}{a}$ as[4] the largest integer $\leq \frac{b}{a}$ and the *ceiling* $\left\lceil \frac{b}{a} \right\rceil$ of $\frac{b}{a}$ as the smallest integer $\geq \frac{b}{a}$. We define $r = r\left(\frac{b}{a}\right)$ by

$$b = a \left\lfloor \frac{b}{a} \right\rfloor + r\left(\frac{b}{a}\right). \tag{3}$$

REMARK 1.17. Note that $0 \leq r\left(\frac{b}{a}\right) < a$ and that (3) is another way of writing the division algorithm. The formula is also valid, with proper interpretation, for negative a since $\frac{b}{-a} = \frac{-b}{a}$, $\left\lfloor \frac{b}{-a} \right\rfloor = \left\lfloor \frac{-b}{a} \right\rfloor$, $\left\lceil \frac{b}{-a} \right\rceil = \left\lceil \frac{-b}{a} \right\rceil$ and $r\left(\frac{b}{-a}\right) = r\left(\frac{-b}{a}\right)$.

THEOREM 1.18. *Let a and $b \in \mathbb{Z}$, not both 0. There exists a unique $d = (a, b) = \gcd(a, b) \in \mathbb{Z}_{>0}$ such that*
(i) *$d|a$ and $d|b$ and*
(ii) *$c|d$ whenever $c \in \mathbb{Z}$, $c|a$ and $c|b$.*

[4]For this definition we need the concept of order relations on the rationals. See, for example, the next chapter for a discussion of this topic.

PROOF. Let

$$D = \{as + bt; s \text{ and } t \in \mathbb{Z} \text{ and } as + bt > 0\}.$$

The set D is not empty (it contains[5] either $|a|$ or $|b|$) and is bounded from below (by 0). It hence contains a smallest (positive) element $d = as_o + bt_o$, where s_o and $t_o \in \mathbb{Z}$. We have produced d. Now we must verify its claimed properties. For the proof of (ii), note that $c \neq 0$ and we may assume that $c \in \mathbb{Z}_{>0}$. Since it divides both a and b, it obviously divides d. Thus establishing (ii). By the division algorithm $a = qd + r$, where r and $q \in \mathbb{Z}$ with $0 \leq r < d$. Thus

$$r = a - qd = a - q(as_o + bt_o) = a(1 + qs_o) + b(-qt_o),$$

and if $r > 0$, then it belongs to D and is smaller than d. This contradiction shows that $r = 0$ and hence $d|a$. Similarly $d|b$. We have established existence. For uniqueness assume that $d_1 \in \mathbb{Z}_{>0}$ also satisfies conditions (i) and (ii) (with d replaced by d_1, of course). We use (i) for d and (ii) with $c = d_1$ to conclude that $d_1|d$. Similarly $d|d_1$. Since both d and d_1 are positive integers, we conclude that $d = d_1$. □

DEFINITION 1.19. The last theorem defined the two symbols (a, b) and $\gcd(a, b)$ that we abbreviated by the symbol d. We call d, the *greatest common divisor* of a and b, and we say that a and b are *relatively prime* if $d = 1$.

COROLLARY 1.20 (of proof). *For all a and $b \in \mathbb{Z}$, not both 0, (a, b) is the smallest positive integral linear combination of a and b.*

REMARK 1.21. Note that $(a, 0) = |a|$ for $a \in \mathbb{Z}_{\neq 0}$, and that $(a, b) = (|a|, |b|)$ for a and $b \in \mathbb{Z}$, not both 0. It is convenient to extend the definition of the gcd to include $(0, 0) = 0$. Note also that $(a, 1) = 1$ for all integers a; that is, all integers are relatively prime to 1.

EXAMPLE 1.22. $(25, 12) = (25, -12) = 1$, $1 = 1 \cdot 25 + (-2)12$ and $1 = 1 \cdot 25 + 2(-12)$.

LEMMA 1.23. *Let a and $b \in \mathbb{Z}$, and let $b = aq + r$ with q and $r \in \mathbb{Z}$. Then $(a, b) = (a, r)$.*

PROOF. Let $d = (a, b)$. Then $d|r$ and thus $d|(a, r)$. But also $(a, r)|b$ (and trivially $(a, r)|a$); hence $(a, r)|d$ and we must have that $(a, r) = d$. □

THEOREM 1.24 (The Euclidean algorithm). *Let a and $b \in \mathbb{Z}$ with $a \neq 0$. Then*
(a) *if a divides b, there exists a unique $q_1 \in \mathbb{Z}$ such that*

$$b = aq_1 \text{ and } (a, b) = |a|,$$

and
(b) *if a does not divide b, there exists a unique $n \in \mathbb{Z}_{>0}$, unique $r_1, r_2, ..., r_n \in \mathbb{Z}_{>0}$ and unique $q_1, q_2, ..., q_n, q_{n+1} \in \mathbb{Z}$ such that*

$$\begin{aligned}
b = r_{-1} &= aq_1 + r_1,\ 0 < r_1 < |a| \\
a = r_0 &= r_1q_2 + r_2,\ 0 < r_2 < r_1 \\
r_1 &= r_2q_3 + r_3,\ 0 < r_3 < r_2 \\
&\ \ \vdots \\
r_{n-2} &= r_{n-1}q_n + r_n,\ 0 < r_n < r_{n-1} \\
r_{n-1} &= r_nq_{n+1}
\end{aligned}$$

[5] If $a \neq 0$, then D contains $a = 1a$ if $a > 0$ and it contains $-a = (-1)a$ if $a < 0$

and $(a, b) = r_n$.

PROOF. Part (a) of the theorem has, of course, already been established. For part (b), the existence and uniqueness of n, and the collections of r_i and q_i follow from the division algorithm. The form of the last line in the list of equations follows from the fact that the r_i are strictly decreasing. The last lemma tells us that

$$(b, a) = (a, r_1) = (r_1, r_2) = ... = (r_{n-2}, r_{n-1}) = (r_{n-1}, r_n) = r_n.$$

□

REMARK 1.25. It is usuful to introduce some convenient notational conventions.

- To have consistency of natation we labeled $b = r_{-1}$ and $a = r_0$.
- The last line of the algorithm reads

$$r_{n-1} = r_n q_{n+1} + r_{n+1} \text{ with } r_{n+1} = 0.$$

- Note also that for $i = 1,\ 2,\ ...,\ n+1$, $q_i = \left\lfloor \frac{r_{i-2}}{r_{i-1}} \right\rfloor$.

EXAMPLE 1.26. We apply the Euclidean algorithm to $a = 30$ and $b = 172$:

$$\begin{aligned} 172 &= 30 \cdot 5 + 22 \\ 30 &= 22 \cdot 1 + 8 \\ 22 &= 8 \cdot 2 + 6 \\ 8 &= 6 \cdot 1 + 2 \\ 6 &= 2 \cdot 3 \end{aligned} \quad .$$

Thus $(172, 30) = 2$. We know that there exist integers r and s such that $2 = 172r + 30s$. We find them by reading the Euclidean algorithm back-wards (starting with the next to last line):

$$\begin{aligned} 2 = 8 - 6 &= 8 - (22 - 2 \cdot 8) \\ = 3 \cdot 8 - 22 &= 3(30 - 22) - 22 \\ = 3 \cdot 30 - 4 \cdot 22 &= 3 \cdot 30 - 4(172 - 5 \cdot 30) \\ = 23 \cdot 30 - 4 \cdot 172 & \end{aligned} \quad .$$

Thus $r = -4$ and $s = 23$.
We expect to get the same result for $a = 172$ and $b = 30$. The calculations for the Euclidean algorithm should also read more or less the same as above. They do, except that the calculations have an extra line at the start:

$$30 = 172 \cdot 0 + 30 \ .$$

We systematize the above procedure using ideas suggested by the row reduction method of linear algebra. We describe the *GCD algorithm* . (We use the notation introduced in Theorem 1.24.) The algorithm consists of calculating $n + 2$ matrices and producing $n + 1$ arrows (corresponding to row operations on matrices) between them; the computations involve only 2×2 integer matrices and integer vectors written as columns. We fix a and $b \in \mathbb{Z}$ and assume that neither integer divides the other.[6] The aim is to compute (a, b) and express it as an integral linear combination of a and b. It involves no loss of generality to assume that

[6]The case where either $a|b$ or $b|a$ is, of course, trivial.

$|b| > |a|$. For notational and computational convinience we use expanded (2×3) matrices of the form

$$\left[\begin{array}{cc|c} \alpha & \beta & y \\ \gamma & \delta & x \end{array}\right] \tag{4}$$

with integer entries. This last expanded matrix is understood to stand for the matrix product

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} b \\ a \end{bmatrix} = \begin{bmatrix} y \\ x \end{bmatrix}. \tag{5}$$

The key to the method is the realization that standard row operations preserve this symbolism. We now describe the first three steps in the algorithm to find (a, b) and express it as an integral linear combination of a and b.

$$\left[\begin{array}{cc|c} 1 & 0 & b = aq_1 + r_1 \\ 0 & 1 & a \end{array}\right] \overset{q_1}{\rightarrow} \left[\begin{array}{cc|c} 1 & -q_1 & r_1 \\ 0 & 1 & a = r_1q_2 + r_2 \end{array}\right] \overset{q_2}{\rightarrow} \left[\begin{array}{cc|c} 1 & -q_1 & r_1 \\ -q_2 & 1 + q_1q_2 & r_2 \end{array}\right].$$

The first expanded matrix is obvious: the 2×2 identity matrix followed after the long vertical dash by the column vector $\begin{bmatrix} b \\ a \end{bmatrix}$. We have supplied an equality for b using the first step of the Euclidean algorithm to justify the method. The substitution $b = aq_1 + r_1$ is not needed in practice. Recall that $q_1 = \left\lfloor \frac{b}{a} \right\rfloor$. The q_1 over the first arrow indicates that we should multiply the second row by q_1 and subtract it from the first row to obtain the second expanded matrix; that is, we are subtracting from the first row the largest integral multiple of the second row that leaves the rightmost entry of the first row nonnegative. The q_2 over the second arrow indicates that we should multiply the first row (again this is this the row whose third entry has smallest absolute in its column) by q_2 and subtract it from the second row to obtain the third expanded matrix; that is, we are subtracting from the second row the largest integral multiple of the first row that leaves the leftmost entry of the second nonnegative. For convenience we place the arrow on the same line as the row whose multiple is being subtracted. We stop this alternating process when we first obtain a 0 as the rightmost entry. If, at this stage, the row with the $\neq 0$ rightmost entry is $[r, s, d]$, then $(a, b) = d = ra + sb$. The line with the 0 entry in the last matrix $[\rho, \sigma, 0]$ tells us that $0 = \rho a + \sigma b$.

We illustrate with $a = 30$ and $b = 172$:

$$\left[\begin{array}{cc|c} 1 & 0 & 172 \\ 0 & 1 & 30 \end{array}\right] \overset{5}{\rightarrow} \left[\begin{array}{cc|c} 1 & -5 & 22 \\ 0 & 1 & 30 \end{array}\right] \overset{1}{\rightarrow} \left[\begin{array}{cc|c} 1 & -5 & 22 \\ -1 & 6 & 8 \end{array}\right] \overset{2}{\rightarrow} \left[\begin{array}{cc|c} 3 & -17 & 6 \\ -1 & 6 & 8 \end{array}\right]$$

$$\overset{1}{\rightarrow} \left[\begin{array}{cc|c} 3 & -17 & 6 \\ -4 & 23 & 2 \end{array}\right] \overset{3}{\rightarrow} \left[\begin{array}{cc|c} 15 & -86 & 0 \\ -4 & 23 & 2 \end{array}\right].$$

We conclude (once again) that $(172, 30) = 2 = -4 \cdot 172 + 23 \cdot 30$. Also that $0 = 15 \cdot 172 - 86 \cdot 30$.

Signs do not alter much. We take up the case $a = 30$ and $b = -172$:

$$\left[\begin{array}{cc|c} 1 & 0 & -172 \\ 0 & 1 & 30 \end{array}\right] \overset{-6}{\rightarrow} \left[\begin{array}{cc|c} 1 & 6 & 8 \\ 0 & 1 & 30 \end{array}\right] \overset{3}{\rightarrow} \left[\begin{array}{cc|c} 1 & 6 & 8 \\ -3 & -17 & 6 \end{array}\right] \overset{1}{\rightarrow} \left[\begin{array}{cc|c} 4 & 23 & 2 \\ -3 & -17 & 6 \end{array}\right]$$

$$\overset{3}{\rightarrow} \left[\begin{array}{cc|c} 4 & 23 & 2 \\ -15 & -86 & 0 \end{array}\right].$$

We conclude (not surprisingly) that $(-172, 30) = 2 = 4(-172)+23\cdot 30$ and $0 = (-15)(-172)-86\cdot 30$. It may be only slightly surprising that the introduction of a minus sign shortened the calculation.

THE GCD ALGORITHM – a formal description

The algorithm can be described as a diagram consisting of $n+2$ matrices $\{\mathbb{A}_i\}; i = 0,\ 1,\ ...,\ n+1$, of the form (4) (that hence satisfy (5)), and $n+1$ maps

$$q_i : \mathbb{A}_{i-1} \to \mathbb{A}_i, \quad i = 1,\ 2,\ ...,\ ,\ n+1.$$

The i^{th} such map is represented by an arrow with the number q_i above it[7]:

$$\mathbb{A}_0 = \left[\begin{array}{cc|c} 1 & 0 & r_{-1} \\ 0 & 1 & r_0 \end{array}\right] \overset{q_1}{\to} \mathbb{A}_1 = \left[\begin{array}{cc|c} 1 & -q_1 & r_1 \\ 0 & 1 & r_0 \end{array}\right] \overset{q_2}{\to} \mathbb{A}_2 = \left[\begin{array}{cc|c} 1 & -q_1 & r_1 \\ -q_2 & 1+q_1q_2 & r_2 \end{array}\right]$$

$$\overset{q_3}{\to} \mathbb{A}_3 = \left[\begin{array}{cc|c} 1+q_3q_2 & -q_1-q_3(1+q_1q_2) & r_3 \\ -q_2 & 1+q_1q_2 & r_2 \end{array}\right] ...$$

$$... \ \mathbb{A}_i = \left[\begin{array}{cc|c} \alpha_i & \beta_i & r_{i-1} \\ \gamma_i & \delta_i & r_i \end{array}\right] \overset{q_{i+1}}{\to} \mathbb{A}_{i+1} = \left[\begin{array}{cc|c} \alpha_{i+1} & \beta_{i+1} & r_{i+1} \\ \gamma_{i+1} & \delta_{i+1} & r_i \end{array}\right] ...$$

$$... \ \mathbb{A}_n = \left[\begin{array}{cc|c} \alpha_n & \beta_n & r_{n-2} \\ \gamma_n & \delta_n & r_{n-1} \end{array}\right] \overset{q_{n+1}}{\to} \mathbb{A}_{n+1} = \left[\begin{array}{cc|c} \alpha_{n+1} & \beta_{n+1} & (a,b) \\ \gamma_{n+1} & \delta_{n+1} & 0 \end{array}\right].$$

The starting matrix is $\mathbb{A}_0 = \left[\begin{array}{cc|c} 1 & 0 & b \\ 0 & 1 & a \end{array}\right]$. For $i = 1,\ 2,\ ...,\ n+1$, the number q_i is obtained from the entries in the matrix $\mathbb{A}_{i-1}$, and the matrix $\mathbb{A}_i$ is obtained by applying the operator q_i to the the matrix $\mathbb{A}_{i-1}$. This operator depends on the parity of the integer i. For the above diagram, we have assumed that i is even and n is odd. The integer q_i is computed from the last column of the matrix $\mathbb{A}_{i-1}$. For even i, the operator q_i takes the second row of the matrix $\mathbb{A}_{i-1}$ and turns it into the second row of the matrix $\mathbb{A}_i$; and it sets the first row of the matrix $\mathbb{A}_i$ to be the first row of the matrix $\mathbb{A}_{i-1}$ minus q_i times its second row. For odd i, the roles of the rows are reversed.

Proof. We need to verify that each of the matrices $\mathbb{A}_i$ satifies (5). We use induction on i. The matrix $\mathbb{A}_0$ satisfies (5) by construction. So assume that for a given integer s, $0 \le s < n+1$, the matrix $\mathbb{A}_s$ satisfies (5). Let us assume that s is even.[8] Thus

$$\alpha_s b + \beta_s a = r_{s-1}$$

and

$$\gamma_s b + \delta_s a = r_s.$$

We let $q_{s+1} = \left\lfloor \frac{r_{s-1}}{r_s} \right\rfloor$. Now

$$\alpha_{s+1} = \alpha_s - q_{s+1}\gamma_s,$$
$$\beta_{s+1} = \beta_s - q_{s+1}\delta_s,$$
$$\gamma_{s+1} = \gamma_s,$$
$$\delta_{s+1} = \delta_s$$

[7]We view q_i as an operator (map between matrices) and as a number (an integer); this should not cause confusion.

[8]The argument for odd s is similar.

and

$$r_{s+1} = r_{s-1} - q_{s+1}r_s.$$

Hence

$$\alpha_{s+1}b+\beta_{s+1}a = (\alpha_s - q_{s+1}\gamma_s)\,b+(\beta_s - q_{s+1}\delta_s)\,a = r_{s-1}-q_{s+1}(\gamma_s b+\delta_s a) = r_{s-1}-q_{s+1}r_s = r_{s+1}$$

and

$$\gamma_{s+1}b + \delta_{s+1}a = \gamma_s b + \delta_s a = r_s;$$

finishing the induction argument. □

MATHEMATICA SESSION #2

We illustrate the use of the GCD algorithm by computing $(11235, 603)$. This is a transcript of an interacive session.

m0 = {{1, 0, 11235}, {0, 1, 603}}
$\{\{1, 0, 11235\}, \{0, 1, 603\}\}$
q1 = Floor[11235/603]
18
m1 = m0 − 18{{0, 1, 603}, {0, 0, 0}}
$\{\{1, -18, 381\}, \{0, 1, 603\}\}$
q2 = Floor[603/381]
1
m2 = m1 − {{0, 0, 0}, {1, −18, 381}}
$\{\{1, -18, 381\}, \{-1, 19, 222\}\}$
q3 = Floor[381/222]
1
m3 = m2 − {{−1, 19, 222}, {0, 0, 0}}
$\{\{2, -37, 159\}, \{-1, 19, 222\}\}$
q4 = Floor[222/159]
1
m4 = m3 − {{0, 0, 0}, {2, −37, 159}}
$\{\{2, -37, 159\}, \{-3, 56, 63\}\}$
Floor[159/63]
2
m5 = m4 − 2{{−3, 56, 63}, {0, 0, 0}}
$\{\{8, -149, 33\}, \{-3, 56, 63\}\}$
q5 = Floor[63/33]
1
m6 = m5 − {{0, 0, 0}, {8, −149, 33}}
$\{\{8, -149, 33\}, \{-11, 205, 30\}\}$
q6 = Floor[33/30]
1
m7 = m6 − {{−11, 205, 30}, {0, 0, 0}}
$\{\{19, -354, 3\}, \{-11, 205, 30\}\}$
q7 = Floor[30/3]
10
m8 = m7 − 10{{0, 0, 0}, {19, −354, 3}}

$\{\{19, -354, 3\}, \{-201, 3745, 0\}\}$
GCD[112305, 603]
3

END OF PROGRAM

(1) All but the last command of the program implement the GCD algorithm.
(2) The matrix $m7$ yields the gcd
$$(11235, 603) = 3 = 19 \cdot 11235 - 354 \cdot 603$$
and the companion identity
$$03 = -201 \cdot 11235 + 3745 \cdot 603.$$
(3) The last section of the program shows the command that MATHEMATICA uses to compute the gcd of two integers.

DEFINITION 1.27. Let $n \in \mathbb{Z}_{>0}$ and let $a_1, ..., a_n \in \mathbb{Z}$. We define the *greatest common divisor*
$$(a_1, ..., a_n) = \gcd\ (a_1, ..., a_n)$$
of $a_1, ..., a_n$ to be 0 if all the a_i are 0 and otherwise as the positive integer m with the following two properties:
(i) $m|a_i$ for $i = 1, 2, ..., n$ and
(ii) whenever $c \in \mathbb{Z}$, $c \neq 0$ and $c|a_i$ for $i = 1, 2, ..., n$, then also $c|m$.

REMARK 1.28. Some obseravations are required.

- It should be checked that the concept is well defined (that is, that m exists and is unique) as is done in the next theorem and that the definition for $n = 2$ agrees with the previous one that we used as is obvious.

- For all $0 \neq a \in \mathbb{Z}$, $(a) = |a|$. So for $n = 1$ there are no issues involving existence or uniqueness of m.

THEOREM 1.29. *Let $n \in \mathbb{Z}_{>1}$. For all $a_1, ..., a_n \in \mathbb{Z}$, $(a_1, ..., a_n)$ exists and is unique. Further*
$$(a_1, ..., a_n) = ((a_1, ..., a_{n-1}), a_n). \tag{6}$$

PROOF. If all the $a_i = 0$, then there is nothing to prove. So assume that they are not all zero. We use induction on $n \geq 2$. For the base case, $n = 2$, the existence of the gcd has been established and (6) reads
$$(a_1, a_2) = (|a_1|, a_2);$$
a correct formula. So we assume now that $k > 2$ and that by induction we have the existence of $(a_1, ..., a_{k-1})$ and (6) for $n = k - 1$. We proceed to establish the existence of $(a_1, ..., a_k)$ as well as (6) for $n = k$. Let $m = ((a_1, ..., a_{k-1}), a_k)$. By the induction hypothesis $(a_1, ..., a_{k-1})$ exists and is unique. The case $n = 2$, tells us that m exists and is unique. We have only to verify that m has the required properties. So $m|(a_1, ..., a_{k-1})$ and $m|a_k$ from the $n = 2$ assumption. But for $i = 1$, ..., $k - 1$, $(a_1, ..., a_{k-1})|a_i$; so also $m|a_i$. If $c \in \mathbb{Z}$, $c \neq 0$ and $c|a_i$ for $i = 1$, ..., k, then also $c|(a_1, ..., a_{k-1})$ (the induction $k - 1$ case) and hence $c|m$ (the $n = 2$ case). The proof of the uniqueness of the gcd is left to the reader. □

THEOREM 1.30. *Let a, b and $c \in \mathbb{Z}$, none 0, and $(a,b) = 1$.*
(i) *If $a|bc$, then $a|c$.*
(ii) *If $a|c$ and $b|c$, then $ab|c$.*

PROOF. That a and b are relatively prime tells that there exist integers r and s such that

$$1 = ar + bs.$$

Thus $c = car + cbs$. Assume that $a|bc$. Since $a|car$ and $a|bsc$, we see that then $a|c$, establishing (i). Assume that $a|c$ and $b|c$, then $ab|cb$ and $ba|ca$. Thus also $ba|car$ and $ab|cbs$ and hence $ab|(car + cbs) = c$. □

DEFINITION 1.31. Let a and $b \in \mathbb{Z}$. We define the *least common multiple* M of a and b, in symbols $M = \text{lcm}(a,b)$, to be 0 if a and $b = 0$. Otherwise, we define the lcm as the unique $M \in \mathbb{Z}_{>0}$ that satisfies
(i) if $a \neq 0$, then $a|M$ and if $b \neq 0$, then $b|M$ and
(ii) if $a \neq 0$ ($b \neq 0$) and c is a multiple of a (b), then $M|c$.

We leave it to the reader to define $\text{lcm}(a_1, ..., a_n)$ and to prove the analogue of Theorem 1.29 for the lcm of n integers.

EXERCISES

(1) For each of the following pairs of integers a and b, find (a,b) and express it as $ar + bs$ with r and s integers:
   (a) $a = 7$ and $b = 11$.
   (b) $a = -55$ and $b = 25$.
   (c) $a = -75$ and $b = 21$.
   (d) $a = -45$ and $b = -81$.
   (e) $a = 5245$ and $b = 1345$.
   (f) $a = 6321$ and $b = -291$.
(2) The *Fibonnacci sequence* $\{F_n\}$ is defined inductively by the condition that the first two terms of the sequence are 1 and each subsequent term is the sum of the two preceding terms. Write down the formulae that define the terms of this sequence and prove that for all $n \in \mathbb{Z}_{>0}, (F_n, F_{n+1}) = 1$.
(3) Let a, b and $c \in \mathbb{Z}$, with at most one of these equal to zero. Assume that $(a,c) = 1 = (b,c)$. Show that $(ab,c) = 1$.
(4) Show that the binomial coefficients $\begin{pmatrix} n \\ k \end{pmatrix} \in \mathbb{Z}_{>0}$.
(5) (a) Let $m, n \in \mathbb{Z}_{\geq 0}$. Prove the identity:

$$\sum_{i=0}^{k} \binom{m}{i}\binom{n}{k-i} = \binom{m+n}{k}.$$

Hint: Consider the polynomial equation

$$\sum_{k=0}^{m+n} \binom{m+n}{k} z^k = (1+z)^{m+n} = (1+z)^m(1+z)^n.$$

(b) Show that if $n \geq 1$, then

$$\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}.$$

(6) Show that if $n \in \mathbb{Z}_{>0}$, then

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0.$$

(7) Show that for all a and $b \in \mathbb{Z}$ with $a \neq 0$, $\left\lfloor \frac{b}{a} \right\rfloor = -\left\lceil \frac{-b}{a} \right\rceil$.

(8) Augment the argument of Remark 1.15 to complete the proof of the division algorithm (both the existence and uniqueness claims) as given by (3) (consider the four cases of possible signs of a and b). Base the proof of existence on Theorem 1.13 and then supply a uniqueness proof. Give an alternate proof of existence that is valid in all cases (thus not relying on Theorem 1.13) by considering as before the set of integers

$$D = \{b - ak; k \in \mathbb{Z} \text{ and } b - ak \geq 0\},$$

and establishing that this set is nonempty.

(9) Let a,b r and $s \in \mathbb{Z}$, not all zero. Assume that $d = ar + bs$. Is $|d| = a, b$? What integers can be written as integral linear combinations of a and b?

(10) Let $n \in \mathbb{Z}_{>0}$ and $a_1, ..., a_n \in \mathbb{Z}$, not all zero. Show that there exist and $r_1, ..., r_n \in \mathbb{Z}$, not all zero, such that

$$(a_1, ..., a_n) = \sum_{i=1}^{n} a_i r_i.$$

(11) Let n be a positive integer and let $a_1, a_2, ..., a_n$ be n integers, not all zero. Define $\text{lcm}(a_1, ..., a_n)$ and prove that for $n \geq 2$,

$$\text{lcm}(a_1, ..., a_n) = \text{lcm}(\text{lcm}(a_1, ..., a_{n-1}), a_n).$$

(12) In the gcd algorithm, we started with integers a and b with $0 < |a| < |b|$. What does the algorithm produce

- if we strart with a and ka, with a and k non-zero integers?
- if we started with the integer $a \neq 0$ and 0?

4. Primes

The additive structure of the positive integers is rather simple. An arbitrary positive integer n is constructed from the integers 1 (n copies of the same integer) by $n-1$ additions. The multiplicative structure of the positive integers is more complicated. We turn now to the multiplicative building blocks of $Z_{>0}$.

Definition 1.32. A number $p \in \mathbb{Z}_{>1}$ is *prime* provided it has precisely two distinct positive divisors, namely 1 and p.

Remark 1.33. Note that 1 is not a prime.

We have a fairly efficient method for producing (relatively short) lists of primes known as the sieve of Eratosthenes. It consists of a number of steps. Let us choose a positive integer say N and we want to produce a list of the primes less than or equal to N. We proceed as follows.

- (First step.) We start with the list integers $2, 3, ..., N$. Notice that the first entry in our list is the prime 2.
- (Second step.) We remove from our list all proper multiples of 2; that is, integers of the form $\{2i; i \in \mathbb{Z}_{>0}, 2 \leq i \leq \frac{N}{2}\}$. Notice that the first two entries in the resulting list are the first two primes; namely 2 and 3.
- (Third step.) We remove from our list all proper multiples of 3; that is, integers of the form $\{3i; i \in \mathbb{Z}_{>0}, 2 \leq i \leq \frac{N}{3}\}$. Notice that the first 3 entries in the resulting list are the first two primes 2, 3 and 5.
- After r steps, we have produced a list that starts with the first r primes: $2, 3, ..., p_r$.
- (The $r+1^{st}$ step.) We remove from the list produced after r steps all proper multiples of the r^{th} prime p_r; that is, integers of the form $\{p_r i; i \in \mathbb{Z}_{>0}, 2 \leq i \leq \frac{N}{p_r}\}$. The resulting list starts with the first $r + 1$ primes.
- (The stopping time.) We are done as soon as $p_{r+1}^2 > N$.

We need to prove that the above procedure does what we claim. We will do so after proving the next theorem (FTA). Obviously the *sieve of Eratosthenes algorithm* is best performed by a computer. A sample MAPLE program using $N = 200$ follows.

MAPLE SESSION #2.

```
> set1 := {seq(i, i = 2..200)};
```

set1 := {2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192, 193, 194, 195, 196, 197, 198, 199, 200}

```
> set2 := set1 minus {seq( 2*i, i = 2..100)};
```

set2 := {2, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45, 47, 49, 51, 53, 55, 57, 59, 61, 63, 65, 67, 69, 71, 73, 75, 77, 79, 81, 83, 85, 87, 89, 91, 93, 95, 97, 99, 101, 103, 105, 107, 109, 111, 113, 115, 117, 119, 121, 123, 125, 127, 129, 131, 133, 135, 137, 139, 141, 143, 145, 147, 149, 151, 153, 155, 157, 159, 161, 163, 165, 167, 169, 171, 173, 175, 177, 179, 181, 183, 185, 187, 189, 191, 193, 195, 197, 199}

```
> set3 := set2 minus {seq( 3*i, i = 2..67)};
```

set3 := {2, 3, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, 47, 49, 53, 55, 59, 61, 65, 67, 71, 73, 77, 79, 83, 85, 89, 91, 95, 97, 101, 103, 107, 109, 113, 115, 119, 121, 125, 127, 131, 133, 137, 139, 143, 145, 149, 151, 155, 157, 161, 163, 167, 169, 173, 175, 179, 181, 185, 187, 191, 193, 197, 199}

```
> set5 := set3 minus {seq( 5*i, i = 2..40)};
```

set5 := {2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59, 61, 67, 71, 73, 77, 79, 83, 89, 91, 97, 101, 103, 107, 109, 113, 119, 121, 127, 131, 133, 137, 139, 143, 149, 151, 157, 161, 163, 167, 169, 173, 179, 181, 187, 191, 193, 197, 199}

```
> set7 := set5 minus {seq( 7*i, i = 2..29)};
```

set7 := {2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 121, 127, 131, 137, 139, 143, 149, 151, 157, 163, 167, 169, 173, 179, 181, 187, 191, 193, 197, 199}

```
> set11 := set7 minus {seq( 11*i, i = 2..19)};
```

set11 := {2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 169, 173, 179, 181, 191, 193, 197, 199}

```
> set13 := set11 minus {seq( 13*i, i = 2..17)};
```

set13 := {2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199}

```
> set17 := set13 minus {seq( 13*i, i = 2..12)};
```

set17 := {2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199}

END OF PROGRAM

We will see later that care must be used in employing the MAPLE set theoretic command `minus`.

THEOREM 1.34. *Let a, $b \in \mathbb{Z}$ and p be a prime. If $p|ab$, then either $p|a$ or $p|b$.*

PROOF. Assume that p does not divide a. Then $(p, a) = 1$; which implies that $p|b$ by the last theorem. □

LEMMA 1.35. *Let $a_i \in \mathbb{Z}$ for $i = 1$, 2, ..., r (with $r \in \mathbb{Z}_{>0}$). If the prime p divides the product $a_1...a_r$, then $p|a_i$ for some i.*

PROOF. The proof is by induction on r. The base case, $r = 1$ is trivial. So assume that $r > 1$ and that $p|(a_1...a_{r-1})a_r$. The previous lemma say that either $p|(a_1...a_{r-1})$ or $p|a_r$. In the former case, the induction hypothesis guarantees that $p|a_i$ for some $1 \leq i \leq r - 1$. □

THEOREM 1.36 (The fundamental theorem of arithmetic, FTA). *Let $n \in \mathbb{Z}_{>1}$. Then there exists a unique $r \in \mathbb{Z}_{>0}$ and primes p_1, p_2 ..., p_r such that*

$$n = p_1 p_2 ... p_r = \prod_{i=1}^{r} p_i.$$

The decomposition of n into a product of primes is unique except for order; that is, if also

$$n = q_1 q_2 ... q_s$$

for some $s \in \mathbb{Z}_{>0}$ and primes q_j, $j = 1$, ..., s, then $s = r$ and for each j, there exists an i such that $q_j = p_i$.

PROOF. We use strong induction on $n \geq 2$ to show that factorization is possible. The base case is trivial since $n = 2$ is prime. So assume that $n > 2$. If n is prime, there is nothing to do. Otherwise $n = ab$ with a, $b \in \mathbb{Z}$, $1 < a < n$ and $1 < b < n$. By the strong induction assumption, both a and b can be factored as products of primes. Hence so can their product ab.

We use induction on $r \geq 1$ to show that factorization is unique. If $r = 1$, then $n = p_1$ is prime. If also $n = q_1 q_2 ... q_s$. Then $p_1 | q_j$ for some j and it follows that $p_1 = q_j$ and $s = 1$. So assume that $r > 1$ and that

$$n = p_1 p_2 ... p_r = q_1 q_2 ... q_s.$$

Then $p_1 | q_1 q_2 ... q_s$ and it must be the case that $p_1 | q_j$ for some j. As before we conclude that $p_1 = q_j$. Reordering the q_i, we may and do assume that $j = 1$. Thus also $p_2 ... p_r = q_2 ... q_s$ we conclude by induction that $r - 1 = s - 1$ and that each p_i $(i > 1)$ is a q_j $(j > 1)$. □

REMARK 1.37. We shall abbreviate "the fundamental theorem of arithmetic" by "FTA." At times it will be useful to write the factorization of an integer $n \geq 1$ in a slightly different form

$$n = p_1^{k_1} p_2^{k_2} ... p_t^{k_t} = \prod_{i=1}^{t} p_i^{k_i},$$

where $t \in \mathbb{Z}_{>0}$, $p_1, p_2, ..., p_t$ are DISTINCT primes and the $k_i \in \mathbb{Z}_{>0}$. This factorization is again unique if we list the primes in ascending order. We can also include (unnecessary) primes p_i with exponent $k_i = 0$ in the products in equation (1.37). By doing so, we loose uniqueness, but (as we shall see shortly) gain some advantages in simplifying formulae. Note that $n = 1$ is represented by using any t and all the $k_i = 0$.

COROLLARY 1.38. *There are infinitely many primes.*

PROOF. Let p_1, p_2, ..., p_n be a collection of $n \in \mathbb{Z}_{>0}$ distinct primes. Then either $p_1 p_2 ... p_n + 1$ is prime or some prime p divides it. Since $p \neq p_i$ for $i = 1$, ..., n. We have in all cases produced a prime not in our list of n of them. There hence must be infinitely many of them. □

DEFINITION 1.39. We can list (*enumerate*) the infinitely many primes in increasing order as

$$p_1, p_2, ..., p_n, ... \quad .$$

Note that this means in particular, that the entries in the list continue forever, that $p_n < p_{n+1}$, and that $p_n \geq n + 1$ ($p_n > n + 1$ for $n > 2$). We will from now on keep the above notation and call p_n, the n^{th} *prime*.

COROLLARY 1.40. *Let a and $b \in \mathbb{Z}_{>0}$ and write*

$$a = \prod_{i=1}^{r} p_i^{n_i} \text{ and } b = \prod_{i=1}^{r} p_i^{m_i},$$

where $r \in \mathbb{Z}_{>0}$, the p_i are primes, and the n_i and m_i are non-negative integers. Then
(i) *$a|b$ if and only if $n_i \leq m_i$ for each i,*
(ii) $\gcd(a,b) = \prod_{i=1}^{r} p_i^{\min\{n_i,m_i\}}$,
(iii) $\text{lcm}(a,b) = \prod_{i=1}^{r} p_i^{\max\{n_i,m_i\}}$, *and*
(iv) $\gcd(a,b)\,\text{lcm}(a,b) = ab$.

PROOF. Part (i) is obvious. To prove (ii), let $d = \prod_{i=1}^{r} p_i^{\min\{n_i,m_i\}}$. Then by part (i), $d|a$ and $d|b$. If $c \in \mathbb{Z}_{>0}$ divides both a and b, then $c = \prod_{i=1}^{r} p_i^{k_i}$ with integers $0 \leq k_i \leq \min\{n_i, m_i\}$. Thus $c|d$ and it follows that $d = (a,b)$. The proof of (iii) is similar to the last argument and (iv) follows from the observation that for all pairs of integers m and n,

$$m + n = \min\{m,n\} + \max\{m,n\}.$$

□

EXAMPLE 1.41. Since $135 = 3^3 5$ and $639 = 3^2 71$, we have $\gcd(135, 639) = 3^2 = 9$ and $\text{lcm}(135, 639) = 3^3 5 \cdot 71 = 9585$.

We can now formulate a proposition yielding the sieve of Eratosthenes algorithm.

PROPOSITION 1.42. *Fix an integer $N > 5$ and consider the steps and the list in the sieve of Eratosthenes algorithm. Let a be the smallest integer such that $p_{a+1}^2 < N$.*
(a) *For all $r \in \mathbb{N}$, $1 \leq r \leq a+1$, after r steps, the first, r entries in our list are primes.*
(b) *After $a+1$ steps, the list consists only of primes.*

PROOF. Part (a) is proven by induction on r. It is certainly true for $r = 1$. So assume that $r > 1$ and that after $r-1$ steps, the list starts with $r-1$ primes. If after the r^{th} step, a_r, the r^{th} element in our list were not prime, then it would be divisible by a p_j with $j \leq (r-1)$. But this is impossible since proper multiples of p_j were eliminated from the list at the j^{th} step. We prove part (b) by contradiction. We know by the first part that after $a+1$ steps, the first $a+1$ entries in our list are primes: $p_1, p_2, ..., p_{a+1}$. If an entry a_k in this list with $k > a+1$ is not prime, then since $a_k > p_{a+1}$, $a_k = bc$ with one of b or $c \leq p_{a+1}$. Say that $b \leq p_{a+1}$. By FTA, we may assume that b is a prime. But this contradicts that a_k was eliminated from our list in the b-th step. □

DEFINITION 1.43. Let $r \in \mathbb{Z}_{\geq 2}$ and $m_1,\ m_2,\ ...,\ m_r$ a collection of r integers. We say that this set is *relatively prime* if $(m_i, m_j) = 1$ for all $1 \leq i < j \leq r$.

REMARK 1.44. The concept introduced above is stronger than the reqirement that

$$(m_1,\ m_2,\ ...,\ m_r) = 1$$

as shown by the set consisting of the three integers 2, 3 and 4.

EXERCISES

(1) Show that $n \in \mathbb{Z}_{>0}$ is a prime whenever $2^n - 1$ is.
(2) Prove that there are infinitely many primes of the form $4n+3$, $n \in \mathbb{Z}_{\geq 0}$.

WORKSHEET #2

(1) (Definition) Remember that a prime number is an integer $p > 1$ whose only positive divisors are 1 and p itself. This means that a prime number does not admit a representation as product of two integers each strictly smaller than p and strictly bigger than 1.
(2) (Factorization in MAPLE) The computer system MAPLE has a routine that computes the factorization of integers, provided they are not too long. The appropriate command is `ifactor`. For example, if one wants to know the factorization of the number 1743756435671253155121751498513846136, one enters the command
    `> ifactor(1743756435671253155121751498513846136);`
    after a few seconds, MAPLE replies
    $(2)^3(41)(960956229634381)(666787244268091)(8297)$
    this is the factorization of the entered integer into a product of primes.
(3) (Fermat numbers) The French mathematician Pièrre de Fermat considered numbers of the form $2^n + 1$ to provide prime numbers.
    Using MAPLE, compute the first twenty numbers $2^n + 1$, and using `ifactor` determine which ones are prime.
(4) From the previous computations, we can make an educated guess: only numbers of the form $2^{2^k} + 1$ (that is, when $n = 1, 2, 4, 8, 16, \ldots$) are prime. Fermat thought that all the numbers of the form $2^{2^k} + 1$ were prime, unfortunately he was wrong.
    Using MAPLE, check that the two numbers $2^{32} + 1$ and $2^{64} + 1$ are not prime.
(5) The above computations lead us to think that if a number of the form $2^n + 1$ is prime, then n should be of the form $n = 2^k$ for some $k \geq 0$. Prove this statement. (Hint: Assume n is an odd integer ≥ 3 , then the expression $x^n + 1$ factors as $(x + 1)(x^{n-1} - x^{n-2} + x^{n-3} - \cdots + 1)$.)
(6) (Optional) It is also possible to get primes from numbers of the form $2^n - 1$. Repeat the above steps to guess which numbers of this form are prime.

5. The rationals, algebraic numbers and other beasts

The reader is surely familiar with other number systems. We briefly review some of these – they will not be used much in this book, except to discuss examples of algebraic structures.

5.1. The rationals, $\mathbb{Q}$. The rationals can be constructed from the integers by use of equivalence relations. Those unfamiliar with this topic should first study §3 of Chapter 2. Let $S = \mathbb{Z} \times \mathbb{Z}_{>0}$. Thus the elements of S are ordered pairs[9] (a, b) of integers with $b > 0$. We introduce a relation R on S by saying that $(a, b)R(a', b')$ if and only if $ab' = ba'$. We note that:
1. R is *reflexive* since $(a, b)R(a, b)$,
2. R is *symmetric* since $(a, b)R(a', b')$ obviously implies that $(a', b')R(a, b)$.
3. R is *transitive*. To prove this assume that $(a, b)R(a', b')$ and $(a', b')R(a'', b'')$. These two statements are equivalent to $ab' = ba'$ and $a'b'' = b'a''$. We consider cases:
3a. $a' = 0$. In this case, also $a = 0 = a''$. Thus certainly $ab'' = ba''$ or $(a, b)R(a'', b'')$.
3b. $a' \neq 0$. We start with $a'b'' = b'a''$ and multiply both sides by a to obtain $aa'b'' = ab'a''$. After substituting ba' for ab' in the right hand side of the last equality we obtain $aa'b'' = ba'a''$. Since $a' \neq 0$, we can cancel it from both sides to obtain $ab'' = ba''$ as required.

[9]We are thinking, of course, of the ordered pair of integers (a, b) as the fraction $\frac{a}{b}$.

The set of equivalence classes of R, the set of *rational* numbers, is denoted by $\mathbb{Q}$ and the equivalence class of $(a, b) \in S$ is customarily written as $\frac{a}{b}$. We define addition and multiplication in $\mathbb{Q}$ by

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \text{ and } \frac{a}{b}\frac{c}{d} = \frac{ac}{bd}.$$

Since $b \neq 0 \neq d$, both $\frac{ad+bc}{bd}$ and $\frac{ac}{bd} \in S$. We must still verify that these operations are well defined; that is do not depend on the choice of representatives used. So assume that $\frac{a}{b} = \frac{a'}{b'}$ and $\frac{c}{d} = \frac{c'}{d'}$. We must verify that $\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$ and that $\frac{ac}{bd} = \frac{a'c'}{b'd'}$. We leave that as an exercise for the reader. We note that we can think of $\mathbb{Z} \subset \mathbb{Q}$ if we identify $n \in \mathbb{Z}$ with $\frac{n}{1} \in \mathbb{Q}$.

What have we gained? Every non-zero rational number $\frac{a}{b}$ (thus $a \neq 0$) has a multiplicative inverse $\frac{b}{a}$. Is this enough for most applications? The answer is a resounding no since what we think of as simple numbers, for example $\sqrt{2}$, are not in $\mathbb{Q}$; that is, "the rationals have holes." To be more precise, we prove

THEOREM 1.45. *For all $r \in \mathbb{Q}$, $r^2 \neq 2$.*

PROOF. Assume that for some $\frac{a}{b}$ with a and $b \in \mathbb{Z}$, $b > 0$, we have $\frac{a^2}{b^2} = 2$. If $d = (a, b)$, then we write $a = da_1$ and $b = db_1$ with $a_1 \in \mathbb{Z}$, $b_1 \in \mathbb{Z}_{\neq 0}$, and $(a_1, b_1) = 1$. Then $\frac{a}{b} = \frac{a_1}{b_1}$ and we conclude that $a_1^2 = 2b_1^2$. Thus a_1^2 is even and so must be a_1 (as a consequence of the fundamental theorem of arithmetic). Thus b_1^2 and hence also b_1 is even. We conclude that $2|(a_1, b_1)$; a contradiction. □

REMARK 1.46. The theorem states that the equation $x^2 - 2 = 0$ has no solutions in $\mathbb{Q}$.

5.2. The reals, $\mathbb{R}$. The study of the *reals*, $\mathbb{R}$, belongs properly to analysis rather than algebra. We confine ourselves to the briefest of discussions. The construction of the reals from the rationals is more sophisticated than the construction of the rationals from the integers. One method is to identify the reals as the collection of certain subsets of rational-numbers known as *Dedekind cuts*. These are subsets $\alpha \subset \mathbb{Q}$ with the following properties:

- $\alpha \neq \emptyset$ and $\alpha \neq \mathbb{Q}$.
- If $a \in \alpha$ and $b \in \mathbb{Q}$ with $b < a$, then $b \in \alpha$.
- For all $a \in \alpha$ there exists a $b \in \alpha$ with $b > a$.

We identify a rational r with the Dedekind cut

$$\{\rho \in \mathbb{Q};\ \rho < r\}.$$

With this identification, $\mathbb{Q} \subset \mathbb{R}$. One must do some work to properly define addition and multiplication of real numbers. What have we gained? We certainly filled in some holes in the rationals since

$$\sqrt{2} = \mathbb{Q}_{\leq 0} \cup \{r \in \mathbb{Q}; 0 < r \text{ and } r^2 < 2\}.$$

But much more has been acomplished: we have filled in *all* the holes in the sense that any set S of reals that is bounded from above, must have a *least upper bound*[10]. The proof of this *completeness* property is rather simple if one understands what the various concepts mean. A point $s \in S$ is a subset of $\mathbb{Q}$. It hence makes sense to define $*s = \cup_{s \in S} s$; this is the least upper bound for the set S.

[10]For precise definitions consult any book on analysis.

5.3. The complex numbers, $\mathbb{C}$. Even though the real numbers are analytically complete, they are not algebraically complete in the sense that the equation $x^2 + 1 = 0$ has no solutions in $\mathbb{R}$. One way to remedy this problem is to artificially introduce a solution to this equation by defining the operations of addition and multiplication on ordered pairs of real numbers: $(a, b) \in \mathbb{R}^2$. If both (a, b) and $(a', b') \in \mathbb{R}^2$, we define

$$(a, b) + (a', b') = (a + a', b + b') \text{ and } (a, b)(a', b') = (aa' - bb', ab' + ba').$$

With this additive and multiplicative structure, $\mathbb{R}^2$ is a model for the complex numbers $\mathbb{C}$. We will study this system further in §5 of Chapter 2. For the moment, we limit the discussion to a few observations.

- The reals are a subset of $\mathbb{C}$ consisting of the ordered pairs $(a, 0)$ with $a \in \mathbb{R}$.
- We define $\imath = (0, 1)$. We then observe that $\imath^2 = -1$; that is, $\pm\imath$ solve the equation $x^2 + 1 = 0$.
- The complex number (a, b) is usually written as $a + b\imath$. The usual laws of arithmetic (addition and multiplication) for $\mathbb{R}$ then apply to $\mathbb{C}$ with the convention that $\imath$ is a new quantity ($\notin \mathbb{R}$) whose square is -1.
- The complex numbers are *algebraicaly complete* in the sense that every polynomial equation (here z stands for an inderminate, $n \in \mathbb{Z}_{>0}$, $a_i \in \mathbb{C}$ for all intgers i with $0 \leq i \leq n$)
$$a_n z^n + a_{n-1} z^{n-1} + ... + a_1 z + a_0 = 0$$
has a solution $z \in \mathbb{C}$.

5.4. The algebraic numbers.

Definition 1.47. A number $\alpha \in \mathbb{C}$ is *algebraic* if it satisfies an equation of the form

$$a_0 \alpha^n + a_1 \alpha^{n-1} + a_n = 0,$$

where $n \in \mathbb{Z}_{>0}$, $a_0 \in \mathbb{Z}_{\neq 0}$, and $a_i \in \mathbb{Z}$ for $1 \leq i \leq n$. All other numbers are called *transcendental*.

Remark 1.48.

- A complex number is algebraic if and only if it is a root of a monic polynomial of positive degree with rational coefficients.

- It is rather obvious that each rational number is algebraic. Thus the rationals are a subset of the algebraic numbers.

- It is not easy (it requires some preparation) to prove that the algebraic numbers form a field (as defined in Section 1 of Chapter 5). See Chapter 9.

5.5. The quaternions, $\mathbb{H}$. The number systems discussed so far, $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ are all subsets of $\mathbb{C}$. As a matter of fact we have the tower of proper inclusions

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

Are there any number systems that are supersets of $\mathbb{C}$? The answer is yes, many. But in going to "bigger" systems we now begin to loose rather than gain. One such system, the *quaternions*, is described in discussing examples of groups in Chapter 3. In passing from the complex numbers to the quaternions, we loose the commutativity of multiplication.

EXERCISES

(1) In our definition of the rationals we used an intermediate set $S = \mathbb{Z} \times \mathbb{Z}_{>0}$. What would happen if we had defined this set as $S = \mathbb{Z} \times \mathbb{Z}$?
(2) Prove that the operations of addition and multiplication on $\mathbb{Q}$ are well defined.
(3) Introduce order relations ($<$, $\leq$, $>$, $\geq$) on $\mathbb{Q}$ and show that they are compatible (agree) with the corresponding order relations on $\mathbb{Z}$.
(4) Show that the set of algebraic numbers is countable. Before doing this problem, you may want to review some of the material of the next chapter on cardinality.

6. Modular arithmetic

This section deals with what is commonly called "clock arithmetic." It involves arithmetic on (for applications, large) finite sets. It will be the basis for our study of coding (in §9).

DEFINITION 1.49. Let $n \in \mathbb{Z}_{>0}$ and a and $b \in \mathbb{Z}$. We say that a is *congruent* or *equivalent to b modulo n* or (for short) *mod n* (in symbols $a \equiv b \mod n$)[11] provided $n|(a-b)$.

The division algorithm implies the following

PROPOSITION 1.50. *Let $n \in \mathbb{Z}_{>0}$ and $a \in \mathbb{Z}$. There exists a unique $r \in \mathbb{Z}$, $0 \leq r < n$ such that $a \equiv r \mod n$.*

DEFINITION 1.51. Let $n \in \mathbb{Z}_{>0}$ and $a \in \mathbb{Z}$. We define the *congruence class* of *a modulo n*,

$$[a]_n = \{b \in \mathbb{Z}; b \equiv a \mod n\}.$$

An element of the set

$$[a]_n = \{..., a-3n, a-2n, a-n, a, a+n, a+2n, ...,\}$$

is called a *representative* of the congruence class $[a]_n$. The last proposition showed how to choose a *canonical*[12] representative for each congruence class; that is, an integer in the set

$$\{0, 1, ..., n-1\},$$

to be called the *standard representative* of the class. We denote by $\mathbb{Z}_n$ the set of congruence classes of the integers modulo n, and usually represend a congrunence class $[a]_n \in \mathbb{Z}_n$ by an integer $a \in [a]_n$, $0 \leq a < n$. When there can be no confusion, we will denote $[a]_n$ also by $[a]$ or just a.

DEFINITION 1.52. Let $n \in \mathbb{Z}_{>0}$ and a and $b \in \mathbb{Z}$. We define the operations of addition ($+$) and multiplication ($\cdot$)[13] on $\mathbb{Z}_n$ by

$$[a]_n + [b]_n = [a+b]_n$$

and

$$[a]_n[b]_n = [ab]_n.$$

[11]Throughout this section n is a positive integer fixed once and for all. The theory developed for the case $n = 1$ is completely trivial.

[12]Meaning involving no choices.

[13]As usual the $\cdot$ is omitted in most cases.

We must show the last definitions are well defined (make sense). First let us interpret what the definitions say. To add (multiply) two congruence classes, say $[a]_n$ and $[b]_n$, choose representatives a and b of these classes. Add (multiply) these representatives to get $a+b$ (ab in case of multiplication) and then take their respective congruence classes $[a+b]_n$ ($[ab]_n$ for multiplication). What happens if we choose different representatives α and β for the classes $[a]_n$ and $[b]_n$? We use that $[a]_n = [\alpha]_n$ and $[b]_n = [\beta]_n$ to conclude that

$$\alpha = a + kn \text{ and } \beta = b + ln \text{ for some } k \text{ and } l \in \mathbb{Z}.$$

Thus

$$\alpha + \beta = a + b + (k+l)n \text{ and } \alpha\beta = ab + (kb + la)n + kln^2 = ab + (kb + la + kln)n$$

and we conclude that

$$[\alpha + \beta]_n = [a + b]_n \text{ and } [\alpha\beta]_n = [ab]_n$$

as required for the operations to make sense.

As a matter of fact the system $(\mathbb{Z}_n, +, \cdot)$ (that is, the set $\mathbb{Z}_n$ with its binary operations $+$ and $\cdot$) shares many (but not all) properties of the more familiar system $(\mathbb{Z}, +, \cdot)$. The set $\mathbb{Z}_n$ contains a *zero* element $[0]_n$ and a *(multiplicative) identity* $[1]_n$.[14] We illustrate with the addition and multiplication tables for $\mathbb{Z}_6$.

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

and

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

.

In all our tables on congruence arithmetic a denotes $[a]_n$ (with n understood from the context). In the above two tables, we have listed the elements of $\mathbb{Z}_6$ in the first rows and first columns. In the first (second) of these table the sum (product) $a + b$ (ab) appears in the intersection of the row indexed by a and the column indexed by b. Notice and explain the symmetries in the above tables. The addition tables are rather easy to construct. Some more work is required to produce the multiplication tables. We reproduce here the MAPLE programs that give in matrix form the multiplication tables for $\mathbb{Z}_{17}$ and $\mathbb{Z}_{24}$. We then print the resulting matrices in standard format.

MAPLE SESSION #3.

```
> k := 17;
```

$$k := 17$$

```
> aa := array(1..k,1..k):
  for i to k do for j to k do aa[i,j] := (i-1) * (j-1) mod k end do end
  do:
  print(aa);
```

[14] We will show later in the book that the system $(\mathbb{Z}_n, +, \cdot)$ forms a *commutative ring*. When there can be no confusion, we will use the symbol $\mathbb{Z}_n$ to reprersent this set, the *commutative group* $(\mathbb{Z}_n, +)$ or the ring $(\mathbb{Z}_n, +, \cdot)$.

END OF PROGRAM

MULTIPLICATION MATRIX FOR $\mathbb{Z}_{17}$

$$\begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\
0 & 2 & 4 & 6 & 8 & 10 & 12 & 14 & 16 & 1 & 3 & 5 & 7 & 9 & 11 & 13 & 15 \\
0 & 3 & 6 & 9 & 12 & 15 & 1 & 4 & 7 & 10 & 13 & 16 & 2 & 5 & 8 & 11 & 14 \\
0 & 4 & 8 & 12 & 16 & 3 & 7 & 11 & 15 & 2 & 6 & 10 & 14 & 1 & 5 & 9 & 13 \\
0 & 5 & 10 & 15 & 3 & 8 & 13 & 1 & 6 & 11 & 16 & 4 & 9 & 14 & 2 & 7 & 12 \\
0 & 6 & 12 & 1 & 7 & 13 & 2 & 8 & 14 & 3 & 9 & 15 & 4 & 10 & 16 & 5 & 11 \\
0 & 7 & 14 & 4 & 11 & 1 & 8 & 15 & 5 & 12 & 2 & 9 & 16 & 6 & 13 & 3 & 10 \\
0 & 8 & 16 & 7 & 15 & 6 & 14 & 5 & 13 & 4 & 12 & 3 & 11 & 2 & 10 & 1 & 9 \\
0 & 9 & 1 & 10 & 2 & 11 & 3 & 12 & 4 & 13 & 5 & 14 & 6 & 15 & 7 & 16 & 8 \\
0 & 10 & 3 & 13 & 6 & 16 & 9 & 2 & 12 & 5 & 15 & 8 & 1 & 11 & 4 & 14 & 7 \\
0 & 11 & 5 & 16 & 10 & 4 & 15 & 9 & 3 & 14 & 8 & 2 & 13 & 7 & 1 & 12 & 6 \\
0 & 12 & 7 & 2 & 14 & 9 & 4 & 16 & 11 & 6 & 1 & 13 & 8 & 3 & 15 & 10 & 5 \\
0 & 13 & 9 & 5 & 1 & 14 & 10 & 6 & 2 & 15 & 11 & 7 & 3 & 16 & 12 & 8 & 4 \\
0 & 14 & 11 & 8 & 5 & 2 & 16 & 13 & 10 & 7 & 4 & 1 & 15 & 12 & 9 & 6 & 3 \\
0 & 15 & 13 & 11 & 9 & 7 & 5 & 3 & 1 & 16 & 14 & 12 & 10 & 8 & 6 & 4 & 2 \\
0 & 16 & 15 & 14 & 13 & 12 & 11 & 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1
\end{bmatrix}$$

MULTIPLICATION MATRIX FOR $\mathbb{Z}_{24}$

$$\begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 & 22 & 23 \\
0 & 2 & 4 & 6 & 8 & 10 & 12 & 14 & 16 & 18 & 20 & 22 & 0 & 2 & 4 & 6 & 8 & 10 & 12 & 14 & 16 & 18 & 20 & 22 \\
0 & 3 & 6 & 9 & 12 & 15 & 18 & 21 & 0 & 3 & 6 & 9 & 12 & 15 & 18 & 21 & 0 & 3 & 6 & 9 & 12 & 15 & 18 & 21 \\
0 & 4 & 8 & 12 & 16 & 20 & 0 & 4 & 8 & 12 & 16 & 20 & 0 & 4 & 8 & 12 & 16 & 20 & 0 & 4 & 8 & 12 & 16 & 20 \\
0 & 5 & 10 & 15 & 20 & 1 & 6 & 11 & 16 & 21 & 2 & 7 & 12 & 17 & 22 & 3 & 8 & 13 & 18 & 23 & 4 & 9 & 14 & 19 \\
0 & 6 & 12 & 18 & 0 & 6 & 12 & 18 & 0 & 6 & 12 & 18 & 0 & 6 & 12 & 18 & 0 & 6 & 12 & 18 & 0 & 6 & 12 & 18 \\
0 & 7 & 14 & 21 & 4 & 11 & 18 & 1 & 8 & 15 & 22 & 5 & 12 & 19 & 2 & 9 & 16 & 23 & 6 & 13 & 20 & 3 & 10 & 17 \\
0 & 8 & 16 & 0 & 8 & 16 & 0 & 8 & 16 & 0 & 8 & 16 & 0 & 8 & 16 & 0 & 8 & 16 & 0 & 8 & 16 & 0 & 8 & 16 \\
0 & 9 & 18 & 3 & 12 & 21 & 6 & 15 & 0 & 9 & 18 & 3 & 12 & 21 & 6 & 15 & 0 & 9 & 18 & 3 & 12 & 21 & 6 & 15 \\
0 & 10 & 20 & 6 & 16 & 2 & 12 & 22 & 8 & 18 & 4 & 14 & 0 & 10 & 20 & 6 & 16 & 2 & 12 & 22 & 8 & 18 & 4 & 14 \\
0 & 11 & 22 & 9 & 20 & 7 & 18 & 5 & 16 & 3 & 14 & 1 & 12 & 23 & 10 & 21 & 8 & 19 & 6 & 17 & 4 & 15 & 2 & 13 \\
> 0 & 12 & 0 & 12 & 0 & 12 & 0 & 12 & 0 & 12 & 0 & 12 & 0 & 12 & 0 & 12 & 0 & 12 & 0 & 12 & 0 & 12 & 0 & 12 \\
0 & 13 & 2 & 15 & 4 & 17 & 6 & 19 & 8 & 21 & 10 & 23 & 12 & 1 & 14 & 3 & 16 & 5 & 18 & 7 & 20 & 9 & 22 & 11 \\
0 & 14 & 4 & 18 & 8 & 22 & 12 & 2 & 16 & 6 & 20 & 10 & 0 & 14 & 4 & 18 & 8 & 22 & 12 & 2 & 16 & 6 & 20 & 10 \\
0 & 15 & 6 & 21 & 12 & 3 & 18 & 9 & 0 & 15 & 6 & 21 & 12 & 3 & 18 & 9 & 0 & 15 & 6 & 21 & 12 & 3 & 18 & 9 \\
0 & 16 & 8 & 0 & 16 & 8 & 0 & 16 & 8 & 0 & 16 & 8 & 0 & 16 & 8 & 0 & 16 & 8 & 0 & 16 & 8 & 0 & 16 & 8 \\
0 & 17 & 10 & 3 & 20 & 13 & 6 & 23 & 16 & 9 & 2 & 19 & 12 & 5 & 22 & 15 & 8 & 1 & 18 & 11 & 4 & 21 & 14 & 7 \\
0 & 18 & 12 & 6 & 0 & 18 & 12 & 6 & 0 & 18 & 12 & 6 & 0 & 18 & 12 & 6 & 0 & 18 & 12 & 6 & 0 & 18 & 12 & 6 \\
0 & 19 & 14 & 9 & 4 & 23 & 18 & 13 & 8 & 3 & 22 & 17 & 12 & 7 & 2 & 21 & 16 & 11 & 6 & 1 & 20 & 15 & 10 & 5 \\
0 & 20 & 16 & 12 & 8 & 4 & 0 & 20 & 16 & 12 & 8 & 4 & 0 & 20 & 16 & 12 & 8 & 4 & 0 & 20 & 16 & 12 & 8 & 4 \\
0 & 21 & 18 & 15 & 12 & 9 & 6 & 3 & 0 & 21 & 18 & 15 & 12 & 9 & 6 & 3 & 0 & 21 & 18 & 15 & 12 & 9 & 6 & 3 \\
0 & 22 & 20 & 18 & 16 & 14 & 12 & 10 & 8 & 6 & 4 & 2 & 0 & 22 & 20 & 18 & 16 & 14 & 12 & 10 & 8 & 6 & 4 & 2 \\
0 & 23 & 22 & 21 & 20 & 19 & 18 & 17 & 16 & 15 & 14 & 13 & 12 & 11 & 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1
\end{bmatrix}$$

The above program needs no explanatory remarks. In the output, we have omitted the previously used first column and first row. So the (i, j)-entry of the output matrix is the standard representative of $[(i-1)(j-1)]_n$. The first columns and first rows of the output matrices are, of course, superfluous.

EXAMPLE 1.53. Let us show that $11|(10!+1)$ or equivalently that $10!+1 \equiv 0 \mod 11$. We do not do the brute force calculation, but reduce modulo 11. Start with

$$10! = 10{\cdot}9{\cdot}8{\cdot}7{\cdot}6{\cdot}5(4{\cdot}3{\cdot}2) \equiv (10{\cdot}9)8{\cdot}7{\cdot}6(5{\cdot}2) \equiv 2(8{\cdot}7)6{\cdot}10 \equiv 2{\cdot}1{\cdot}6{\cdot}10 \equiv (2{\cdot}6)10 \equiv 10 \mod 11.$$

Hence

$$10!+1 \equiv 10+1 \equiv 0 \mod 11.$$

DEFINITION 1.54. Let $n \in \mathbb{Z}_{>1}$ and $a \in \mathbb{Z}$. We say that $[a]_n$ is *invertible* in $\mathbb{Z}_n$ or *has an inverse (modulo n)* if there exists a $b \in \mathbb{Z}$ such that $[a]_n[b]_n = [1]_n$. The invertible elements in $\mathbb{Z}_n$ are also called *units*. We say that a non-zero congruence class $[a]_n$ is a *zero divisor (modulo n)* if there exists an integer b such that $[b]_n \neq [0]_n$ but $[a]_n[b]_n = [0]_n$.

THEOREM 1.55. *Let $n \in \mathbb{Z}_{>1}$ and $a \in \mathbb{Z}$. Then $[a]_n$ has an inverse modulo n if and only if $(a,n) = 1$. If in fact r and $s \in \mathbb{Z}$ satisfy $ar + sn = 1$, then $[r]_n$ is an inverse of $[a]_n$.*

PROOF. Suppose that $[a]$ is invertible[15] with inverse $[k]$ ($k \in \mathbb{Z}$). Then $ak \equiv 1 \mod n$; that is, $n|(ak-1)$. Therefore there exists a $t \in \mathbb{Z}$ such that $nt = ak - 1$. This implies that $(a,n) = 1$. Conversely, if $(a,n) = 1$, then there exists integers r and s such that $ar + sn = 1$. Therefore $n|(1-ar)$ and $ar \equiv 1 \mod n$; the last equation says $[a]_n[r]_n = [1]_n$. □

PROPOSITION 1.56. *Let $n \in \mathbb{Z}_{>1}$ and $a \in \mathbb{Z}$. If $[a]_n$ is invertible modulo n, then its inverse $[b]_n$ is unique and is hence written as $[a]_n^{-1}$*

PROOF. If for $c \in \mathbb{Z}$, $[c]_n$ is also an inverse of $[a]_n$, then $[a]([b]-[c]) = [0]$. Thus $n|a(b-c)$ and since $(a,n) = 1$, $n|(b-c)$. Thus $[b] = [c]$. □

EXAMPLE 1.57. Since $1 = -91{\cdot}507 + 118{\cdot}391$, $[391]_{507}^{-1} = [118]_{507}$ (and $[116]_{391}^{-1} = [300]_{391}$).

EXAMPLE 1.58. Since $(215, 795) = 5$, 215 does not have an inverse modulo 795 and 795 does not have an inverse modulo 215. Note that $[795]_{215} = [150]_{215}$.

EXAMPLE 1.59. It is rather obvious that $(73, 23) = 1$. So that both $[73]_{23}^{-1}$ and $[23]_{73}^{-1}$ exist. To find them, we proceed to express $(73, 23)$ as a linear combination of 73 and 23 using the GCD algorithm:

$$\left[\begin{array}{cc|c} 1 & 0 & 73 \\ 0 & 1 & 23 \end{array}\right] \xrightarrow{3} \left[\begin{array}{cc|c} 1 & -3 & 4 \\ 0 & 1 & 23 \end{array}\right] \xrightarrow{5} \left[\begin{array}{cc|c} 1 & -3 & 4 \\ -5 & 16 & 3 \end{array}\right] \xrightarrow{1} \left[\begin{array}{cc|c} 6 & -19 & 1 \\ -5 & 16 & 3 \end{array}\right].$$

Thus $6 \cdot 73 - 19 \cdot 23 = 1$, $[23]_{73} = [-19]_{73} = [54]_{23}$ and $[73]_{23} = [6]_{23}$.

COROLLARY 1.60. *Let $n \in \mathbb{Z}_{>1}$ and a, b and $c \in \mathbb{Z}$. If $(n,c) = 1$ and $ac \equiv bc \mod n$, then $a \equiv b \mod n$.*

PROOF. We rewrite the congruence $ac \equiv bc \mod n$ as $[a]_n[c]_n = [b]_n[c]_n$. Since n and c are relatively prime, $[c]_n^{-1}$ exists and the lemma follows by multiplying each side of the last equality by $[c]_n^{-1}$. □

COROLLARY 1.61. *Let $n \in \mathbb{Z}_{>0}$. Then each non-zero $[a]_n$ is either invertible or a zero divisor, but not both.*

[15]The subscript n is dropped since it fixed throughout the argument. When clear from the context we will also drop the [ ] from the notation.

PROOF. Let $a \in \mathbb{Z}$ and assume that $[a]_n$ is non-zero and not invertible. Thus $d = (n, a) > 1$. It follows that $a = kd$ and $n = ld$ for some positive integers k and $l > 1$. Hence $al = kld$ is divisible by n. Thus $[a]_n[l]_n = [0]_n$; that is, $[a]_n$ is a zero divisor. □

COROLLARY 1.62. *Let $p \in \mathbb{Z}_{>0}$ be a prime. Then every non-zero element in $\mathbb{Z}_p$ is invertible.*

DEFINITION 1.63. For each $n \in \mathbb{Z}_{>0}$, we let $\mathbb{Z}_n^*$ be the set of invertible congruence classes in $\mathbb{Z}_n$.

THEOREM 1.64. *Let $n \in \mathbb{Z}_{>1}$. Then $\mathbb{Z}_n^*$ is closed under multiplication; that is, if $[a]$ and $[b] \in \mathbb{Z}_n^*$, then so does $[a][b]$.*

PROOF. Let p be a prime. Since $(n, a) = 1$, either p does not divide n or p does not divide a. Similarly (either p does not divide n) or it does not divide b. Hence either p does not divide n or p does not divide ab. It must be the case that $(n, ab) = 1$. □

Note that $\mathbb{Z}_8^*$ consists of $\{[1], [3], [5], [7]\}$ and thus $|\mathbb{Z}_8^*| = 4$. It is easy to construct by brute force the multiplication table for $\mathbb{Z}_8^*$. It is, of course, a subset of the multiplication table for $\mathbb{Z}_8$ (that the reader should construct and compare to the one below) and is described by

$\cdot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

.

For larger n, we may use MAPLE to construct the multiplication tables. The construction of the first of these tables for the prime 17 offers no challenges. It can readily be modified to produce the multiplication table for $\mathbb{Z}_n^*$ for any prime n by merely changing the first line of the program.

MAPLE SESSION #4.

```
> n := 17;
```

$$n := 17$$

```
> f:= x -> x;
```

$$f := x \rightarrow x$$

```
> aa := array(1..(n-1),1..(n-1)):

> for i to (n-1) do for j to (n-1) do aa[i,j] := f(i) * f(j) mod n end
  do end do:

> print(aa);
```

$$\begin{bmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\
2 & 4 & 6 & 8 & 10 & 12 & 14 & 16 & 1 & 3 & 5 & 7 & 9 & 11 & 13 & 15 \\
3 & 6 & 9 & 12 & 15 & 1 & 4 & 7 & 10 & 13 & 16 & 2 & 5 & 8 & 11 & 14 \\
4 & 8 & 12 & 16 & 3 & 7 & 11 & 15 & 2 & 6 & 10 & 14 & 1 & 5 & 9 & 13 \\
5 & 10 & 15 & 3 & 8 & 13 & 1 & 6 & 11 & 16 & 4 & 9 & 14 & 2 & 7 & 12 \\
6 & 12 & 1 & 7 & 13 & 2 & 8 & 14 & 3 & 9 & 15 & 4 & 10 & 16 & 5 & 11 \\
7 & 14 & 4 & 11 & 1 & 8 & 15 & 5 & 12 & 2 & 9 & 16 & 6 & 13 & 3 & 10 \\
8 & 16 & 7 & 15 & 6 & 14 & 5 & 13 & 4 & 12 & 3 & 11 & 2 & 10 & 1 & 9 \\
9 & 1 & 10 & 2 & 11 & 3 & 12 & 4 & 13 & 5 & 14 & 6 & 15 & 7 & 16 & 8 \\
10 & 3 & 13 & 6 & 16 & 9 & 2 & 12 & 5 & 15 & 8 & 1 & 11 & 4 & 14 & 7 \\
11 & 5 & 16 & 10 & 4 & 15 & 9 & 3 & 14 & 8 & 2 & 13 & 7 & 1 & 12 & 6 \\
12 & 7 & 2 & 14 & 9 & 4 & 16 & 11 & 6 & 1 & 13 & 8 & 3 & 15 & 10 & 5 \\
13 & 9 & 5 & 1 & 14 & 10 & 6 & 2 & 15 & 11 & 7 & 3 & 16 & 12 & 8 & 4 \\
14 & 11 & 8 & 5 & 2 & 16 & 13 & 10 & 7 & 4 & 1 & 15 & 12 & 9 & 6 & 3 \\
15 & 13 & 11 & 9 & 7 & 5 & 3 & 1 & 16 & 14 & 12 & 10 & 8 & 6 & 4 & 2 \\
16 & 15 & 14 & 13 & 12 & 11 & 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1
\end{bmatrix}$$

END OF PROGRAM

Compare the last output with that of the of the previous MAPLE session for the prime 17. What is the difference? The program for non-primes is more interesting.

MAPLE SESSION #5.

```
> n := 24:
> zstarn:=select(x->if (gcd(x,n)=1) then true; else false;  end if,
  {seq(i,i=1..n)});
```

$$zstarn := \{1, 5, 7, 11, 13, 17, 19, 23\}$$

```
> with(numtheory):

Warning, the protected name order has been redefined and unprotected

> phi(n);
```

$$8$$

```
> aa := array(1..phi(n),1..phi(n)):
> for i to (phi(n)) do for j to (phi(n)) do aa[i,j] := zstarn[i] *
  zstarn[j] mod n end do end do;
> print(aa);
```

$$\begin{bmatrix}
1 & 5 & 7 & 11 & 13 & 17 & 19 & 23 \\
5 & 1 & 11 & 7 & 17 & 13 & 23 & 19 \\
7 & 11 & 1 & 5 & 19 & 23 & 13 & 17 \\
11 & 7 & 5 & 1 & 23 & 19 & 17 & 13 \\
13 & 17 & 19 & 23 & 1 & 5 & 7 & 11 \\
17 & 13 & 23 & 19 & 5 & 1 & 11 & 7 \\
19 & 23 & 13 & 17 & 7 & 11 & 1 & 5 \\
23 & 19 & 17 & 13 & 11 & 7 & 5 & 1
\end{bmatrix}$$

END OF PROGRAM

The second command of the above program produces the list of $\varphi(n)$[16] positive integers that are $\leq n$ and relatively prime to n. The entry `phi(n)` was included only as very weak consistency check on our program. By changing 24 to 72 in the first line of the program, we obtain the multiplication table for $\mathbb{Z}_{72}$. It results in the following table.

1	5	7	11	13	17	19	23	25	29	31	35	37	41	43	47	49	53	55	59	61	65	67	71
5	25	35	55	65	13	23	43	53	1	11	31	41	61	71	19	29	49	59	7	17	37	47	67
7	35	49	5	19	47	61	17	31	59	1	29	43	71	13	41	55	11	25	53	67	23	37	65
11	55	5	49	71	43	65	37	59	31	53	25	47	19	41	13	35	7	29	1	23	67	17	61
13	65	19	71	25	5	31	11	37	17	43	23	49	29	55	35	61	41	67	47	1	53	7	59
17	13	47	43	5	1	35	31	65	61	23	19	53	49	11	7	41	37	71	67	29	25	59	55
19	23	61	65	31	35	1	5	43	47	13	17	55	59	25	29	67	71	37	41	7	11	49	53
23	43	17	37	11	31	5	25	71	19	65	13	59	7	53	1	47	67	41	61	35	55	29	49
25	53	31	59	37	65	43	71	49	5	55	11	61	17	67	23	1	29	7	35	13	41	19	47
29	1	59	31	17	61	47	19	5	49	35	7	65	37	23	67	53	25	11	55	41	13	71	43
31	11	1	53	43	23	13	65	55	35	25	5	67	47	37	17	7	59	49	29	19	71	61	41
35	31	29	25	23	19	17	13	11	7	5	1	71	67	65	61	59	55	53	49	47	43	41	37
37	41	43	47	49	53	55	59	61	65	67	71	1	5	7	11	13	17	19	23	25	29	31	35
41	61	71	19	29	49	59	7	17	37	47	67	5	25	35	55	65	13	23	43	53	1	11	31
43	71	13	41	55	11	25	53	67	23	37	65	7	35	49	5	19	47	61	17	31	59	1	29
47	19	41	13	35	7	29	1	23	67	17	61	11	55	5	49	71	43	65	37	59	31	53	25
49	29	55	35	61	41	67	47	1	53	7	59	13	65	19	71	25	5	31	11	37	17	43	23
53	49	11	7	41	37	71	67	29	25	59	55	17	13	47	43	5	1	35	31	65	61	23	19
55	59	25	29	67	71	37	41	7	11	49	53	19	23	61	65	31	35	1	5	43	47	13	17
59	7	53	1	47	67	41	61	35	55	29	49	23	43	17	37	11	31	5	25	71	19	65	13
61	17	67	23	1	29	7	35	13	41	19	47	25	53	31	59	37	65	43	71	49	5	55	11
65	37	23	67	53	25	11	55	41	13	71	43	29	1	59	31	17	61	47	19	5	49	35	7
67	47	37	17	7	59	49	29	19	71	61	41	31	11	1	53	43	23	13	65	55	35	25	5
71	67	65	61	59	55	53	49	47	43	41	37	35	31	29	25	23	19	17	13	11	7	5	1

EXERCISES

(1) Let n and m be positive integers. Consider the set $\mathbb{Z}_n \times \mathbb{Z}_m$ of ordered pairs (a, b) with $a \in \mathbb{Z}_n$ and $b \in \mathbb{Z}_m$. Introduce a multiplication on such pairs by defining $(a, b)(c, d) = (ac, bd)$.
   - Show this multiplication is well defined.
   - Construct this multiplication for $\mathbb{Z}_3 \times \mathbb{Z}_5$ and compare it to the multiplication table for $\mathbb{Z}_{15}$.
   - Construct the multiplication table for $\mathbb{Z}_4 \times \mathbb{Z}_6$ and compare it to the multiplication table for $\mathbb{Z}_{24}$.

(2) Fix a positive integer n. The multiplication table for $\mathbb{Z}_n^*$ that we have been using is a $\varphi(n) \times \varphi(n)$ matrix M constructed as follows. Let $x_1, x_2, ..., x_{\varphi(n)}$ be increasing list of integers j with $1 \leq j < n$ and $(j, n) = 1$. The (i, j)-entry of the matrix M is the standard representative of $[x_i x_j]$. Show that M is a symmetric matrix. What property of multiplication of congruence classes does the symmetry of M reflect?

(3) In this exercise we study simple divisiblity tests for positive integes N.
   - Show that N is divisble by 3 if and only if the sum of the digits in N is.
   - Devise and establish similar (or simpler) divisibilty tests for 4, 5, 6 and 7.

[16] The Euler φ-function is introduced in Section 8.

7. Solutions of linear congruences

We are interested in solving *linear congruences*; that is, equations of the form

$$ax \equiv b \mod n \text{ equivalently } [a]_n X = [b]_n, \tag{7}$$

where $n \in \mathbb{Z}_{>0}$, a and $b \in \mathbb{Z}$ are fixed and we are looking for integers x that satisfy (in the equivalent formulation we are looking for X, equivalence classes of integers modulo n) equation (7). If $a = 0$ or $a = 1$, we already know the answer, so we may assume from now on that $1 < a < n$. However, we work without this restriction. It pays for us to concentrate on the formulation in terms of equivalence classes. There are some immediate differences from ordinary equations:

- The equation $[2]_3 X = [1]_3$ has a unique solution $X = [2]_3$.
- The equation $[2]_4 X = [1]_4$ has no solutions.
- The equation $[2]_4 X = [0]_4$ has two solutions: $X = [0]_4$ and $[2]_4$.

This is more or less the general picture as seen in

THEOREM 1.65. *Let $n \in \mathbb{Z}_{>0}$, a, $b \in \mathbb{Z}$. Then (7) has solutions if and only if $d = (a, n)|b$. If $d|b$, there are exactly d congruence classes of solutions modulo n and all these solutions are congruent modulo $\frac{n}{d}$.*

PROOF. For $c \in \mathbb{Z}$, let $[c]_n$ be a solution to (7). Then $ac \equiv b \mod n$; that is, $[a]_n[c]_n = [b]_n$ or $ac - nk = b$ for some $k \in \mathbb{Z}$. Thus $d|b$. Conversely, assume that $d|b$. We divide (7) by d and obtain

$$\frac{a}{d}x \equiv \frac{b}{d} \mod \frac{n}{d} \text{ or equivalently } \left[\frac{a}{d}\right]_{\frac{n}{d}} X = \left[\frac{b}{d}\right]_{\frac{n}{d}}, \tag{8}$$

where in the last equation X represents a congruence class modulo $\frac{n}{d}$. It is easy to see that as equations for unknown integers x, (7) and (8) are equivalent; an $x \in \mathbb{Z}$ that solves one also solves the other. The same is true for equivalence classes X once one understands that equivalence class X modulo $\frac{n}{d}$ that solves (8) corresponds to d equivalence classes modulo n that solve (7). To see this, pick any $x \in X$ and let $X_0 = [x]_n$. Then $X_0 \subset X$ and we define for any integer a,

$$X_a = X_0 + a = \{y + a; y \in X_0\} = [x + a]_n.$$

It is easily seen that

$$X = X_0 \cup X_{\frac{n}{d}} \cup X_{2\frac{n}{d}} \cup \ldots \cup X_{(d-1)\frac{n}{d}}.$$

Since $\left(\frac{a}{d}, \frac{n}{d}\right) = 1$, (8) has a unique solution $X = \left[\frac{a}{d}\right]^{-1}_{\frac{n}{d}} \left[\frac{b}{d}\right]_{\frac{n}{d}}$. □

REMARK 1.66. It is useful to consider various special cases.

- $n = 1$: In this case every $x \in \mathbb{Z}$ is a solution and $X = \mathbb{Z}$.
- $n|a$ or equivalently $[a]_n = [0]_n$: In this case, once again, every $x \in \mathbb{Z}$ is a solution. In terms of equivalence classes, every class is a solution (there are n such solutions).
- $[a]_n$ is a zero divisor (in particular $[a]_n \neq [0]_n$): In this case, we consider two subcases: (a) $\left[\frac{b}{d}\right]_{\frac{n}{d}} = [0]_{\frac{n}{d}}$: $[0]_{\frac{n}{d}}$ is the only solution of (8) and thus (7) has d solutions

$$[0]_n, \ \left[\frac{n}{d}\right]_n, \ \ldots, \ \left[(d-1)\frac{n}{d}\right]_n;$$

all but the first of these are zero divisors, and
(b) $\left[\frac{b}{d}\right]_{\frac{n}{d}} \neq [0]_{\frac{n}{d}}$: Let $\left[\frac{\alpha}{d}\right]_{\frac{n}{d}}$, with $\alpha \in \mathbb{Z}$ such that $0 < \alpha < d$ be the unique solution of (8), then (7) has d solutions

$$[\alpha]_n,\ \left[\alpha + \frac{n}{d}\right]_n,\ ...,\ \left[\alpha + (d-1)\frac{n}{d}\right]_n;$$

all are zero divisors.

COROLLARY 1.67. *Equation* (7) *has a unique equivalence class of solutions if and only if* $d = (a, n) = 1$*; in particular, whenever* n *is a prime and* n *does not divide* a*.*

EXAMPLE 1.68. To solve $6x \equiv 2 \mod 17$ we note that since 17 is a prime and 6 is not a multiple of 17, the unique solution is $X = [6]_{17}^{-1}[2]_{17} = [3]_{17}[2]_{17} = [6]_{17}$.

EXAMPLE 1.69. To solve a more substantial looking problem like $432x \equiv 12 \mod 546$ we need to do some more work. It is easily seen that $432 = 2^4 3^3$ and $546 = 2 \cdot 3 \cdot 7 \cdot 13$ and thus $6 = (432, 546)$. Hence $[72]_{91}X = [2]_{91}$ has a unique solution. To find it we need to calculate $[72]_{91}^{-1}$. This is, perhaps, best done by the GCD algorithm:

$$\left[\begin{array}{cc|c} 1 & 0 & 91 \\ 0 & 1 & 72 \end{array}\right] \xrightarrow{1} \left[\begin{array}{cc|c} 1 & -1 & 19 \\ 0 & 1 & 72 \end{array}\right] \xrightarrow{3} \left[\begin{array}{cc|c} 1 & -1 & 19 \\ -3 & 4 & 15 \end{array}\right] \xrightarrow{1} \left[\begin{array}{cc|c} 4 & -5 & 4 \\ -3 & 4 & 15 \end{array}\right]$$

$$\xrightarrow{3} \left[\begin{array}{cc|c} 4 & -5 & 4 \\ -15 & 19 & 3 \end{array}\right] \xrightarrow{1} \left[\begin{array}{cc|c} 19 & -24 & 1 \\ -15 & 19 & 3 \end{array}\right].$$

We read of that $19 \cdot 91 - 24 \cdot 72 = 1$; which tells us that $[72]_{91}^{-1} = [-24]_{91} = [67]_{91}$. So that $X = [43]_{91}$. In terms of congruence classes modulo 546, we have 6 solution; namely,

$$[43]_{546}, [134]_{546}, [225]_{546}, [316]_{546}, [407]_{546}, [498]_{546}.$$

THEOREM 1.70 (The Chinese remainder theorem, CRT). *Let* $r \in \mathbb{Z}_{>0}$ *and let* $m_1, m_2, ..., m_r$ *be relatively prime positive integers. Let* $a_1, a_2, ..., a_r$ *be any set of integers. Then the system of congruences*

$$x \equiv a_i \mod m_i, \quad i = 1, ..., r$$

has a unique solution modulo $M = m_1...m_r$*.*

PROOF. The theorem is obviously true for $r = 1$. So assume that $r > 1$. Observe however that the argument that follows holds (with appropriate understanding of symbols) for the case $r = 1$. Let $M_k = \frac{M}{m_k} = m_1...m_{k-1}\hat{m}_k m_{k+1}...m_r$, where $\hat{m}_k$ indicates that the m_k term is missing from the product. Then since $(m_i, m_j) = 1$ if $i \neq j$, we conclude that $(m_k, M_k) = 1$. Thus there exists $y_k \in \mathbb{Z}$ such that $[y_k]_{m_k} = [M_k]_{m_k}^{-1}$. We set

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + ... + a_r M_r y_r.$$

Then

$$[x]_{m_i} = [a_1]_{m_i}[M_1]_{m_i}[y_1]_{m_i} + [a_2]_{m_i}[M_2]_{m_i}[y_2]_{m_i} + ... + [a_r]_{m_i}[M_r]_{m_i}[y_r]_{m_i}.$$

But $[M_j]_{m_i} = 0$ if $j \neq i$. Hence

$$[x]_{m_i} = [a_i]_{m_i}[M_i]_{m_i}[y_i]_{m_i} = [a_i]_{m_i}.$$

If y is another solution the system of congruences, then for each i, $m_i|(y - x)$ hence lcm $(m_1, m_2, ..., m_r) = M|(y - x)$. □

EXAMPLE 1.71. To solve simultaneously (in $\mathbb{Z}$) the three equations

$$x \equiv 2 \mod 7,$$

$$x \equiv 0 \mod 9$$

and

$$2x \equiv 6 \mod 8,$$

we first solve the last equation to obtain $x \equiv 3$ or $7 \mod 8$: which is equivalent to $x \equiv 3 \mod 4$. We can replace our system of equation by the equivalent system

$$x \equiv 2 \mod 7,$$

$$x \equiv 0 \mod 9$$

and

$$x \equiv 3 \mod 4,$$

whose solution is

$$x \equiv 2 \cdot 36 \cdot 1 + 0 + 3 \cdot 63 \cdot 3 \equiv 135 \mod 252.$$

It is clear that computers should be of use in applications of CRT. We illustrate what can and cannot be done in MAPLE. Our first example is the solution of the system

$$x \equiv 12 \mod 13,$$

$$x \equiv 13 \mod 14,$$

$$x \equiv 14 \mod 23$$

and

$$x \equiv 15 \mod 25.$$

It would be quite a time consuming task to rely solely on calculators to solve this problem. We approach this problem as an algorithm involving a few steps.
1. We first verify that the hypothesis of CRT are satisfied (that is, that the moduli are relatively prime).
2. We know that the solution is a congruence class $a \mod M$. We compute M as the product of the moduli.
3. We determine next the smallest positive a. It is in the intersection of several sets that are easily described; the k^{th} set is a subset of the set of solutions to the k^{th} equation.

MAPLE SESSION #6.

```
> gcd(13,14);
                                1
> gcd(13,23);
                                1
> gcd(13,25);
                                1
> gcd(14,23);
                                1
> gcd(14,25);
                                1
```

```
> gcd(23,25);
```

$$1$$

```
> 13 * 14 * 23 * 25;
```

$$104650$$

```
> set1 := {seq( 12 + 13*i,i=0..200)}:  set2 := {seq( 13 +
  14*i,i=0..200)}:  set3 := {seq( 14 + 23*i,i=0..200)}:  set4 := {seq(
  15 + 25*i,i=0..200)}:
```

```
> set1 intersect set2 intersect set3 intersect set4;
```

$$\{\}$$

```
> set1 := {seq( 12 + 13*i,i=0..20000)}:  set2 := {seq( 13 +
  14*i,i=0..20000)}:  set3 := {seq( 14 + 23*i,i=0..20000)}:  set4 :=
  {seq( 15 + 25*i,i=0..20000)}:
```

```
> set1 intersect set2 intersect set3 intersect set4;
```

$$\{34215,\ 138865,\ 243515\}$$

```
> chrem([12,13,14,15],[13,14,23,25]);
```

$$34215$$

END OF PROGRAM

- The first 6 lines of the program are just a check on the hypothesis for the Chinese remainder theorem. They can be combined into a single command as is done in the next program.
- The 8^{th} line of the program defines the sets whose intersection should yield a solution. However we have truncated the sets too quickly as is shown by the next line.
- The next to the last section of the program shows that the simultaneous solutions to the set of four equations is the congruence class

$$34215 \mod 104650$$

  (we use the single calculation $104650 = 138865 - 34215$).
- The last section of the program shows the single MAPLE command needed to get the smallest positive solution.

A slightly different picture emerges in the MAPLE solution to a similar set of congruences involving bigger numbers

$$x \equiv 12 \mod 993,$$

$$x \equiv 13 \mod 994,$$

$$x \equiv 14 \mod 1003$$

and

$$x \equiv 15 \mod 1007.$$

MAPLE SESSION #7.

```
> [gcd(993,994),
> gcd(993,1003),
> gcd(993,1007),
> gcd(994,1003),
> gcd(994,1007),gcd(1003,1007)];
```

$$[1, 1, 1, 1, 1, 1]$$

```
> 993 * 994 * 1003 * 1007;
```

$$996933147882$$

```
> set1 := {seq( 12 + 993*i,i=0..200)}:  set2 := {seq( 13 +
  994*i,i=0..200)}:  set3 := {seq( 14 + 1003*i,i=0..200)}:  set4 :=
  {seq( 15 + 1007*i,i=0..200)}:
> set1 intersect set2 intersect set3 intersect set4;
```

$$\{\}$$

```
> set1 := {seq( 12 + 993*i,i=0..20000)}:  set2 := {seq( 13 +
  994*i,i=0..20000)}:  set3 := {seq( 14 + 1003*i,i=0..20000)}:  set4 :=
  {seq( 15 + 1007*i,i=0..20000)}:
> set1 intersect set2 intersect set3 intersect set4;
```

$$\{\}$$

```
> set1 := {seq( 12 + 993*i,i=0..2000000)}:  set2 := {seq( 13 +
  994*i,i=0..2000000)}:  set3 := {seq( 14 + 1003*i,i=0..2000000)}:
  set4 := {seq( 15 + 1007*i,i=0..2000000)}:


Warning, computation interrupted
> chrem([12,13,14,15],[993,994,1003,1007]);
```

$$630257901363$$

END OF PROGRAM

Note that the naive calculations that look for a solution as an intersection of four sets runs into time problems (hence the interruption). However, the `chrem` MAPLE command is powerful enough to perform its calculation in a very short period of time. It follows that MAPLE uses a more sophisticated algorithm in solving simultaneous congruence equations.

REMARK 1.72. The hypothesis that $(m_i, m_j) = 1$ for $i \neq j$ cannot be replaced by the weaker hypothesis $(m_1, m_2, ..., m_r) = 1$ as is easily shown by the example

$$x \equiv 0 \mod 2,$$

$$x \equiv 0 \mod 3$$

and

$$x \equiv 1 \mod 4$$

that has no solutions; since the first of theses three equations says that x must be even and the last that it must be odd.

We end this section with a brief introduction to non-linear congruences.

EXAMPLE 1.73. We start with the equation

$$x^2 - 1 \equiv 0 \mod n.$$

It is equivalent to the equation

$$(x-1)(x+1) \equiv 0 \mod n.$$

So if x is a solution, then $x-1$ and $x+1$ are either 0 or zero divisors. Thus if n is prime, the only solutions are $x = 1$ and $x = n-1$ (modulo n, of course). For composite n, $x = 1$, $x = n-1$ are still solutions. But there may be others (extra solutions) as well. They are to be found among the x for which both $x \pm 1$ are zero divisors. The zero divisors for $n = 6$ are 2, 3 and 4. Thus only $x = 3$ could be an extra solution, but it is not. For $n = 8$, the solutions are 1, 3, 5 and 7. The zero divisors in this case are 2, 4 and 6. Each extreme pair of these accounts for one solution. For $n = 25$, only 5 is a zero divisor. Hence, only 1 and 24 are solutions.

EXAMPLE 1.74. We continue with the equation

$$x^2 + 1 \equiv 0 \mod n$$

and try to find its roots. Once again the answer depends on n. For $n = 2$, 1 is a solution. There are no solutions for $n = 3$ and 4. For $n = 5$, $x = 2$ and 3 are the solutions. Obviously this is a place where a symbolic computation program will help. Using MAPLE (a worksheet is included below), we see that for $n = 125$, $x = 57$ and 68 are solutions leading us to the factorization

$$x^2 + 1 \equiv (x-57)(x-68) \mod 125.$$

Perhaps more surprising is the case $n = 65$ where 8, 18, 47 and 57 are solutions giving us two factorizations

$$x^2 + 1 \equiv (x-8)(x-57) \mod 65$$

and

$$x^2 + 1 \equiv (x-18)(x-47) \mod 65.$$

A self-explanatory MAPLE program (reproduced below) facilitates the computations in this example.

MAPLE SESSION #8.

```
> msolve({x^2 + 1 = 0}, 2);
```

$$\{x = 1\}$$

```
> msolve({x^2 + 1 = 0}, 3);
> msolve({x^2 + 1 = 0}, 4);
> msolve({x^2 + 1 = 0}, 5);
```

$$\{x = 2\}, \{x = 3\}$$

```
> msolve({x^2 + 1 = 0}, 125);
```

$$\{x = 57\}, \{x = 68\}$$

```
> msolve({x^2 + 1 = 0}, 65);
```

$$\{x = 8\}, \{x = 18\}, \{x = 47\}, \{x = 57\}$$

```
> msolve({x^2 + 1 = 0}, 13);
```

$$\{x = 5\}, \{x = 8\}$$

```
> msolve({x^2 + 1 = 0}, 17);
```

$$\{x = 4\}, \{x = 13\}$$

```
> msolve({x^2 + 1 = 0}, 19);
```

END OF PROGRAM

EXAMPLE 1.75. Our last example of this section is a brief discussion of the polynomial

$$x^3 - x^2 + x + 2. \tag{9}$$

We investigate whether it can have any integral roots. One can learn from more advanced algebra books (or courses) that the only possible integral roots of the polynomial are ± 1 and ± 2 and that none of these are in fact roots to conclude that the equation has no integer roots (see Section 10). Without more advanced results we can come to the same conclusion using modular arithmetic. If (9) had an integer root, then for every $n \in \mathbb{Z}_{>1}$ reducing modulo n, we would certainly have a root in $\mathbb{Z}_n$. Let $f(r) = r^3 - r^2 + r + 2$. Then $f(0) = 2$, $f(1) = 3$, $f(2) = 8$, $f(3) = 23$ and $f(4) = 54$. So the equation $f(r) \equiv 0 \mod 5$ has no solutions. Hence (9) cannot have any integral solutions.

8. Euler

Let us fix a positive integer n. For $a \in \mathbb{Z}$, we have determined conditions that guarantee the existence of $[a]_n^{-1}$ and algorithms for computing it. Two results that give formulae for this inverse (due to Fermat for n prime and to Euler for the general case) turn out to have good applications to cryptography.

DEFINITION 1.76. Let $n \in \mathbb{Z}_{>0}$ and $a \in \mathbb{Z}$. The integer a (or the equivalence class $[a]_n$) has *finite multiplicative order modulo* n if there exists a $k \in \mathbb{Z}_{>0}$ such that

$$[a]_n^k = ([a^k]_n) = [1]_n.$$

If a has finite multiplicative order modulo n, then the smallest k as above is the *(multiplicative) order of* a *(and of* $[a]_n$*) modulo* n; in symbols $\mathrm{ord}_n a$ (ord $[a]_n$) or ord a (ord $[a]$) when the n is clear from the context.

REMARK 1.77. Only $[1]_n$ has order 1.

THEOREM 1.78. *Let* $n \in \mathbb{Z}_{>0}$ *and* $a \in \mathbb{Z}$. *The following conditions are equivalent:*
(a) *The integer* a *has finite multiplicative order modulo* n.
(b) $(a, n) = 1$.
(c) $[a]_n$ *is invertible.*
(d) $[a]_n \neq [0]_n$ *and* $[a]_n$ *is not a zero divisor.*

PROOF. The equivalence of conditions (b), (c) and (d) has already been established. If a has finite multiplicative order, then $[a]_n^k = [a]_n[a]_n^{k-1} = [1]_n$ and so $[a]_n$ is invertible. Thus (a) implies (c). To establish the converse (that (c) implies (a)), consider the list of $n + 1$ elements

$$[a]_n, [a]_n^2, ..., [a]_n^{n+1}$$

in $\mathbb{Z}_n$. Since $|\mathbb{Z}_n| = n$, two elements in the list must be the same. Thus

$$[a]_n^k = [a]_n^t \text{ for some } 1 \leq k < t \leq n+1.$$

If $[a]_n$ is invertible, we can multiply both sides of the last equation by $[a]_n^{-k}$ and conclude that $[1]_n = [a]_n^{t-k}$. □

THEOREM 1.79. *Suppose that $a \in \mathbb{Z}$ has order k modulo n. Then*

$$a^r \equiv a^s \mod n \text{ if and only if } r \equiv s \mod k.$$

PROOF. The fact that a has order k modulo n means that $a^k = 1 + nw$ for some $w \in \mathbb{Z}$. If $r \equiv s \mod k$, then $r = s + tk$ for some $t \in \mathbb{Z}$. Then

$$a^r = a^{s+tk} = a^s a^{tk} = a^s(1+nw)^t \equiv a^s \mod n.$$

Conversely, if $a^r \equiv a^s \mod n$, we may without loss of generality assume that $r \leq s$. Since $(a, n) = 1$, $[a]_n^{-1}$ exists and we conclude that $1 \equiv a^{s-r} \mod n$. The division algorithm tells us that $s - r = qk + u$ for some q and $u \in \mathbb{Z}$ with $0 \leq u < k$. Therefore $1 \equiv a^{s-r} \equiv a^u \mod n$. Since k is the smallest positive integer with $a^k \equiv 1 \mod n$, we conclude that $u = 0$. □

THEOREM 1.80 (Fermat's little theorem). *Let p be a prime and suppose that $a \in \mathbb{Z}$ is not a multiple of p. Then $a^{p-1} \equiv 1 \mod p$. Hence for all $a \in \mathbb{Z}$, $a^p \equiv a \mod p$.*

PROOF. The group[17] $\mathbb{Z}_p^*$ has $p-1$ elements:

$$[1]_p, [2]_p, ..., [p-1]_p.$$

For $[a]_p \in \mathbb{Z}_p^*$, denote by $[a]_p\mathbb{Z}_p^*$ the set of multiples of $[a]_p$ in $\mathbb{Z}_p^*$:

$$[a]_p\mathbb{Z}_p^* = \{[a]_p[b]_p; [b]_p \in \mathbb{Z}_p^*\} = \{[a]_p[1]_p, [a]_p[2]_p, ..., [a]_p[p-1]_p\} \subseteq \mathbb{Z}_p^*.$$

We observe next that $\left|[a]_p\mathbb{Z}_p^*\right| = p-1$ because no two elements of $\mathbb{Z}_p^*$ are equal. (If $[a]_p[b]_p = [a]_p[c]_p$, then since $[a]_p$ is invertible, $[b]_p = [c]_p$.) Hence

$$[1]_p[2]_p...[p-1]_p = [a]_p[1]_p[a]_p[2]_p...[a]_p[p-1]_p = [a]_p^{p-1}[1]_p[2]_p...[p-1]_p$$

and it follows (by cancellation) that $[a]_p^{p-1} = [1]_p$. This establishes the first part of the theorem; also that $a^p \equiv a \mod p$ whenever p does not divide a. But this last assertion is trivial for multiples of p. □

COROLLARY 1.81. *Let p be a prime and suppose that $a \in \mathbb{Z}$ is not divisible by p. Then the order of $a \mod p$ divides $(p-1)$.*

PROOF. The theorem shows that $[a]_p^{p-1} = [1]_p$. If k is the order of $a \mod p$, then $[a]_p^k = [1]_p$ and Theorem 1.79 tells us that $p - 1 \equiv k \mod k$. □

EXAMPLE 1.82. For all primes p, the order of $[1]_p$ is, of course, 1 and the order of $[p-1]_p$ is 2 provided p is odd. All possibilities allowed by the theorem do occur. In $\mathbb{Z}_7^*$, for example, the orders of the *units* $[1]_7, [2]_7, [3]_7, [4]_7, [5]_7$ and $[6]_7$ are 1, 3, 6, 3, 6 and 2, respectively.

We now come to one of the most important functions in number theory, the *Euler φ-function.*

DEFINITION 1.83. For each $n \in \mathbb{Z}_{>0}$, we let $\varphi(n) = |\mathbb{Z}_n^*|$. Thus $\varphi(n)$ is the number of positive integers $\leq n$ that are relatively prime to n. (Note that $\varphi(1) = 1$.)

[17]Language to be justified later.

The reader should check that the entries in the following table are correct.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6

It is perhaps surprising that there is an easy formula for $\varphi(n)$. We now begin the journey toward (1.86).

PROPOSITION 1.84. *If p is a prime and $n \in \mathbb{Z}_{>0}$, then*

$$\varphi(p^n) = p^n - p^{n-1}.$$

PROOF. The only integers between 1 and p^n (including both ends) that are not relatively prime to p^n are the multiples of p, namely

$$p, 2p, ...p^{n-1}p.$$

There are exactly p^{n-1} such integers. □

THEOREM 1.85. *If a and b are relatively prime positive integers, then*

$$\varphi(ab) = \varphi(a)\varphi(b).$$

PROOF. Since $\varphi(1) = 1$, there is nothing to prove if either a or $b = 1$. So assume that both are in $\mathbb{Z}_{>1}$. The theorem says that the number of elements in $\mathbb{Z}_{ab}^*$, $|\mathbb{Z}_{ab}^*|$, is the product of $|\mathbb{Z}_a^*|$ and $|\mathbb{Z}_b^*|$. We construct a one-to-one surjective map[18]

$$f : \mathbb{Z}_a^* \times \mathbb{Z}_b^* \to \mathbb{Z}_{ab}^*.$$

A point in the direct product $\mathbb{Z}_a^* \times \mathbb{Z}_b^*$ is a pair $([r]_a, [s]_b)$, where r and s are positive integers relatively prime to a and b, respectively. By the Chinese remainder theorem, there is a unique congruence class $[t]_{ab}$ (the notation is meant to imply that we are choosing a representative $t \in \mathbb{Z}$ of this class) such that

$$t \equiv r \mod a \text{ and } t \equiv s \mod b.$$

Since $t = r + ka$ for some $k \in \mathbb{Z}$ and $(r, a) = 1$, we conclude that $(t, a) = 1$. Similarly $(t, b) = 1$. Thus $(t, ab) = 1$; that is, $[t]_{ab} \in \mathbb{Z}_{ab}^*$. Hence we define f by

$$f([r]_a, [s]_b) = [t]_{ab}.$$

We need to show that the map is f is an isomorphism (one-to-one and onto). We proceed indirectly by constructing a map

$$g : \mathbb{Z}_{ab}^* \to \mathbb{Z}_a^* \times \mathbb{Z}_b^*$$

that is an inverse of f. Let $[t]_{ab} \in \mathbb{Z}_{ab}^*$. Choose the unique r and $s \in \mathbb{Z}$ such that $0 \le r < a$, $0 \le s < b$, $[t]_a = [r]_a$ and $[t]_b = [s]_b$. We define

$$g([t]_{ab}) = ([r]_a, [s]_b).$$

We must show that $[r]_a \in \mathbb{Z}_a^*$; that is, that $(a, r) = 1$. This is shown as follows. Since $(ab, t) = 1$, we must also have that $(a, t) = 1$. Since $t \equiv r \mod a$ it follows from $(a, t) = 1$ that $(a, r) = 1$. Similarly we see that $[s]_b \in \mathbb{Z}_b^*$. It is clear from the uniqueness part of the Chinese remainder theorem that $f \circ g$ is the identity self map of $\mathbb{Z}_{ab}^*$. Hence g is injective and f is surjective. The fact that g is one-to-one tells us that $|\mathbb{Z}_{ab}^*| \ge |\mathbb{Z}_a^*||\mathbb{Z}_b^*|$. The fact that f is onto tells us that $|\mathbb{Z}_{ab}^*| \le |\mathbb{Z}_a^*||\mathbb{Z}_b^*|$. The last two inequalities imply equality. □

[18] As we shall see later, an isomorphism between groups.

THEOREM 1.86. *Let $n \in \mathbb{Z}_{>1}$ have prime factorization $n = \prod_{i=1}^{r} p_i^{n_i}$ with the p_i distinct primes and the exponents $n_i > 0$. Then*

$$\varphi(n) = \prod_{i=1}^{r} \left(p_i^{n_i} - p_i^{n_i - 1}\right) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

PROOF. The first formula is proven by induction on r. The base case $r = 1$ is the content of Proposition 1.84. So assume that we have the formula for $r = k \geq 1$ and proceed to establish it for $r = k + 1$. Write

$$n = \prod_{i=1}^{k+1} p_i^{n_i} = \left(\prod_{i=1}^{k} p_i^{n_i}\right) p_{k+1}^{n_{k+1}}.$$

Since $\left(\prod_{i=1}^{k} p_i^{n_i}, p_{k+1}^{n_{k+1}}\right) = 1$, we conclude by the induction hypothesis and the last theorem that

$$\varphi\left(\prod_{i=1}^{k+1} p_i^{n_i}\right) = \varphi\left(\left(\prod_{i=1}^{k} p_i^{n_i}\right) p_{k+1}^{n_{k+1}}\right) = \left(\prod_{i=1}^{k} \left(p_i^{n_i} - p_i^{n_i - 1}\right)\right)\left(p_{k+1}^{n_{k+1}} - p_{k+1}^{n_{k+1}-1}\right) =$$

$$\prod_{i=1}^{k+1} \left(p_i^{n_i} - p_i^{n_i - 1}\right).$$

This finishes the proof of the first equality; the second equality is a consequence of an easy algebraic manipulation. □

Our next result is a generalization of Fermat's little theorem.

THEOREM 1.87 (Euler). *Let $n \in \mathbb{Z}_{\geq 2}$ and suppose that $a \in \mathbb{Z}$ is relatively prime to n. Then $a^{\varphi(n)} \equiv 1 \mod n$.*

PROOF. The argument here is a generalization of the one used to establish Fermat's little theorem. The group $\mathbb{Z}_n^*$ has $\varphi(n)$ elements. As before, $[a]_n \in \mathbb{Z}_n^*$ and $[a]_n\mathbb{Z}_n^*$ denotes the set of multiples of $[a]_n$ in $\mathbb{Z}_n^*$: $[a]_n\mathbb{Z}_n^* = \{[a]_n[b]_n; [b]_n \in \mathbb{Z}_n^*\}$. As in the earlier proof $|[a]_n\mathbb{Z}_n^*| = \varphi(n)$ because no two elements of $\mathbb{Z}_n^*$ are equal. Hence

$$\prod_{b \in \mathbb{Z}_n^*} b = \prod_{b \in \mathbb{Z}_n^*} ab = a^{\varphi(n)} \prod_{b \in \mathbb{Z}_n^*} b,$$

and Euler's theorem follows by cancellation. □

COROLLARY 1.88. *Let $n \in \mathbb{Z}_{\geq 2}$ and suppose that $a \in \mathbb{Z}$ is relatively prime to n. Then the order of $a \mod n$ divides $\varphi(n)$.*

EXAMPLE 1.89. We determine the congruence class $\mod 14$ of 3^{19}. We can, of course use the MAPLE command `> 3^{19} \mod 14`; and receive 3 as the answer. But this problem can be solved and was solved before and without MAPLE. The order of 3 modulo 14 divides $\varphi(14) = 6$. Hence $3^{18} \equiv 1 \mod 14$ and thus $3^{19} \equiv 3 \mod 14$.

EXAMPLE 1.90. We determine the last two digits of 7^{2962}. Again MAPLE readily supplies the answer; although it (version 7) has trouble obtaining the last two digits of $7^{2962!}$. The last two digits of an integer are determined by its congruence class $\mod 100$. The order of $7 \mod 100$ divides $\varphi(100) = \varphi(2^2 5^2) = 2 \cdot 20 = 40$. Hence $7^{40r} \equiv 1 \mod 100$ for every

positive integer r. Thus $7^{2962} = 7^{99\cdot 40+2} \equiv 49 \mod 100$ and $7^{2962!} \equiv 1 \mod 100$ because $40|2962!$. Can we determine this way the last two digits of 6^{2962}? Not exactly as before. $6^{2962} = 2^{2962}3^{2962}$. As before $3^{2962} \equiv 9 \mod 100$. But at this point we do not have the tools to conclude (without a brute force calculation using MAPLE, for example) that $2^{2962} \equiv 4 \mod 100$.

DEFINITION 1.91. Let $a \in \mathbb{Z}$ with $(a, n) = 1$. The *(multiplicative) inverse* of $[a]_n \in \mathbb{Z}_n^*$ is the unique $[b]_n \in \mathbb{Z}_n^*$ with $[a][b] = [ab] = [1]$. We have seen that if $[a]$ has order k, then its inverse exists and $[b] = [a]^{k-1} = [a]^{\varphi(n)-1}$.

REMARK 1.92. We have been studying three systems. The language will be established in subsequent chapters:

- $(\mathbb{Z}_n, +, \cdot)$ is a *commutative ring*.
- $(\mathbb{Z}_n, +)$ is a *cyclic abelian group* of *order* n with generator $[1]$.
- $(\mathbb{Z}_n^*, \cdot)$ is an abelian group of order $\varphi(n)$; usually not cyclic.

EXERCISES

(1) Find the orders of
   (a) $2 \mod 31$,
   (b) $3 \mod 75$ and
   (c) $4 \mod 27$.

(2) Show that $a \in \mathbb{Z}$ has order k modulo n if and only if $k \in \mathbb{Z}_{>0}$ is the smallest integer such that $a^k - 1 = nw$ for some $w \in \mathbb{Z}$.

(3) Prove that a and a^5 have the same last digit for all $a \in \mathbb{Z}_{>0}$.

(4) Let a and $b \in \mathbb{Z}$. Prove that

$$\varphi\left(\frac{a}{\gcd(a,b)}\right)\varphi\left(\frac{b}{\gcd(a,b)}\right) = \varphi\left(\frac{\operatorname{lcm}(a,b)}{\gcd(a,b)}\right).$$

(5) For what positive integers n is $\varphi(n) \leq 8$?

(6) In this exercise we study an additive version of the (multiplicative) order function.
   - Verify the entries in

Order of elements of $\mathbb{Z}_{24}^*$

a	1	5	7	11	13	17	19	23
ord a	1	2	2	2	2	2	2	2

   - Let $n \in \mathbb{Z}_{>0}$ and let $a \in \mathbb{Z}_n$. In analogy with the definition of the multplivative order of $a \in \mathbb{Z}_n^*$, define the additive order of $a \in \mathbb{Z}_n$.
   - Your definition should produce the following:

Order of elements of $\mathbb{Z}_{24}$

a	0	1	2	3	4	5	6	7	8	9	10	11
ord a	1	24	12	8	6	24	4	24	3	12	12	24

a	12	13	14	15	16	17	18	19	20	21	22	23
ord a	2	24	12	8	3	24	4	24	12	8	12	24

9. Public key cryptography

Let us assume that we have a large number, $N \in \mathbb{Z}_{>0}$, of people who want to communicate (say on the web) in a more or less secure manner. Electronically, we can only transmit numbers. So the first task is to translate the letters of our alphabet to numbers. We can certainly choose a subset of the integers between 1 and 100 to accomplish this. Say we may set up the following correspondence

$$A = 03,\ B = 07,\ C = 13,\ D = 17, E = 21,\ ...,\ Y = 77,\ Z = 91,$$
$$blank = 93,\ , = 98,\ . = 99,$$

known as a *code book* or an *encryption algorithm*. The message 170377 would hence be read as DAY. We share the code book between our set of N correspondents. We now have no problem sending messages to each other. If our code is secure (more on this later), only the N communicators:

$$\Pi_1, \Pi_2, ..., \Pi_N$$

can *code* (changing the letters to numbers) and *decode* (changing the numbers back to the "correct" letters) messages. There is a problem with this scheme. Say that two communicators Π_1 and Π_2 want to keep the information they exchange from all the other communicators Π_j, $j > 2$. This can certainly be accomplished if each pair of communicators had their own code book. But this would require a huge number, $\begin{pmatrix} N \\ 2 \end{pmatrix} = \frac{N(N-1)}{2}$, of code books.

We consider a way to cut down the number of code books. Say that Π_1 wants to be able to receive messages from each Π_j, $j > 1$, in such a way that if $j \neq k$, j and $k > 1$, then neither Π_j nor Π_k can decode the other's message. This can be accomplished through what is known as a *public key code*. In this system Π_1 publishes (for everyone to know) an encryption algorithm that only s/he can decode. Sounds hard, but it is really easy in theory. We describe the *RSA system*, one of several that accomplishes this, named after its inventors: Rivest, Shamir and Adleman.

We (Π_1) start(s) by selecting two very large distinct primes p and q and forming their product $n = pq$ which is the *base* for the *encryption algorithm*. We know that

$$\varphi(n) = (p-1)(q-1);$$

but a knowledge of n which we publish is insufficient to determine $\varphi(n)$ since in practice it is very difficult to factor large integers[19]. Next we choose a number a relatively prime to $\varphi(n)$, the *exponent* for the encryption algorithm which we also publish. Assign a positive number (consisting, for convenience, of a fixed number of digits) to each letter in the alphabet (the alphabet usually includes, the ordinary (English) letters, the digits 0 through 9, punctuation marks, and other special symbols) to form a *dictionary* – also part of the public knowledge. A message to be transmitted now consists of a large number of positive integers which form when written sequentially a *digited message*. Break the digited message into blocks b of length less than the number of digits[20] in p and in q, but larger than the number of symbols in two letters of the alphabet (so that no block contains only zeros). The block b is a non-zero integer. By construction $1 \leq b < p$ and $1 \leq b < q$. In particular, b cannot divide p nor q and thus $(b, n) = 1$. We encode the block b, by computing the standard representative m of b^a mod n. The encoding can be done by anyone who knows the dictionary (the construction of

[19]This is the key to the method.

[20]Remember than in practice p, q and b are very large.

b), the base (n) and the exponent (a). We (Π_1) need (needs) to recover b from m. By the construction we outlined, $(b, n) = 1$ and hence $[b]_n$ is a unit in $\mathbb{Z}_n$ (thus in $\mathbb{Z}_n^*$). So is $[m]_n$, a power of $[b]_n$. Raising $[m]_n$ to the x^{th} power is the same as raising $[b]_n$ to the ax^{th} power. An appropriate power, for example, $1 + \alpha\varphi(n)$ or $1 + \beta \operatorname{ord}_n a$ (with α and β arbitrary integers), of $[b]_n$ yields back $[b]_n$

Now Π_1 kept p and q (equivalently $\varphi(n)$) secret. S/he will use this information to choose the appropriate x. We know that $1 = (a, \varphi(n))$; thus 1 can be written as an integral linear combination

$$ax + \varphi(n)y$$

of a and $\varphi(n)$. The integers x and y are computed by the methods at our disposal: namely, the Euclidean or GCD algorithms. Anyone who knows $\varphi(n)$ can obtain x (and hence decode the message) – but only Π_1 knows this value. Even the sender of the message cannot decode what s/he sent, if s/he forgot to keep a copy of the message before it was encoded. With the above value of x, we have

$$ax = 1 - y\varphi(n)$$

and thus

$$m^x \equiv b^{ax} \equiv b \mod n.$$

WORKSHEET #3

On the construction and deconstruction of codes.

(1) In this exercise on the RSA code, you will encode a message for transmission, decode a transmitted message, and then break an intercepted coded message. All coding in this exercise assumes that the primes p and q are chosen between 100 and 200.

(2) We use the alphabet

$$A = 03,\ B = 07,\ C = 13,\ D = 17,\ E = 21,\ F = 31,\ G = 32,$$

$$H = 33,\ I = 34,\ J = 35,\ K = 36,\ L = 37,\ M = 38,\ N = 39,$$

$$O = 40,\ P = 41,\ Q = 43,\ R = 44,$$

$$S = 45,\ T = 46,\ U = 47,\ V = 48,\ W = 49,\ X = 50,\ Y = 77,\ Z = 91,$$

$$blank = 93,\ , = 98,\ . = 99.$$

Assume throughout this exercise that the transmission blocks have length 5. (This is suggested by the size of n.)

(3) The base n for the encryption algorithm for the SUPERSECRET CODE is publicly announced to be 23711. The exponent a for the encryption algorithm is chosen as (and announced to be) 121.

(4) Encode the message

STUDY MATHEMATICS.

(5) The secret part of the SUPERSECRET CODE is the fact that $\varphi(n) = 23400$.

(6) Decode the intercepted message

136151991720194080401297100951137682019412971014141860601859174 75

(7) Another SECRET CODE uses the base $n = 12091$ and exponent $a = 121$. The value of $\varphi(n)$ is under continuous lock and key. You will need to discover it to decode the intercepted message:

$$01111095650956504835012310990701111089500096604835$$
$$09907048350895006338080860990704835016090895000966048351152 8$$

(8) What is $\varphi(n)$? What is the content of the intercepted message?
(9) What in addition to $\varphi(n)$ did you need to know in order to break the code?
(10) Which code is easier to break, the SECRET CODE or the SUPERSECRET CODE? Why?

10. A collection of beautiful results

In this section we collect some beautiful consequences of the theory developed in this chapter, especially if the results suggest futher areas and questions for study. We limit the discussion to results relevant to the high school mathematics curriculum. Some of the proofs "formally" require material to be developed in subsequent chapters of this book.

Primes cannot be congruent to 0 mod 4. The unique even prime is the only one congruent to 2 mod 4. An odd prime is hence congruent to 1 or 3 mod 4.

THEOREM 1.93. *Infinitely many primes are congruent to* 3 mod 4.

PROOF. The set of primes congruent to 3 mod 4 is certainly not empty, since it contains 3, 7 and 11, for example. Assume that it is a finite set: $\{3 = p_1,\ p_2,\ ...,\ p_r\}$. It suffices to produce a prime $p \equiv 3 \mod 4$ not on this list. Let

$$Q = 4p_2...p_r + 3.$$

Then obviusly $Q \equiv 3 \mod 4$. Consider the prime factorization of Q. Since Q is odd, the prime 2 does not appear in this factorization, Since 3 does not divide Q, neither does this prime. If only primes $\equiv 1 \mod 4$ appeared, then Q would also be $\equiv 1 \mod 4$. We conclude that at least one prime $p \neq 3$, $p \equiv 3 \mod 4$ must appear in the factoriation. Now $p \neq p_j$ for $2 \leq j \leq r$ since such a p_j does not divide Q. We have produced a prime $p \equiv 3 \mod 4$ not on our list. □

REMARK 1.94. The theorem suggests many avenues for further exploration.

- There are infinitely many primes $\equiv 1 \mod 4$, but this is harder to establish than our last result.
- It is a consequence of a theorem of G. Lejeune Dirichlet that there are infinitely many primes p of the form are $an + b,\ n \in \mathbb{Z}_{>0}$, where a and b are fixed integers with $(a, b) = 1$.
- In 2004, Ben Green and Terrence Tao proved, the remarkable result that there are arbitrarily long arithmetic progressions of primes.

The next two theorems will appear more relevant after, and serve as an inducement for, the study of polynomials – in the last few chapters of this book.

THEOREM 1.95. *If $\alpha \in \mathbb{Q}$ is a root of the monic polynomial*

$$x^n + a_1x^{n-1} + \ ... \ a_n$$

with integer coefficients (thus $n \in \mathbb{Z}_{>0}$ and $a_j \in \mathbb{Z}$ for $1 \leq j \leq n$), then $\alpha \in \mathbb{Z}$.

PROOF. Since $\alpha = \frac{a}{b},\ a \in \mathbb{Z},\ b \in \mathbb{Z}_{>0}$, is a root of the above polynomial

$$\left(\frac{a}{b}\right)^n + a_1\left(\frac{a}{b}\right)^{n-1} + \ ... \ a_n = 0,$$

it involves no loss of generality to assume that $(a, b) = 1$. Clearing fractions in the last equation we obtain

$$a^n + a_1 a^{n-1} b + \ ... \ a_n b^n = 0$$

equivalently

$$a^n = -b\left(a_1 a^{n-1} + \ ... \ a_n b^{n-1}\right).$$

Thus $b|a^n$. Since $(a, b) = 1$, the last divisibilty condition guarantees that $b = 1$ and thus $\alpha = a$. □

THEOREM 1.96. *If $\alpha \in \mathbb{Z}$ is a root of the monic polynomial*

$$p(x) = x^n + a_1 x^{n-1} + \ ... \ a_n,$$

then $\alpha|a_n$.

PROOF. The proof is by induction on n, the degree of the monic polynomial. If $n = 1$, then the polynomial is of the form $x + a$ and $-a$ is its root. Consider the general case $n > 1$. If the polynomial $p(x)$ does not have an integral root, there is nothing to prove. If it has an integral root α, then by the division algorithm for polynomials

$$x^n + a_1 x^{n-1} + \ ... \ a_n = (x^{n-1} + b_1 x^{n-2} + \ ... \ b_{n-1})(x - \alpha),$$

where $b_j \in \mathbb{Z}$ for $j = 1,\ 2,\ ...,\ n - 1$. Now $\alpha|a_n = -b_{n-1}\alpha$. If the polynomial $p(x)$ has another integral root β, then β must be a root of the polynomial $x^{n-1} + b_1 x^{n-2} + \ ... \ b_{n-1}$ of degree $n - 1$. The induction hypothesis tells us that $\beta|b_{n-1}$ and hence also $\beta|a_n$. □

CHAPTER 2

Foundations

This chapter consists of material that should be familiar to most readers (students). It should be reviewed, as needed, to establish a common notation for the author and reader. The last section on complex number is needed only for a discussion of examples and the study of roots of polynomials.

1. Naive set theory

A *set* is a formally undefined object (informally, a collection of objects) containing (formally undefined) *members* or *elements*. The notation $x \in X$ (as well as $X \ni x$) is to denote that X is a set and that x is an element of X (we will also say that x *belongs* to X); similarly, $x \notin X$ is to denote that X is a set and that x is not an element of X. In Chapter 1 we worked with sets of integers and we denoted by expressions enclosed by braces {....} collections of integers. Typical ways of describing the set of even integers between between 2 and 20 (inclusive) are:

$$\{2, 4, 6, 8, 10, 12, 14, 16, 28, 20\},$$

$$\{2r; r \in \mathbb{Z} \text{ and } 1 \leq r \leq 10\}$$

and

$$\{r \in \mathbb{Z}; r \text{ is even and } 1 \leq r \leq 21\}.$$

To avoid logical complications we work in a *universal* set U and assume that all the members of all sets under study are in U. Thus all set are subsets (defined below) of U.

Definition 2.1. We reserve the symbol $\emptyset$ for the *emptyset*; the set containing no elements. For a given set X, X^c denotes its *complement* consisting of the points in U that are not in X;

$$X^c = \{x \in U; x \notin X\}.$$

Given two sets X and Y, we define several relations between them and operations on them. We say that X *equals* Y (in symbols $X = Y$), if both sets contain exactly the same elements. We say that X is a *subset* of Y (or X is *included* in Y) (in symbols $X \subseteq Y$ or $Y \supseteq X$) if every element $x \in X$ also belongs to Y. (Note that by our conventions, $X \subseteq U$, $X = Y$ if and only if $X \subseteq Y$ and $Y \subseteq X$, and $\emptyset \subseteq X$.) The set inclusion $X \subseteq Y$ is *proper* (in symbols $X \subset Y$) if $X \neq Y$. We define the *union* and *intersection* of X and Y by

$$X \cup Y = \{x \in U; x \in X \text{ or } x \in Y\}$$

and

$$X \cap Y = \{x \in U; x \in X \text{ and } x \in Y\}.$$

The collection of sets satisfies many basic properties similar to those satisfied by the integers as illustrated in the following

PROPOSITION 2.2. *Let X, Y and Z be three sets (all contained in the same universal set U). The following properties hold:*

(1) *(idempotence) $X \cap X = X$ and $X \cup X = X$,*
(2) *(complementarity) $X \cap X^c = \emptyset$ and $X \cup X^c = U$,*
(3) *(commutativity) $X \cap Y = Y \cap X$ and $X \cup Y = Y \cup X$,*
(4) *(associativity) $X \cap (Y \cap Z) = (X \cap Y) \cap Z$ and $X \cup (Y \cup Z) = (X \cup Y) \cup Z$,*
(5) *(de Morgan's laws) $(X \cap Y)^c = X^c \cup Y^c$ and $(X \cup Y)^c = X^c \cap Y^c$,*
(6) *(distributivity) $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$ and $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$,*
(7) *(complementation is an involution) $(X^c)^c = X$,*
(8) *(properties of $\emptyset$) $X \cap \emptyset = \emptyset$ and $X \cup \emptyset = X$,*
(9) *(properties of U) $X \cap U = X$ and $X \cup U = U$, and*
(10) *(absorption properties) $X \cap (X \cup Y) = X$ and $X \cup (X \cap Y) = X$.*

PROOF. We establish only the first equality in (5) and (7) leaving it to the reader to fill in sequentially the missing proofs. We start with (5). Let $x \in (X \cap Y)^c$. Then $x \notin X \cap Y$. So $x \notin X$ or $x \notin Y$. In the first possibility, $x \in X^c$; in the second $x \in Y^c$. So certainly $x \in X^c \cup Y^c$ and thus $(X \cap Y)^c \subseteq X^c \cup Y^c$. Conversely, if $x \in X^c \cup Y^c$, then either $x \in X^c$ or $x \in Y^c$. So either $x \notin X$ or $x \notin Y$. So certainly, $x \notin X \cap Y$ and hence $x \in (X \cap Y)^c$. Thus we have the inclusion $(X \cap Y)^c \supseteq X^c \cup Y^c$. The two inclusions we have established show that the two sets are equal.

To show that (7) holds we note that $x \in (X^c)^c$ if and only if $x \notin (X^c)$ if and only if $x \in X$. □

DEFINITION 2.3. (INFORMAL) If X is a set, we denote by $|X|$, its *cardinality*, the number of elements it contains. Note that $|X| \in \mathbb{N} \cup \{\infty\}$. (The symbol ∞, *infinity*, is so far undefined.) See Definition 2.18 for a formal definition of cardinality of a set.

DEFINITION 2.4. The *(Cartesian) product* of the two sets X and Y is defined as the set of ordered pairs whose first components are from X and second, from Y:

$$X \times Y = \{(x, y); x \in X \text{ and } y \in Y\}.$$

The *difference* of two sets X and Y is defined by

$$X - Y = X \cap Y^c.$$

EXERCISES

(1) Prove (6) of Proposition 2.2.
(2) If X is a set with $n \in \mathbb{Z}_{>0}$ elements. How many elements are there in $P(X)$, the set of subsets of X.
(3) Show that $|X \times Y| = |X|\ |Y|$. Include the possibility that either or both sets are empty or contain infinitely many elements. What is the appropriate interpretation of $0 \cdot \infty$ in this context?

2. Functions

Perhaps the most important concept in mathematics is that of a function (from one set to another). The concept alone is not sufficient. We must also have good notation for it.

DEFINITION 2.5. (INFORMAL) Let X and Y be sets. A *function* (*map* or *mapping*) f from X to Y is an assignment of an element $f(x) \in Y$, to each element $x \in X$. We use the self-explanatory notation

$$f : X \to Y \text{ and } f : X \ni x \mapsto f(x) \in Y$$

to give more information on f. The set X is the *domain* of f, the set Y, its *target* or *codomain* and

$$f(X) = \{y \in Y; y = f(x) \text{ for some } x \in X\} \subseteq Y,$$

its *range* or *image*.

DEFINITION 2.6. The *graph*, $\mathrm{Gr}(f)$, of a function $f : X \to Y$ is defined by

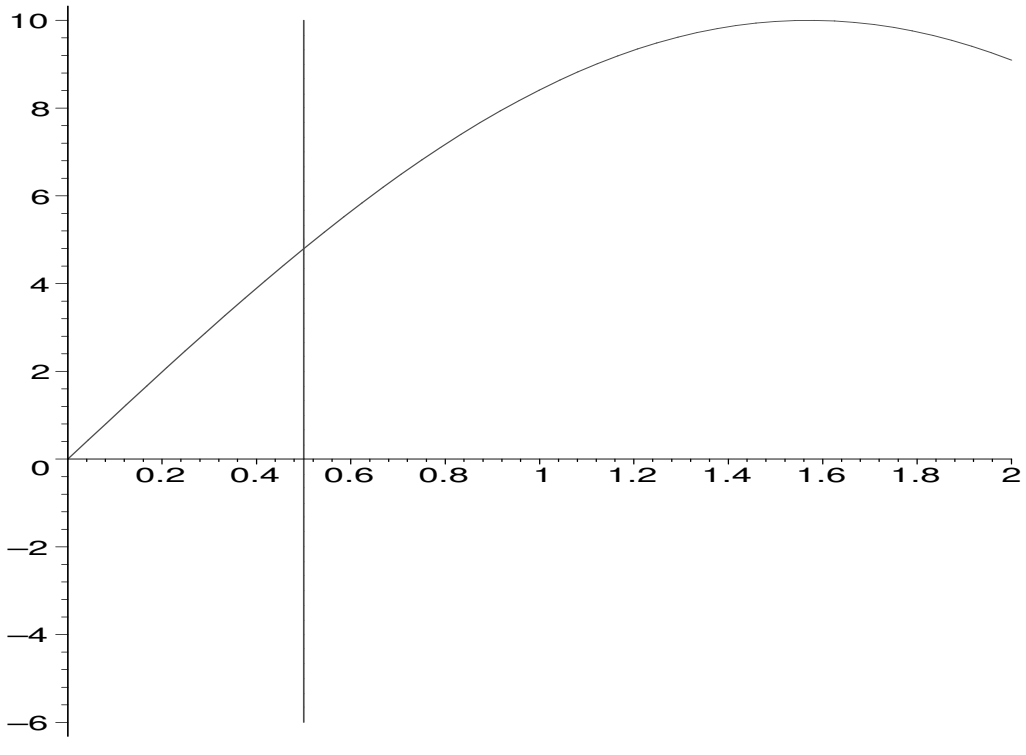
$$\mathrm{Gr}(f) = \{(x, y) \in X \times Y; y = f(x)\} \subseteq X \times Y.$$

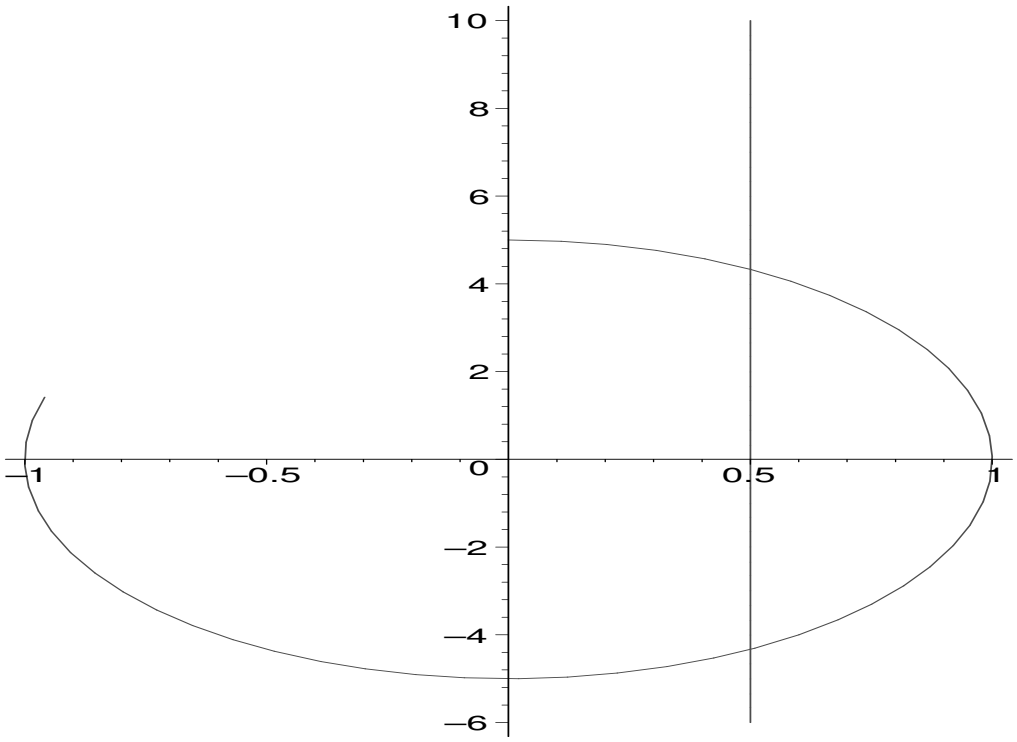
Note that for each $x \in X$, there is precisely one $y \in Y$ such that $(x, y) \in \mathrm{Gr}(f)$. Thus for a function $f : \mathbb{R} \to \mathbb{R}$, $\mathrm{Gr}(f)$ is a subset of $\mathbb{R}^2$ with some additional properties (see two examples below).

We are now ready for a formal definition of a function.

DEFINITION 2.7. Let X and Y be sets. A *function* $f : X \to Y$ is a subset $G \subseteq X \times Y$ with the properties
(1) for all $x \in X$, there exists a $y \in Y$ such that $(x, y) \in G$, and
(2) whenever (x, y_1) and $(x, y_2) \in G$, then $y_1 = y_2$.
For a given $x \in X$, the unique $y \in Y$ with $(x, y) \in G$ is denoted by $f(x)$ and called the *image* of x under f.

Thus for functions $f : I \to \mathbb{R}$ defined on an interval $I \subseteq \mathbb{R}$, the graph of f intersects any vertical line at most once. The first of the next two figures illustrates the intersection of a graph of a function with a vertical line; while in the second, the curved figure is not the graph of a function.





DEFINITION 2.8. A function $f : X \to Y$ is *injective* or *one-to-one* or an *injection* if whenever x_1 and $x_2 \in X$ with $f(x_1) = f(x_2)$, then $x_1 = x_2$. The function is *surjective* or *onto* or a *surjection* if for every $y \in Y$ there exists at least one $x \in X$ with $f(x) = y$. Finally, f is *bijective* or a *bijection* if it is both injective and surjective.

DEFINITION 2.9. Let X and Y be sets. The *identity* function on X, id_X, is the function which takes every element of X onto itself:

$$\mathrm{id}_X : X \ni x \mapsto x \in X.$$

Whenever the set X is clear from the context, we will denote id_X by id. If we choose a $c \in Y$, then the *constant* function on X, f_c, is the function which takes every element of X onto c:

$$f_c : X \ni x \mapsto c \in Y.$$

DEFINITION 2.10. Let $f : X \to Y$ and $g : Y \to Z$ be functions. We define the *composite* function or *composition*

$$g \circ f : X \in x \mapsto g(f(x)) \in Z.$$

If $f : X \to X$, the composition $f \circ f$ is also denoted by f^2 and $f^{\circ 2}$. Similarly[1], the composition of f with itself $n \in \mathbb{Z}_{\geq 0}$ times is denoted by f^n and $f^{\circ n}$. Note that $f^0 = \mathrm{id}_X$.

PROPOSITION 2.11. *If $f : X \to Y$, $g : Y \to Z$ and $h : Z \to W$ are functions, then $h \circ (g \circ f) = (h \circ g) \circ f$.*

PROOF. Both functions send $x \in X$ to $h(g(f(x))) \in W$. □

[1]Under certain circumstances (for example, if $Y = \mathbb{R}$) functions can be multiplied. In such cases f^n also stands for the n-fold product of f. The context usually makes it clear which meaning applies.

DEFINITION 2.12. Let $f : X \to Y$ be a function. A function $g : Y \to X$ is an *inverse* of f if $g \circ f = \mathrm{id}_X$ and $f \circ g = \mathrm{id}_Y$.

PROPOSITION 2.13. *The inverse function, when it exists, is unique.*

PROOF. Assume that $f : X \to Y$ has inverses $g : Y \to X$ and $h : Y \to X$. Then

$$g = g \circ \mathrm{id}_X = g \circ (f \circ h) = (g \circ f) \circ h = \mathrm{id}_X \circ h = h.$$

□

NOTATION 2.14. The inverse of the function $f : X \to Y$, when it exists, is denoted by f^{-1}.

CAUTION 2.15. If $f : X \to \mathbb{R} - \{0\}$ is a function, then the *reciprocal* function $x \mapsto \frac{1}{f(x)}$ is also denoted at times by f^{-1}. The context usually makes it clear whether the inverse or reciprocal is meant.

PROPOSITION 2.16. *A function has an inverse if and only if it is a bijection.*

PROOF. Let $f : X \to Y$ be a function. If $f^{-1} : Y \to X$ is its inverse, then for x_1 and $x_2 \in X$ with $f(x_1) = f(x_2)$ we have

$$x_1 = f^{-1}(f(x_1)) = f^{-1}(f(x_2)) = x_2.$$

Thus f is injective. For $y \in Y$, $f(f^{-1}(y)) = y$. Hence f is surjective. Conversely if f is bijective, then for each $y \in Y$, there exists a unique $x \in X$ such that $f(x) = y$. Define $f^{-1}(y) = x$. □

COROLLARY 2.17. *If $f : X \to Y$ and $g : Y \to Z$ are bijections. Then*
(i) *$g \circ f : X \to Z$ is a bijection and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$ and*
(ii) *$f^{-1} : Y \to X$ is a bijection and $(f^{-1})^{-1} = f$. Also*
(iii) *$\mathrm{id}_X : X \to X$ is a bijection and $\mathrm{id}_X^{-1} = \mathrm{id}_X$.*

PROOF. Since f and g are bijections, f^{-1} and g^{-1} exist. Let x_1 and $x_2 \in X$ and assume that $(g \circ f)(x_1) = (g \circ f)(x_2)$. Applying g^{-1} to both sides we conclude that $f(x_1) = f(x_2)$. If we now apply f^{-1} to both sides, we see that $x_1 = x_2$. Thus $g \circ f$ is injective. For this part of the proof we only need the injectivity of both f and g. The reader should rework the argument to use only this information. If $z \in Z$, then since g is surjective, there exists a $y \in Y$ such that $g(y) = z$. The surjectivity of f implies the existence of a $x \in X$ with $f(x) = y$. Thus $g(f(x)) = z$ and we conclude that $g \circ f$ is surjective. Now

$$(g \circ f) \circ \left(f^{-1} \circ g^{-1}\right) = g \circ \mathrm{id}_Y \circ g^{-1} = g \circ g^{-1} = \mathrm{id}_Z.$$

Similarly,

$$\left(f^{-1} \circ g^{-1}\right) \circ (g \circ f) = \mathrm{id}_X.$$

This establishes (i). The proofs of (ii) and (iii) are left to the reader. □

DEFINITION 2.18. We say that two sets X and Y have the *same cardinality* if there exists a bijection between them (in symbols $|X| = |Y|$). Note that we have not (yet formally) defined the cardinality $|X|$ of a set X.[2] We now define $|\emptyset| = 0$ and for all $n \in \mathbb{Z}_{>0}$, $|\{1, 2, ..., n\}| = n$. We say that a set X has *finite* cardinality ($|X| < \infty$) or X is a *finite* set, if it is either the empty set ($|X| = 0$ in this case) or in bijective correspondence with the set consisting of the

[2]Only what it means for two sets to have the same cardinality.

first n positive integers for some $n \in \mathbb{Z}_{>0}$ ($|X| = n$). Otherwise, we say that X has *infinite* cardinality and write $|X| = \infty$. Thus $|X|$ denotes the number of elements in X. We say that an infinite set is *countable* or has *countable* cardinality if it is in bijective correspondence with the set of positive integers.

PROPOSITION 2.19. *Suppose X and Y are finite sets, then*

$$|X \cup Y| + |X \cap Y| = |X| + |Y|.$$

PROOF. If either X or $Y = \emptyset$, we may assume that $Y = \emptyset$. In this case $X \cup Y = X$ and $X \cap Y = \emptyset$ and the equality of proposition is trivially true. So assume that neither X nor $Y = \emptyset$ and that $X \cap Y = \emptyset$. Assume that $|X| = n$ and $|Y| = m$. Thus there exist bijections $f : X \to \{1, 2, ..., n\}$ and $g : Y \to \{1, 2, ..., m\}$. We set up a bijection $h : X \cup Y \to \{1, 2, ..., n + m\}$, by defining

$$h(x) = \begin{cases} f(x) \text{ for } x \in X \\ g(x) + n \text{ for } x \in Y \end{cases}.$$

We use the fact that X and Y are disjoint to conclude that h is well defined (makes sense). The map h is clearly both injective and surjective. For the general case we note that that the sets X and $Y - (X \cap Y)$ are disjoint and that

$$X \cup Y = X \cup [Y - (X \cap Y)].$$

Thus

$$|X \cup Y| = |X \cup [Y - (X \cap Y)]| = |X| + |[Y - (X \cap Y)]| = |X| + |Y| - |X \cap Y|.$$

□

REMARK 2.20.
(1) The sets $\mathbb{Z}$ and $\mathbb{Q}$ are countable; so are the sets $2\mathbb{Z}$ and $\mathbb{Q}_{\geq 0}$; the sets $\mathbb{R}$ and $\mathbb{C}$ are not.
(2) A countable union of countable sets is countable.

3. Relations

Relations, our next concept, are generalizations of functions. They play a key role in algebra and almost all branches of mathematics.

DEFINITION 2.21. Let X and Y be sets. A *relation* R from X to Y is a subset of the Cartesian product $X \times Y$ ($R \subseteq X \times Y$). It is convenient to write xRy for $(x, y) \in R$. A relation from X to X is also called a relation on X (these are the most common types).

REMARK 2.22. If $f : X \to Y$ is a function, then $\mathrm{Gr}(f)$ is a relation from X to Y.

DEFINITION 2.23. Let R be a relation on a set X. We say that R is

- *reflexive* if xRx for all $x \in X$,
- *symmetric* if for all x and $y \in X$, xRy implies yRx (equivalently, if for all x and $y \in X$, xRy if and only if yRx),
- *weakly antisymmetric* if for all x and $y \in X$, xRy and yRx implies that $x = y$,
- *antisymmetric* if for all x and $y \in X$, xRy implies that $(y, x) \notin R$, and
- *transitive* if for all x, y and $z \in X$, xRy and yRz implies that xRz.

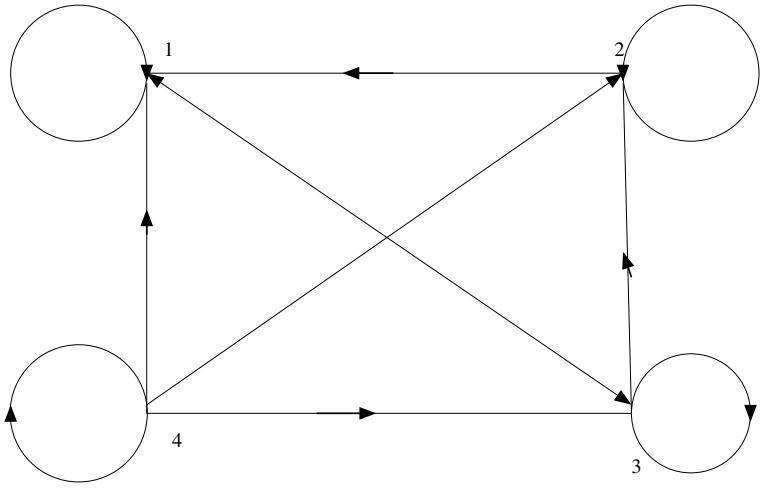
EXAMPLE 2.24. We examine certain relations on $\mathbb{Z}$.

- Equality ($=$) is reflexive, symmetric, weakly antisymmetric, not antisymmetric, and transitive.
- Greater than or equal ($\geq$) is reflexive, not symmetric, weakly antisymmetric, not antisymmetric, and transitive.
- Greater than ($\geq$) is reflexive, not symmetric, weakly antisymmetric, antisymmetric, and transitive.
- Congruence of integers modulo $n \in \mathbb{Z}_{>0}$ ($\equiv \mod n$) is reflexive, symmetric, not weakly antisymmetric, not antisymmetric, and transitive.
- Let $f : \mathbb{Z} \to \mathbb{Z}$ be a function. We define
$$R = \{(x, f(x)); x \in \mathbb{Z}\}.$$
Then R is not reflexive, not symmetric, not weakly antisymmetric, not antisymmetric, and not transitive. Nether is
$$R = \{(f(x), x); x \in \mathbb{Z}\}.$$

DEFINITION 2.25. A *graph* is a collection of points (called *vertices*) and lines (called *edges* joining some pairs of points. A *directed* graph or a *digraph* is a graph where each edge has a direction (an arrow from its *originating* vertex to its *terminating* vertex). We note that two vertices may be joined by more than one edge.

A useful way to represent pictorially a relation R on a set X is by its digraph $\Gamma(R)$ constructed as follows. The vertices of $\Gamma(R)$ are the points $x \in X$. A directed edge starts at x and ends at y if and only if xRy.

EXAMPLE 2.26. Consider the set $X_4 = \{1, 2, 3, 4\}$. We let R be the relation $\geq$. Thus
$$R = \{(1,1), (2,1), (2,2), (3,1), (3,2), (3,3), (4,1), (4,2), (4,3), (4,4)\}.$$
Its directed graph is



Another useful way to represent a relation R on a set X is by an *adjacency matrix* $M(R)$ constructed as follows. We index the rows and columns of $M(R)$ by the points $x \in X$. Each entry in $M(R)$ is either a zero or a one. We define the entry corresponding to the row indexed by x and the column indexed by y to be 1 if xRy and to be 0 if $(x, y) \notin R$.

EXAMPLE 2.27. For the relation R of the previous example

$$M(R) = \begin{array}{c|cccc} & 1 & 2 & 3 & 4 \\ \hline 1 & 1 & 0 & 0 & 0 \\ 2 & 1 & 1 & 0 & 0 \\ 3 & 1 & 1 & 1 & 0 \\ 4 & 1 & 1 & 1 & 1 \end{array}.$$

Note that in general the adjacency matrix of a relation can be infinite. For example, for the relation $=$ on $\mathbb{Z}_{\geq 0}$, the adjacency matrix is infinite symmetric with ones along the diagonal and zeros elsewhere:

$$\begin{array}{c|cccccc} & 0 & 1 & 2 & 3 & 4 & \ldots \\ \hline 0 & 1 & 0 & 0 & 0 & 0 & \ldots \\ 1 & 0 & 1 & 0 & 0 & 0 & \ldots \\ 2 & 0 & 0 & 1 & 0 & 0 & \ldots \\ 3 & 0 & 0 & 0 & 1 & 0 & \ldots \\ 4 & 0 & 0 & 0 & 0 & 1 & \ldots \\ . & & & & & & \\ . & & & & & & \\ . & & & & & & \end{array}.$$

Among the most interesting relations are those that satisfy a number of the properties of Definition 2.23. We give some of these special names.

DEFINITION 2.28. A relation R on a set X is

- a *partial order* if it is reflexive, weekly antisymmetric and transitive (we also say that X is *partially ordered* by R and that X is a *partially ordered* set),
- a *strict* partial order if it is antisymmetric and transitive, and
- an *equivalence relation* if it is reflexive, symmetric and transitive.

EXAMPLE 2.29. The relations $\leq$, $<$ and $=$ on $\mathbb{Z}$ are a partial order, a strict partial order and an equivalence relation, respectively.

DEFINITION 2.30. Let R be a strict partial order on a set X. Let x and $y \in X$. We say that y is an *immediate successor* of x (and x is an *immediate predecessor* of y) if xRy, and if for some $z \in X$, xRz and zRy, then $z = y$. If R is a partial order (perhaps not strict), we modify the above definition by requiring that $y \neq x$.

The concept of successor can be illustrated by a graph. Let R be a partial order on a set X. The *Hasse graph* $\mathcal{G}$ of R is a graph whose vertices are the points of X and if x and $y \in X$ with y is an immediate successor of x, then $\mathcal{G}$ has a directed edge from x to y.

EXAMPLE 2.31. Fix an integer $n \geq 1$. Congruence modulo n is an equivalence relation on $\mathbb{Z}$.

DEFINITION 2.32. Let X and I be nonempty sets. A *partition* of X (*indexed* by I) is a collection of subsets $\{X_i; i \in I\}$ of X such that

$$X_i \cap X_j = \emptyset \text{ if } i \neq j$$

and

$$\bigcup_{i \in I} X_i = X.$$

We call the X_i, the *blocks* of the partition.

Partitions and equivalence relations are essentially the same thing as shown by

THEOREM 2.33. *Let X be a nonempty set. If $\{X_i; i \in I\}$ is a partition of X, we define a relation R on X by xRy for x and $y \in X$ if and only if x and $y \in X_i$ for some $i \in I$. This relation is an equivalence.*

PROOF. It is of course obvious that R defines a relation on X. Let $x \in X$. Since xRx, R is reflexive. If x and $y \in X$ and xRy, then x and y are in the same block of the partition. So yRx and R is symmetric. Now let us take x, y and $z \in X$ with xRy and yRz. Thus x and y are in the same block and y and z are in the same block. We conclude that x and z are in the same block and thus xRz; that is, R is transitive. □

We outline the proof of the converse to the above theorem. Let E be an equivalence relation on X. For each $x \in X$, we form the set

$$E_x = \{y \in X; xEy\}.$$

The collection of subsets of X,

$$\mathbb{V} = \{E_x; x \in X\}$$

contains many equal elements. We remove from $\mathbb{V}$ all but one copy of every collection of equal elements in this set. The remaining sets in $\mathbb{V}$ are the blocks of a partition of X. An $x \in X$ belongs to E_x and since $E_x \in \mathbb{V}$, the union of the sets in $\mathbb{V}$ is all of X. Let x and $z \in X$ and assume that $E_x \cap E_z$ contains an element $y \in X$. Thus xEy and yEz and hence also xEz. But this means that $z \in E_x$. Next, if $w \in E_z$, then wEz. Thus also wEx and $w \in E_z$. We have shown that $E_z \subseteq E_x$. By symmetry, also $E_x \subseteq E_z$ and thus $E_x = E_z$. So the blocks are disjoint.

4. Order relations on $\mathbb{Z}$ and $\mathbb{Q}$

4.1. Orders on $\mathbb{Z}$. Using elementary set theory one constructs the natural numbers $\mathbb{N}$. From $\mathbb{N}$ one proceeds to the construcion of the integers $\mathbb{Z}$ (as the disjoint union of $\mathbb{N}$ and $\mathbb{N} - \{0\}$) and its binary operations of *addition* $+$ and *multiplication* $\cdot$; resulting in the *commutative ring* $(\mathbb{Z}, +, \cdot)$. In this section, as an illustration, we describe one relation on $\mathbb{Z}$.

The most basic relation on $\mathbb{Z}$ is that of equality $(=)$. It is an equivalence relation and it partitions $\mathbb{Z}$ into subsets consisting of single elements.

We turn to a study of a second most important relation on $\mathbb{Z}$.

DEFINITION 2.34. Let a and $b \in \mathbb{Z}$. We say that b is *greater than or equal to* a (in symbols $b \geq a$) if and only if $b - a \in \mathbb{N}$.

As noted earlier $\geq$ is reflexive ($a \geq a$ for all $a \in \mathbb{Z}$ since $a - a = 0 \in \mathbb{N}$), weekly antisymetric (if $a \geq b$ and $b \geq a$, then $a - b$ and $b - a \in \mathbb{N}$ which implies that $a - b = 0$) and transitive (if $a \geq b$ and $b \geq c$, then $a - b$ and $b - c \in \mathbb{N}$ which tells us that also that $a - c \in \mathbb{N}$).

An integer is *positive* if it belongs to $\mathbb{N} - \{0\}$ and *negative* if it does not belong to $\mathbb{N}$. The set of positive integers is closed under addition and multiplication; the set of negative integer under addition, but not multiplication. If a and $b \in \mathbb{Z}$ and c is a positve integer, then the *cancelation property*

$$b \geq a \text{ iff } bc \geq ac$$

holds. All the above properties (propositions) require, of course, formal proofs.

4.2. Orders on $\mathbb{Q}$. Recall that a rational $\frac{a}{b}$ (here $a \in \mathbb{Z}$ and $b \in \mathbb{Z}_{>0}$) is an equivalence class of pairs of integers.

DEFINITION 2.35. Let $\frac{a}{b}$ and $\frac{c}{d}$ be rational numbers. We say that $\frac{c}{d}$ is *greater than or equal to* $\frac{a}{b}$ (in symbols $\frac{c}{d} \geq \frac{a}{b}$) if and only if $cb \geq ad$.

A first task is to show that the concept of $\geq$ is well defined on $\mathbb{Q}$. So assume that $\frac{a}{b} = \frac{a'}{b'}$ and $\frac{c}{d} = \frac{c'}{d'}$. We have to show here that $cb \geq ad$ if and only if $c'b' \geq a'd'$. The definition of rational numbers tells us that $ab' = ba'$ and $cd' = dc'$. Using the last two equalities and the cancelation law, we conclude that

$$cb \geq ad \text{ iff } cbb' \geq adb' = ba'd$$

$$\text{iff } cb' \geq a'd \text{ iff } dc'b' = cb'd' \geq a'dd' \text{ iff } c'b' \geq a'd'.$$

5. The complex numbers

Mostly as a source for examples, we study[3] the complex numbers $(\mathbb{C}, +, \cdot)$ under the operations of addition and multiplication. This number system shares many, but not all, of the properties of the real numbers $(\mathbb{R}, +, \cdot)$. Missing is the *canonical* ordering (in general one studies $(\mathbb{R}, +, \cdot, \geq)$ rather than just $(\mathbb{R}, +, \cdot)$). The complex numbers satisfy all the rules of addition and multiplication satisfied by the real numbers (in the language discussed in §1 of Chapter 5, they form a field) To construct $\mathbb{C}$ we start withth $\mathbb{R}$ and introduce a new symbol $\imath$ that satisfies

$$\imath^2 = -1.$$

We can view $\mathbb{C}$ as consisting of numbers of the form $c = a + b\imath$, with a and $b \in \mathbb{R}$. Addition of such numbers is vector (component) sum; thus

$$(a_1 + b_1\imath) + (a_2 + b_2\imath) = (a_1 + a_2) + (b_1 + b_2)\imath.$$

It agrees with vector addition in $\mathbb{R}^2$ if we identify the complex numbers $\mathbb{C}$ with the Cartesian plane $\mathbb{R}^2$. In this identification we use 1 and $\imath$ as a basis for $\mathbb{C}$ over $\mathbb{R}$ that corresponds to the usual basis $(1, 0)$ and $(0, 1)$ for $\mathbb{R}^2$. Multiplication seems a bit more complicated:

$$(a_1 + b_1\imath)(a_2 + b_2\imath) = (a_1a_2 - b_1b_2) + (a_1b_2 + a_2b_1)\imath.$$

The *multiplicative inverse* or *reciprocal* of non-zero complex number is again a complex number; to describe it, it is convenient to first introduce the *conjugate* $\bar{c}$ of the complex number $a + b\imath$ as

$$\bar{c} = a - b\imath$$

and the *absolute value* or *modulus* $|c|$ of c as

$$|c| = \sqrt{a^2 + b^2} = \sqrt{c\bar{c}}.$$

With these preliminaries out of the way, the reciprocal of the complex number $0 \neq c = a + b\imath$ is easily seen to be

$$\frac{1}{a + b\imath} = \frac{1}{a + b\imath}\frac{a - b\imath}{a - b\imath} = \frac{a - b\imath}{a^2 + b^2} = \frac{\bar{c}}{|c|^2}.$$

[3]Presumably, a review for most readers.

Using the last formula it is easy to compute $\frac{a_1+b_1\imath}{a_2+b_2\imath}$ (we must, of course, assume that $a_2+b_2\imath \neq 0$).

Let us identify the complex number $c = a + b\imath \in \mathbb{C}$ (remember that here both a and $b \in \mathbb{R}$) with the point in the Cartesian plane $(a, b) \in \mathbb{R}^2$. Thus we think of c as a directed line segment from the origin in $\mathbb{R}^2$ to the point $(a, b) \in \mathbb{R}^2$; an arrow (direction). For graphic representations, there is nothing magic about starting at 0. The same vector is obtained by moving the arrow (while preserving its length and direction) to start at any point in the Cartesian plane. The graphic interpretation of complex addition (addition of vectors) is now easily illustrated (see Figure 1).

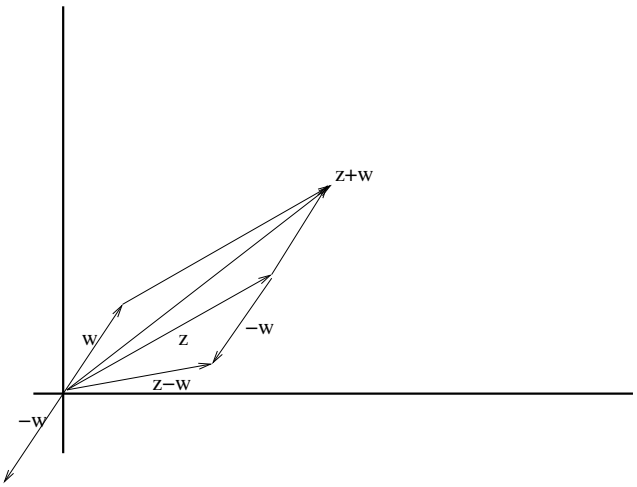


FIGURE 1. **Addition of complex numbers.**

To add the points z and $w \in \mathbb{C}$, we represent them as directed line segments starting at the origin in $\mathbb{R}^2$. We then move the arrow corresponding to w to start at the end point of z. The arrow from the origin to the end point of the transported w now represents the sum $z + w$. We can also transport z to start at the end point of w. We thus form a closed parallelogram; its main diagonal (the one starting at 0) represents $z + w$; its other diagonal (from w to z) transported to 0 represents $z - w$. We have used rectangular coordinates on $\mathbb{R}^2$ for a geometric interpretation of complex addition.

Polar coordinates are useful to obtain a geometric interpretation of complex multiplication. If we represent, the non-zero complex number $c = a + b\imath$ as the point $(a, b) \in \mathbb{R}^2$, then we can associate with it two other real numbers $r = \sqrt{a^2 + b^2} = |c|$ (note that r, the absolute value of the non-zero complex number c is positive) and $\theta = \arcsin \frac{b}{r} = \arccos \frac{a}{r}$. The two equations defining θ specify it uniquely up to an ambiguity of the form $2\pi n$ with $n \in \mathbb{Z}$. (Note that either single equation would involve a "bigger" ambiguity.) We call θ, the *argument* of the complex number c. For $\theta \in \mathbb{R}$, it is convenient to denote the complex number of absolute value 1, $\cos\theta + \imath \sin\theta$, by the symbol $e^{\imath\theta}$. With this convention, the complex number c is represented in *polar coordinates* as

$$c = re^{\imath\theta}.$$

Note that $e^{\imath 0} = 1$ and that we may view the number $c = re^{\imath\theta}$ as the product of 1 and c; this product is obtained by multiplying their moduli and adding their arguments.

In general multiplication of a vector z by the vector c moves the vector z in the counter-clockwise direction through an angle θ and adjusts the length of the resulting vector. Thus, geometrically, the vector (in $\mathbb{R}^2$) corresponding to the product of the non-zero complex numbers $c_1 = r_1 e^{\imath\alpha_1}$ and $c_2 = r_2 e^{\imath\alpha_2}$ is a vector of length $r_1 r_2$ with argument $\alpha_1 + \alpha_2$.

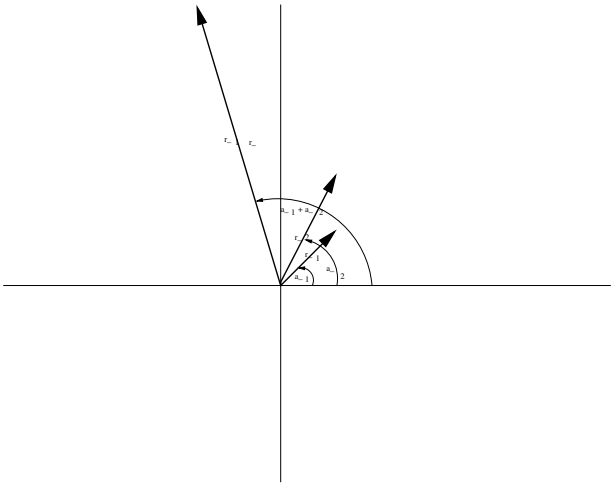


FIGURE 2. **Multiplication of complex numbers.**

From the geometric interpretation of multiplication we see that for all θ and $\varphi \in \mathbb{R}$,

$$e^{\imath\theta} e^{\imath\varphi} = e^{\imath(\theta+\varphi)}.$$

We now transform the last equation to rectangular coordinates:

$$(\cos\theta + \imath \sin\theta)(\cos\varphi + \imath \sin\varphi) = \cos(\theta + \varphi) + \imath \sin(\theta + \varphi).$$

Equating the respective real and imaginary parts of the complex numbers involved, we obtain the angle addition formulae

$$\cos\theta \cos\varphi - \sin\theta \sin\varphi = \cos(\theta + \varphi)$$

and

$$\cos\theta \sin\varphi + \sin\theta \cos\varphi = \sin(\theta + \varphi).$$

Many other identities can be similarly derived.

REMARK 2.36. The complex numbers are complete in the sense of analysis (every Cauchy sequence converges), and as we shall see later, in the algebraic sense (every polynomial over $\mathbb{C}$ has a root).

CHAPTER 3

Groups

In this chapter we introduce, mostly through examples, the most basic algebraic structures; that of a group. We have already encountered several families of groups:

(1) $(\mathbb{Z},\ +)$, $(\mathbb{Q},\ +)$, $(\mathbb{R},\ +)$ and $(\mathbb{C},\ +)$.
(2) $(\{\pm 1\},\ \cdot)$, $(\mathbb{Q}^*,\ \cdot)$, $(\mathbb{R}^*,\ \cdot)$ and $(\mathbb{C}^*,\ \cdot)$, where R^* denotes the set of elements in R that are invertible with respect the mutiplication (usually, but not always, the non-zero elements in R).
(3) $(\mathbb{Z}_n,\ +)$, $n \in \mathbb{Z}_{>0}$.
(4) $(\mathbb{Z}_n^*,\ \cdot)$, $n \in \mathbb{Z}_{>0}$.

The first two sections of the chapter are devoted to the study of one new family of groups, the *permutation groups*. In a sense to be made precise later (in Chapter 4, Section 6.1), all of group theory consists of a study of this family. A main difference between permutation groups and those previously considered groups is that, in general, the product of two permutations do not commute. In the third and final section of the chapter, we formally define the concept of a group and study more examples.

1. Permutation groups

This section is devoted to the study of the most basic operations on sets (mostly finite sets) and their self-maps that lead us very naturally to the concept of a group.

Definition 3.1. Let X be a nonempty set. A *permutation* of X is a bijection from X to itself. We will denote the set of permutations of X by the symbol $\mathrm{Perm}(X)$.

The case of finite X is of most interest. In this case it is convenient to use for X the set X_n consisting of the first n positive integers (we assume throughout that $n \geq 2$)[1]:

$$X_n = \{1, 2, ..., n\}.$$

In this case[2], we use the symbol $S(n)$ for $\mathrm{Perm}(X_n)$ equipped with the operation of composition of functions (which we regard as a *multiplication* on $S(n)$) and call $S(n)$, the *symmetric group*[3] on n symbols (letters or elements).

An element $\pi \in S(n)$ sends the integer $j \in X_n$ to the integer $\pi(j) \in X_n$. A good way to *represent* such a permutation is by a matrix consisting of two rows. The first row lists the

[1]Because the case $n = 1$ is completely trivial.

[2]Also for the case $n = 1$. Of course, $S(1)$ consists of only one element.

[3]We will subsequently define the concept of (abstract) group. Of course, these will be prime examples of the concept.

integers in X_n: $1, 2, ..., n$, in any convenient order, and in the second row, the entry under j is $\pi(j)$:

$$\pi = \begin{pmatrix} 1 & 2 & ... & n \\ \pi(1) & \pi(2) & ... & \pi(n) \end{pmatrix}.$$

THEOREM 3.2. *Fix a positive integer n.*

- *If π and $\sigma \in S(n)$, then so is their composite $\pi \circ \sigma$ which we denote as $\pi\sigma$.*
- *The identity self map of X_n, denoted by* id *or* id_{X_n} *is an element of $S(n)$.*
- *If $\pi \in S(n)$, then so does π^{-1}.*
- $|S(n)| = n!$

PROOF. Only the last statement needs to be verified. To construct a permutation $\pi \in S(n)$, we may send the integer 1 to any of n integers, the integer 2 to any of the remaining $n-1$ integers, etc ... □

EXAMPLE 3.3. We illustrate most of the concepts using examples for $n = 10$. Let

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 4 & 5 & 6 & 7 & 2 & 9 & 10 & 1 & 8 \end{pmatrix}$$

and

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1 & 3 & 4 & 2 & 6 & 7 & 8 & 9 & 10 & 5 \end{pmatrix}.$$

Then

$$\sigma\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 2 & 6 & 7 & 8 & 3 & 10 & 5 & 1 & 9 \end{pmatrix}.$$

Remember that we are composing permutations as functions, thus for two permutations σ and π, $(\sigma\pi)(j) = \sigma(\pi(j))$. We obtain a convenient way to multiply permutations, by realizing that reordering the columns of a given representation of a permutation does not change the permutation. Thus we may use the order of the second row of π to determine the first row of σ to obtain

$$\begin{matrix} \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 4 & 5 & 6 & 7 & 2 & 9 & 10 & 1 & 8 \end{pmatrix} \\ \sigma = \begin{pmatrix} 3 & 4 & 5 & 6 & 7 & 2 & 9 & 10 & 1 & 8 \\ 4 & 2 & 6 & 7 & 8 & 3 & 10 & 5 & 1 & 9 \end{pmatrix} \end{matrix};$$

the representation of $\sigma\pi$ is now easily read-off; it consists of the first and fourth lines of the last array (note in the above "algorithm," we write down first the permutation for the rightmost map (the one we do first). Using the reordering idea, we obtain the representation of π^{-1} from the one for π by interchanging its two rows. Note that

$$\pi\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 5 & 6 & 4 & 2 & 9 & 10 & 1 & 8 & 7 \end{pmatrix} \neq \sigma\pi.$$

The last example showed that the multiplication on $S(n)$ is not commutative. Note that in order to show that two elements σ and $\pi \in S(n)$ do not commute, it is not necessary to compute $\pi\sigma$ and $\sigma\pi$. All we need to do is to find one $j \in X_n$ for which $\pi\sigma(j) \neq \sigma\pi(j)$. In our example, there are many such j; in particular, $3 = \pi\sigma(1) \neq \sigma\pi(1) = 4$.

We note that our way of representing permutations is still rather cumbersome. A more detailed study of $S(n)$ will also suggest better ways to represent elements of this group.

DEFINITION 3.4. Let us introduce the convention that whenever the integer $n+1$ appears, it is replaced[4] by 1. A permutation $\pi \in S(n)$ is *cyclic* if there is a rearrangement $x_1, x_2, ..., x_r, x_{r+1}, ..., x_n$ of the integers $1, 2, ..., n$ such that π *fixes* $x_{r+1}, ..., x_n$ (that is, $\pi(x_j) = x_j$ for $j = r+1, ..., n$) and *cycles* $x_1, x_2, ..., x_r$ (that is, $\pi(x_i) = x_{i+1}$ for $i = 1, ..., r-1$ and $\pi(x_r) = x_1$). The integer r is called the *length* of the cycle, in symbols $l(\pi)$, and π is called an *r-cycle*. A 2-cycle is called a *transposition*.

NOTATION 3.5. *The cycle defined above is conveniently represented by*

$$\pi = (x_1, x_2, ..., x_r).$$

Note that the fixed points $x_{r+1}, ..., x_n$ of the cycle do not appear at all in its new symbol. Whenever appropriate, we will use the symbol $(\cdot)$ to denote the identity cycle. Since cycles are special cases of permutations, we can multiply them. Note that in the product

$$(x_1, x_2, ..., x_r)(y_1, y_2, ..., y_s)$$

we first perform the second permuatation; thus

$$(1,2,4,5)(1,3,6) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 4 & 6 & 5 & 1 & 2 & 7 & 8 & 9 & 10 \end{pmatrix}.$$

We read products of cycles from right to left, but each cycle from left to right.

DEFINITION 3.6. Let $\pi \in S(n)$. We say that π *moves* j ($j \in \mathbb{Z}$, $1 \leq j \leq n$) if $\pi(j) \neq j$. Let π and $\sigma \in S(n)$. We say that π and σ are *disjoint* if every integer moved by π is fixed by σ and every integer moved by σ is fixed by π.

LEMMA 3.7. *Let $\pi \in S(n)$. If $j \in \mathbb{Z}$, $1 \leq j \leq n$, is moved by π, then so are $\pi(j)$ and $\pi^{-1}(j)$.*

PROOF. If $\pi(j)$ is not moved by π, then $\pi(\pi(j)) = \pi(j)$ and applying π^{-1} to both sides of this equation, we get the contradiction that $\pi(j) = j$. If $\pi^{-1}(j)$ is not moved by π, then $j = \pi(\pi^{-1}(j)) = \pi^{-1}(j)$ and applying π to the extreme terms of this equation, we get once again the contradiction that $\pi(j) = j$. □

THEOREM 3.8. *If π and $\sigma \in S(n)$ are disjoint, then they commute.*

PROOF. Let $j \in \mathbb{Z}$, $1 \leq j \leq n$. There are three possibilities:

- Either j is moved by π and hence j and $\pi(j)$ are fixed by σ (By definition j is fixed by σ). If j is moved by π, then so is $\pi(j)$ by the last lemma and hence the disjointness of π and σ gurantees that $\pi(j)$ is fixed by σ.).
- Or j is moved by σ and hence j and $\sigma(j)$ are fixed by π.
- Or j is fixed by both π and σ.

In the first case

$$\pi(\sigma(j)) = \pi(j) = \sigma(\pi(j)),$$

in the second,

$$\pi(\sigma(j)) = \sigma(j) = \sigma(\pi(j)),$$

and in the third

$$\pi(\sigma(j)) = j = \sigma(\pi(j)).$$

[4]We are thus using arithmetic modulo n; however we modified the standard representation of equivalence classes in one case only. The equivalence class $[0]_n$ is represented by n instead of 0.

Thus in all cases, $\pi(\sigma(j)) = \sigma(\pi(j))$. □

EXAMPLE 3.9. Non-disjoint cycles need not commute. This already happens for $n = 3$ since $(1,2)(1,3) = (1,3,2)$ while $(1,3)(1,2) = (1,2,3)$. We can, of course, view this example as taking place in $S(10)$.

EXAMPLE 3.10. Consider our Example 3.3. To represent π by disjoint cycles, we start with $j = 1$ and follow it around under the action of π. Note that

$$\pi(1) = 3,\ \pi^2(1) = \pi(3) = 5,\ \pi^3(1) = \pi(5) = 7,\ \pi^4(1) = \pi(7) = 9 \text{ and } \pi^5(1) = \pi(9) = 1.$$

Thus this part of π is represented by the cycle $(1,3,5,7,9)$. We note that 2 does not appear in this cycle. So we now start with $j = 2$ and follow it around under the action of π:

$$\pi(2) = 4,\ \pi^2(2) = \pi(4) = 6 \text{ and } \pi^3(2) = \pi(6) = 2.$$

Thus this part of π is represented by the cycle $(2,4,6)$ and the first two parts of the transformation are represented by the product $(1,3,5,7,9)(2,4,6)$ (we could have reversed the order). Note that 8 and 10 do not appear in the last product. Continuing the process one more step, we see that

$$\pi = (1,3,5,7,9)(2,4,6)(8,10).$$

In the above steps we tacitly assumed that $\pi \in S(10)$. The same representation holds for $\pi \in S(n)$ with $n > 10$ provided we view the permutation π as fixing each integer j with $11 \leq j \leq n$. In decomposing π into a product of disjoint cycles, the order does not matter. Thus also

$$\pi = (1,3,5,7,9)(8,10)(2,4,6) = (8,10)(2,4,6)(1,3,5,7,9),$$

are among the 6 possible ways of writing π as a product of disjoint cycles.

It is not at all surprising that the above construction is quite general. We indeed have

THEOREM 3.11. *Every $\pi \in S(n)$ can be written as a product, perhaps the empty product, of disjoint cycles. This decomposition into cycles is unique up to order.*

PROOF. If π is the identity, it is represented by the empty product. Otherwise π does not fix every integer. Ignore the integers fixed by π; they do not contribute to any nontrivial cycle. More precisely we remove these integers from the first and second row of the matrix representation of the permutation π. We now have a permutation π_o of a subset of the integers 1, 2, ..., n. Start (what we call *the process*) with the smallest integer k_1 in the domain of this transformation, it is the smallest integer not fixed by π, and follow k_1 around through π or π_o to obtain a set of integers k_1, k_2, ..., such that $\pi(k_i) = k_{i+1}$. We stop this process as soon as we get a repetition in the set k_1, k_2, ..., k_{r+1}. We must get a repetition since for all i, $1 \leq k_i \leq n$. Note that $r > 1$. We claim that $k_{r+1} = k_1$. If $k_{r+1} = k_s$ with $1 < s \leq r$, then

$$\pi(k_{s-1}) = k_s = k_{r+1} = \pi(k_r),$$

and applying π^{-1} to extreme sides of the last displayed equation we get $k_{s-1} = k_r$; contradicting the minimality of $r + 1$. Hence we have

$$\pi(k_1) = k_2,\ \pi(k_2) = k_3,\ ...,\ \pi(k_{r-1}) = k_r,\ \pi(k_r) = k_1$$

for some integer r, $2 \leq r \leq n$, where the collection $k_1, k_2, ..., k_r$ consists of distinct integers. Thus this part of the permutation π is represented by the cycle $(k_1, k_2, ..., k_r)$. Add this new cycle constructed (either on the left or right) to the ones previously constructed. Remove the

integers in this cycle from the matrix representation of π_o. If we have obtained the empty set, we are done. Otherwise, call this new permutation π_0 and repeat the process on it. It is clear that we will eventually stop. This yields the desired decomposition; the uniqueness of the decomposition up to order is obvious from the construction. □

We illustrate with an example.

EXAMPLE 3.12. We simplify the product

$$\pi = (1,4,5,6)(1,7,3)(2,5,4)(2,3).$$

The integers 8, 9 and 10 do not appear in the above product; they are fixed by π. It is easiest if we work with an alternate representation of the permutation. We readily compute

$$\pi = \begin{pmatrix} 2 & 3 & 5 & 4 & 6 & 1 & 7 \\ 4 & 6 & 5 & 2 & 1 & 7 & 3 \end{pmatrix};$$

from which it follows rather quickly that

$$\pi = (2,4)(1,7,3,6).$$

As a result of the last theorem, we can easily construct the multiplication table for $S(n)$, as long as n is not too large. It is an $n \times n$ matrix (ignoring headers) where we index the rows by $x \in S(n)$ and the columns by $y \in S(n)$. The (x, y) entry in the matrix is then the product of the permutations x and y (in this order; that is, xy). For small n, the calculation can be done by hand. We illustrate with the

MULTIPLICATION TABLE FOR $S(3)$.

	$(\cdot)$	$(1,2)$	$(1,3)$	$(2,3)$	$(1,2,3)$	$(1,3,2)$
$(\cdot)$	$(\cdot)$	$(1,2)$	$(1,3)$	$(2,3)$	$(1,2,3)$	$(1,3,2)$
$(1,2)$	$(1,2)$	$(\cdot)$	$(1,3,2)$	$(1,2,3)$	$(2,3)$	$(1,3)$
$(1,3)$	$(1,3)$	$(1,2,3)$	$(\cdot)$	$(1,3,2)$	$(1,2)$	$(2,3)$
$(2,3)$	$(2,3)$	$(1,3,2)$	$(1,2,3)$	$(\cdot)$	$(1,3)$	$(1,2)$
$(1,2,3)$	$(1,2,3)$	$(1,3)$	$(2,3)$	$(1,2)$	$(1,3,2)$	$(\cdot)$
$(1,3,2)$	$(1,3,2)$	$(2,3)$	$(1,2)$	$(1,3)$	$(\cdot)$	$(1,2,3)$

It is quite tedious to produce by hand the multiplication table for $S(n)$ even with relatively small n. For example, for $n = 5$, the multiplication table is a 120×120 matrix. Computers can, once again, help. We illustrate with a program that computes the multiplication table for $S(3)$ as a check on our work and then computes the multiplication table for a subset of $S(n)$, $n \geq 4$ consisting of 8 permutations.

MAPLE SESSION #9

```
> with(group):
> f(1) := [[1]]:  f(2) := [[1,2]]:  f(3) := [[1,3]]:  f(4) := [[2,3]]:
  f(5) := [[1,2,3]]:  f(6) := [[1,3,2]]:
> a := array(1..6,1..6):
> for i to 6 do for j to 6 do a[i,j] := mulperms(f(j),f(i)) end do end
  do;
```

```
> print(a);
```

$$\begin{bmatrix} [] & [[1,2]] & [[1,3]] & [[2,3]] & [[1,2,3]] & [[1,3,2]] \\ [[1,2]] & [] & [[1,3,2]] & [[1,2,3]] & [[2,3]] & [[1,3]] \\ [[1,3]] & [[1,2,3]] & [] & [[1,3,2]] & [[1,2]] & [[2,3]] \\ [[2,3]] & [[1,3,2]] & [[1,2,3]] & [] & [[1,3]] & [[1,2]] \\ [[1,2,3]] & [[1,3]] & [[2,3]] & [[1,2]] & [[1,3,2]] & [] \\ [[1,3,2]] & [[2,3]] & [[1,2]] & [[1,3]] & [] & [[1,2,3]] \end{bmatrix}$$

```
> g(1) := [[1]]:  g(2) := [[1,2,3,4]]:  g(3) := mulperms(g(2), g(2)):
  g(4) := mulperms(g(2), g(3)):  g(5) :=[[3,4],[1,2]]:  g(6) :=
  mulperms(g(2), g(5)):  g(7) := mulperms(g(3), g(5)):  g(8) :=
  mulperms(g(4), g(5)):

> b := array(1..8,1..8):

> for i to 8 do for j to 8 do b[i,j] := mulperms(g(j),g(i)) end do end
  do;

> print(b);
```

$$\begin{bmatrix} [] & [[1,2,3,4]] & [[1,3],[2,4]] & [[1,4,3,2]] & [[1,2],[3,4]] & [[2,4]] & [[1,4],[2,3]] & [[1,3]] \\ [[1,2,3,4]] & [[1,3],[2,4]] & [[1,4,3,2]] & [] & [[1,3]] & [[1,2],[3,4]] & [[2,4]] & [[1,4],[2,3]] \\ [[1,3],[2,4]] & [[1,4,3,2]] & [] & [[1,2,3,4]] & [[1,4],[2,3]] & [[1,3]] & [[1,2],[3,4]] & [[2,4]] \\ [[1,4,3,2]] & [] & [[1,2,3,4]] & [[1,3],[2,4]] & [[2,4]] & [[1,4],[2,3]] & [[1,3]] & [[1,2],[3,4]] \\ [[1,2],[3,4]] & [[2,4]] & [[1,4],[2,3]] & [[1,\ 3]] & [] & [[1,2,3,4]] & [[1,3],[2,4]] & [[1,4,3,2]] \\ [[2,4]] & [[1,4],[2,3]] & [[1,3]] & [[1,2],[3,4]] & [[1,4,3,2]] & [] & [[1,2,3,4]] & [[1,3],[2,4]] \\ [[1,4],[2,3]] & [[1,3]] & [[1,2],[3,\ 4]] & [[2,\ 4]] & [[1,3],[2,4]] & [[1,4,3,2]] & [] & [[1,2,3,4]] \\ [[1,3]] & [[1,2],[3,4]] & [[2,4]] & [[1,4],[2,\ 3]] & [[1,2,3,4]] & [[1,3],[2,4]] & [[1,4,3,2]] & [] \end{bmatrix}$$

END OF PROGRAM

(1) MAPLE denotes the identity permutation by `[]` and the cycle (a, b, c) by `[[a,b,c]]`.
(2) The MAPLE command `multperms(a,b)` for the product of the permutations a and b computes the product ba; that is, MAPLE reads products from left to right – not the way we have been doing.

EXERCISES

(1) In the proof of Theorem 3.8 the case "j is moved by both π and σ" does not occur. Explain why.
(2) What are necessarry and sufficient c0nditions for two distinct transpositions to commute?
(3) Let n be an integer ≥ 2.
   - Let σ be a permutation in $S(n)$. Show that
   $$\sigma(1,2)\sigma^{-1} = (\sigma(1), \sigma(2)).$$
   - Let $1 \leq k \leq n$ and let
   $$\tau = (1,\ 2,\ \ldots\ n).$$
   Show that
   $$\tau^k(1,2)\tau^{-k} = (k+1, k+2).$$
   How should you interpret $n+1$ and/or $n+2$ if they appear in the last equation?

- Let $1 \leq a < b \leq n$. Show that

$$(a,b) = (a+1,a)(a,a-1)...(b-2,b-3)(b-1,b-2)(b-1,b)...(a+1,a+2)(a,a+1).$$

- Conclude that that any $\sigma \in S(n)$ can be written as product of powers of τ and $(1,2)$.

2. The order and sign of a permutation

For this section, we fix once and for all a positive integer n.

DEFINITION 3.13. Let $\pi \in S(n)$. To define the powers π^k of π, we set $\pi^0 = \mathrm{id}$ and $\pi^1 = \pi$. For $k \in \mathbb{Z}_{>0}$, we define inductively $\pi^k = \pi\pi^{k-1}$. We also define $\pi^{-k} = (\pi^{-1})^k$. Note that in the left hand side of the last equality, π^{-1} represents the minus one power of π; while in right hand side, it represents the inverse of π. The same symbol is used for these two objects because they define the same permutation.

PROPOSITION 3.14. *Let π and $\sigma \in S(n)$ and r and $s \in \mathbb{Z}$. Then*

(1) $\pi^r\pi^s = \pi^{r+s}$,
(2) $(\pi^r)^s = \pi^{rs}$,
(3) $\pi^{-r} = (\pi^r)^{-1}$,
(4) *if π and σ commute, then $\pi\sigma^r = \sigma^r\pi$, and*
(5) *if π and σ commute, then $(\pi\sigma)^r = \pi^r\sigma^r$.*

PROOF. We prove only the first and last two assertions, leaving the proofs of the other two to the reader. To establish the first claim we fix s. We now prove the assertion for $r \geq 0$ by induction. The base case $r = 0$ is trivial. We assume the formula for $r \geq 0$ and prove it for $r+1$. Now,

$$\pi^{r+1}\pi^s = \pi\pi^r\pi^s = \pi\pi^{r+s} = \pi^{1+r+s};$$

the first equality uses the definition of the $r+1$ power of π; the second, the induction step; and the third, the definition once again. We have established (1) for all $s \in \mathbb{Z}$ and all $r \in \mathbb{Z}_{\geq 0}$. So, by symmetry, we know that (1) holds if either r or s is non-negative. The reader should at this pont establish (3) which is needed for continuing with the proof of (1). If both r and s are negative, then

$$\pi^r\pi^s = \left(\pi^{-r}\right)^{-1}\left(\pi^{-s}\right)^{-1} = \left(\pi^{-s}\pi^{-r}\right)^{-1} = \left(\pi^{-s-r}\right)^{-1} = \pi^{s+r}.$$

This finishes the proof of (1). We show that (4) holds for $r \geq 0$ by induction on r. The base case, $r = 0$, is a tautology. Assume (4) for $r \geq 0$. Then

$$\pi\sigma^{r+1} = \pi\sigma^r\sigma = \sigma^r\pi\sigma = \sigma^r\sigma\pi = \sigma^{r+1}\pi.$$

To prove (4) for negative r, we first obseve that if $\pi\sigma = \sigma\pi$, then pre-multiplying and post-multiplying both sides by σ^{-1}, we get $\sigma^{-1}\pi = \pi\sigma^{-1}$; that is, if π and σ commute so do π and σ^{-1} (thus also π^{-1} and σ, as will be needed in the next displayed set of equations). Hence for negative r,

$$\pi\sigma^r = \pi(\sigma^{-r})^{-1} = (\sigma^{-r}\pi^{-1})^{-1} = (\pi^{-1}\sigma^{-r})^{-1} = \sigma^r\pi.$$

We establish (5) for non-negative r by induction. The base case. $r = 0$, is again obviously true. So assume that the formula holds for $r \geq 0$. Then

$$(\pi\sigma)^{r+1} = (\pi\sigma)^r\pi\sigma = \pi^r\sigma^r\sigma\pi = \pi^r\sigma^{r+1}\pi = \pi^r\pi\sigma^{r+1} = \pi^{r+1}\sigma^{r+1}.$$

If r is negative, then

$$(\pi\sigma)^r = \left((\pi\sigma)^{-r}\right)^{-1} = \left(\pi^{-r}\sigma^{-r}\right)^{-1} = \sigma^r\pi^r = \pi^r\sigma^r.$$

□

PROPOSITION 3.15. *Let $\pi \in S(n)$. There exists an $m \in \mathbb{Z}_{\geq 1}$ such that $\pi^m = \mathrm{id}$.*

PROOF. The group $S(n)$ has $n!$ elements. The successive powers $\pi, \pi^2, \pi^3, ...$, all belong to $S(n)$. Hence there must exist positive integers $r < s$ such that $\pi^r = \pi^s$. Multiplying both sides by π^{-r} shows that $\mathrm{id} = \pi^{s-r}$. □

DEFINITION 3.16. The *order* of the permutation $\pi \in S(n)$ (in symbols, $o(\pi)$) is the smallest positive integer m such that $\pi^m = \mathrm{id}$.

EXAMPLE 3.17. We record several elementary facts about orders of permutations.

- The order of the identity is 1 and this is the only permutation of order 1.
- The order of every transposition is 2.
- The successive powers of the cycle $(1, 3, 5, 7, 9) \in S(10)$ are

$$(1, 3, 5, 7, 9), (1, 5, 9, 3, 7), (1, 7, 3, 9, 5), (1, 9, 7, 5, 3) \text{ and } (\cdot).$$

  Thus the cycle $(1, 3, 5, 7, 9)$ has order 5.

REMARK 3.18. The properties of the order function on $S(n)$ should be compared to the (multiplicative) order function on $\mathbb{Z}_m^*$.

THEOREM 3.19. *Let r and $s \in \mathbb{Z}$. If $\pi \in S(n)$ has order m, then $\pi^r = \pi^s$ if and only if $r \equiv s \mod m$.*

PROOF. Assume without loss of generality that $r \geq s$. Now $\pi^r = \pi^s$ if and only if $\pi^{r-s} = \mathrm{id}$. Thus we establish the theorem by showing that for $q \in \mathbb{Z}$, $\pi^q = \mathrm{id}$ if and only if $q \equiv 0 \mod m$. If $q = km$ for some $k \in \mathbb{Z}$, then $\pi^q = (\pi^m)^k = \mathrm{id}$. Conversely, assume that $\pi^q = \mathrm{id}$. Using the division algorithm, we write $q = km + \rho$, with k and $\rho \in \mathbb{Z}$ and $0 \leq \rho < m$. Thus $\pi^\rho = \pi^{q-mk} = \pi^q(\pi^m)^{-k} = \mathrm{id}(\mathrm{id})^{-k} = \mathrm{id}$, and thus by the minimality of m, $\rho = 0$. □

PROPOSITION 3.20. *The order $o(\pi)$ of a cycle $\pi \in S(n)$ is its length.*

PROOF. Let $\pi = (a_1, a_2, ..., a_m)$ be a cycle of length m. This cycle moves an a_i to a_{i+1}, provided that for subscripts we interpret all operations modulo m. Thus π^r moves a_i to a_{i+r} and $r = m$ is the first power of π that fixes each a_i. □

PROPOSITION 3.21. *Let π and σ be disjoint cycles in $S(n)$. Then*

$$o(\pi\sigma) = \mathrm{lcm}(o(\pi), o(\sigma)). \tag{10}$$

PROOF. Let $r = o(\pi)$, $s = o(\sigma)$ and $d = \mathrm{lcm}(r, s)$. Then $d = ra = sb$, for some a and $b \in \mathbb{Z}_{>0}$. Thus because π and σ commute, $(\pi\sigma)^d = \pi^{ra}\sigma^{sb} = \mathrm{id}$. It follows that $o(\pi\sigma)|d$. Suppose that $(\pi\sigma)^e = \pi^e\sigma^e = \mathrm{id}$ for some $e \in \mathbb{Z}_{>0}$ (thus $e|o(\pi\sigma)$). Choose an integer k, $1 \leq k \leq n$. If k is moved by π, then it is fixed by σ (hence also by σ^e). Thus

$$k = \mathrm{id}(k) = \pi^e(\sigma^e(k)) = \pi^e(k).$$

Thus $r = o(\pi)|e$. Similarly, $s = o(\sigma)|e$. We conclude that $d = \mathrm{lcm}(r, s)|e$. In particular, $d|o(\pi\sigma)$ and we conclude that $d = o(\pi\sigma)$. □

In the last proof we never used the fact that π and σ were cycles; only that they were disjoint permutations. Hence we also have

COROLLARY 3.22 (of proof). *If π and σ are disjoint permutations in $S(n)$, then* (10) *holds.*

EXAMPLE 3.23. We have seen that the permutation

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 4 & 5 & 6 & 7 & 2 & 9 & 10 & 1 & 8 \end{pmatrix}$$

is decomposed as $(1,3,5,7,9)(2,4,6)(8,10)$. Thus (formally the conclusion follows only after we have established the next theorem)

$$o(\pi) = \text{lcm}(5,3,2) = 30.$$

THEOREM 3.24. *Let $\pi = \tau_1\tau_2...\tau_k$ be the decomposition of $\pi \in S(n)$ as a product of disjoint cycles. Then*

$$o(\pi) = \text{lcm}(o(\tau_1), o(\tau_2)..., o(\tau_k)).$$

PROOF. We use induction on k. The base case $k = 1$ is of course trivial. Assume that $k > 1$ and that we have the formula for permutations π which are products of $k-1$ disjoint cycles. If $\pi = (\tau_1\tau_2...\tau_{k-1})\tau_k$, where the k cycles are disjoint, then the permutations $\tau_1\tau_2...\tau_{k-1}$ and τ_k are also disjoint. Thus by Corollary 3.22,

$$o((\tau_1\tau_2...\tau_{k-1})\tau_k) = \text{lcm}(o(\tau_1\tau_2...\tau_{k-1}), o(\tau_k)),$$

and by the induction assumption,

$$o(\tau_1\tau_2...\tau_{k-1}) = \text{lcm}(o(\tau_1), o(\tau_2)..., o(\tau_k - 1)).$$

Finally,

$$\text{lcm}(o(\tau_1), o(\tau_2), ..., o(\tau_k)) = \text{lcm}(\text{lcm}(o(\tau_1), o(\tau_2)..., o(\tau_{k-1})), o(\tau_k)).$$

□

REMARK 3.25. The usefulness of the theorem is due to the fact that $o(\tau_i)$ is the length of τ_i.

DEFINITION 3.26. Let $\pi = \tau_1\tau_2...\tau_k$ be the decomposition of a non-trivial (meaning $\pi \neq$ id) permutation $\pi \in S(n)$ as a product of disjoint cycles. Since the τ_i commute, it involves no loss of generality to assume that

$$o(\tau_1) \leq o(\tau_2) \leq ... \leq o(\tau_k).$$

We call the k-tuple $(o(\tau_1), o(\tau_2), ..., o(\tau_k))$, the *shape* of π. The identity permutation has the empty shape. Two permutations π_1 and $\pi_2 \in S(n)$ are *conjugate* if there exists a $\sigma \in S(n)$ such that $\pi_2 = \sigma\pi_1\sigma^{-1}$.

Conjugation is an equivalence relation on $S(n)$. We verify that it satisfies the three required properties.

- (Reflexivity) Every $\pi \in S(n)$ is conjugate to itself ($\pi = \text{id}\pi\text{id}^{-1}$).
- (Symmetry) If for π_1 and $\pi_2 \in S(n)$, $\pi_2 = \sigma\pi_1\sigma^{-1}$ for some $\sigma \in S(n)$, then $\pi_1 = \sigma^{-1}\pi_2\sigma$.

- (Transitivity) If for π_1, π_2 and $\pi_3 \in S(n)$ there exist σ_1 and $\sigma_2 \in S(n)$ such that, $\pi_2 = \sigma_1\pi_1\sigma_1^{-1}$ and $\pi_3 = \sigma_2\pi_2\sigma_2^{-1}$, then

$$\pi_3 = \sigma_2\pi_2\sigma_2^{-1} = \sigma_2\sigma_1\pi_1\sigma_1^{-1}\sigma_2^{-1} = (\sigma_2\sigma_1)\pi_1(\sigma_2\sigma_1)^{-1}.$$

Thus conjugation partitions $S(n)$ into *conjugacy classes*. The conjugacy class of $\pi \in S(n)$ is the subset (of $S(n)$)

$$S(n)_\pi = \{\sigma\pi\sigma^{-1}; \sigma \in S(n)\}.$$

It is easily seen that the conjugacy class of the identity consists only of one element (namely, id).

THEOREM 3.27. *The permutations π_1 and $\pi_2 \in S(n)$ are conjugate if and only if they have the same shape.*

PROOF. It is clear by the above remarks that we may assume that both π_1 and $\pi_2 \neq$ id. We begin with some further general remarks about *conjugation* that help us understand what this operation means. For any three permutations π_1, π_2 and $\sigma \in S(n)$,

$$\sigma(\pi_1\pi_2)\sigma^{-1} = (\sigma\pi_1\sigma^{-1})(\sigma\pi_2\sigma^{-1});$$

that is, conjugation (by the same permutation) preserves products. Next, if π_1 sends $i \in X_n$ to j and $\pi_2 = \sigma\pi_1\sigma^{-1}$, then π_2 sends $\sigma(i)$ to $\sigma(j)$; that is, conjugation corresponds to a relabeling of the elements of X_n. Thus if π_1 is the cycle $(x_1, x_2, ..., x_r)$, then

$$\pi_2 = \sigma\pi_1\sigma^{-1} = (\sigma(x_1), \sigma(x_2), ..., \sigma(x_r)).$$

We note that the cycles π_1 and π_2 have the same length.

We are now ready to prove the theorem. We assume that π_1 and $\pi_2 \in S(n)$ are conjugate via the motion σ. Assume that

$$\pi_1 = \tau_1\tau_2...\tau_k \tag{11}$$

is the decomposition of π_1 as a product of disjoint cycles. Then

$$\pi_2 = \sigma\pi_1\sigma^{-1} = (\sigma\tau_1\sigma^{-1})(\sigma\tau_2\sigma^{-1})...(\sigma\tau_k\sigma^{-1})$$

is a decomposition of its conjugate as a product of disjoint cycles . Since τ_i and $\sigma\tau_i\sigma^{-1}$ have the same length, the only if part of the theorem has been established. To prove the if part of the theorem we assume that π_1 and π_2 have the same shape. Let (11) be the decomposition of π_1 as a product of disjoint cycles. Since π_2 has the same shape as π_1, its decomposition as a product of disjoint cycles is given by

$$\pi_2 = \tau_1'\tau_2'...\tau_k',$$

where we have the same number (k) of disjoint cycles and each of the cycles τ_i' (of π_2) has the same length as corresponding cycle τ_i (of π_1). Let $(x_1, x_2, ..., x_r)$ be a typical cycle τ_i and $(x_1', x_2', ..., x_r')$ be the corresponding cycle τ_i'. We define a permutation $\sigma \in S(n)$ by $\sigma(x_j) = x_j'$ if x_j appears in one of the cycles in the decomposition of π_1. This definition makes sense since a fixed x_j appears in at most one such cycle. We set $\sigma(x_j) = x_j$, if x_j does not appear in any of the cycles. It is easy to see that this indeed defines a permutation on n-letters and that it conjugates π_1 to π_2. □

We proceed to the definition of another invariant of a permutation, its sign. In the next definition we use formal expressions in variables (indeterminates) indexed by integers.

DEFINITION 3.28. For $n \in \mathbb{Z}_{\geq 2}$, we define a polynomial Δ in the n *indeterminates* x_1, x_2, ..., x_n by

$$\Delta(x_1, x_2, ..., x_n) = \prod_{1 \leq i < j \leq n} (x_i - x_j),$$

and for $\pi \in S(n)$, we define the polynomial $\pi\Delta$, by

$$\pi\Delta(x_1, x_2, ..., x_n) = \Delta(x_{\pi(1)}, x_{\pi(2)}, ..., x_{\pi(n)}).$$

(The polynomial $\pi\Delta$ is obtained from the polynomial Δ by replacing each appearance of x_i by $x_{\pi(i)}$.) The expressions $(x_i - x_j)$ appearing in the definition of Δ are called, its *factors*. They are transformed to factors $(x_{\pi(i)} - x_{\pi(j)})$ in $\pi\Delta$.

EXAMPLE 3.29. For $n = 3$ and $\pi = (1, 2, 3) = (1, 3)(1, 2)$,

$$\Delta(x_1, x_2, x_3) = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$$

and

$$\pi\Delta(x_1, x_2, x_3) = (x_2 - x_3)(x_2 - x_1)(x_3 - x_1) = (-1)^2\Delta(x_1, x_2, x_3).$$

Note that for π and $\sigma \in S(n)$,

$$(\pi\sigma)\Delta = \pi(\sigma\Delta)$$

since each side is obtained by replacing x_i by $x_{\pi(\sigma(i))}$. The next lemma is, at least at first glance, rather surprising. Its proof is also surprising; it is almost trivial.

LEMMA 3.30. *For each* $\pi \in S(n)$, $\pi\Delta = \pm\Delta$.

PROOF. Both Δ and $\pi\Delta$ have the same number of factors. Consider one of these factors $(x_i - x_j)$ in Δ (thus $1 \leq i < j \leq n$). The *corresponding* factor in $\pi\Delta$ is $(x_{\pi(i)} - x_{\pi(j)})$. We can, of course, assert that $\pi(i) \neq \pi(j)$ because π is a bijection of X_n. Further, for the same reason, there exist unequal positive integers k and l, each $\leq n$, such that $k = \pi(i)$ and $l = \pi(j)$. Thus either $(x_{\pi(i)} - x_{\pi(j)})$ is a factor of Δ (if $k < l$) or $-(x_{\pi(i)} - x_{\pi(j)})$ is a factor of Δ (if $k > l$). Thus each factor of $\pi\Delta$ is either plus or minus a factor of Δ. The result follows by collecting (multiplying) all the minus signs. □

DEFINITION 3.31. The *sign* of the permutation $\pi \in S(n)$, $\text{sgn}(\pi)$, whose value is ± 1, is defined by $\pi\Delta = \text{sgn}(\pi)\Delta$. The definition makes sense as a result of the last lemma. A permutation π is *even* if $\text{sgn}(\pi) = 1$ and *odd* otherwise.

THEOREM 3.32. *For* π *and* $\sigma \in S(n)$,

$$\text{sgn}(\pi\sigma) = \text{sgn}(\pi)\text{sgn}(\sigma).$$

PROOF. From the definitions,

$$(\pi\sigma)\Delta = \text{sgn}(\pi\sigma)\Delta$$

and

$$\pi(\sigma\Delta) = \text{sgn}(\pi)\sigma\Delta = \text{sgn}(\pi)\text{sgn}(\sigma)\Delta.$$

□

PROPOSITION 3.33. *The* sgn *function satisfies the following properties.*

(1) $\text{sgn}(\text{id}) = 1$
(2) *For all* $\pi \in S(n)$, $\text{sgn}(\pi) = \text{sgn}(\pi^{-1})$.

(3) *For all* π *and* $\sigma \in S(n)$, $\operatorname{sgn}(\sigma\pi\sigma^{-1}) = \operatorname{sgn}(\pi)$.
(4) *Every transposition has sign* -1.

PROOF. Since $\mathrm{id}\Delta = \Delta$, (1) follows. If $\pi \in S(n)$, then by the previous theorem and (1),

$$\operatorname{sgn}(\pi)\operatorname{sgn}(\pi^{-1}) = \operatorname{sgn}(\pi\pi^{-1}) = \operatorname{sgn}(\mathrm{id}) = 1.$$

So both $\operatorname{sgn}(\pi)$ and $\operatorname{sgn}(\pi^{-1})$ are either $+1$ or -1, establishing (2). By the previous theorem, for all π and $\sigma \in S(n)$,

$$\operatorname{sgn}(\sigma\pi\sigma^{-1}) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\pi)\operatorname{sgn}(\sigma^{-1})$$

and since σ and σ^{-1} have the same sign by (2), (3) follows. The transposition $(1,2)$ clearly has sign -1 and since an arbitrary transposition has the same shape as $(1,2)$, it is conjugate to $(1,2)$ by Theorem 3.27 and thus with sign -1 as a consequence of (3); finishing the proof of (4). □

EXAMPLE 3.34. Let $A(n)$ denote the set of even permutations in $S(n)$. Then

- $\mathrm{id} \in A(n)$.
- If π and $\sigma \in A(n)$, then $\pi\sigma \in A(n)$.
- If π, then $\pi^{-1} \in A(n)$.
- If $\pi \in A(n)$ and $\sigma \in S(n)$, then $\sigma\pi\sigma^{-1} \in A(n)$.
- Since $n \geq 2$, $(1,2) \notin A(n)$ and so the inclusion $A(n) \subset S(n)$ is proper.
- For $n > 1$, the map $\pi \mapsto (1,2)\pi$ sends even permutations bijectively onto odd permutations. So that

$$|A(n)| = \frac{n!}{2} \text{ for } n \geq 2.$$

- In language to be subsequently introduced, $A(n)$ is a *normal subgroup* of *index* two of $S(n)$, and that for $n \geq 1$,

$$\operatorname{sgn}\colon S(n) \to \{\pm 1\}$$

is a surjective homomorphism with kernel $A(n)$.

LEMMA 3.35. *Every cycle* π *is a product of transpositions. Further*

$$\operatorname{sgn}(\pi) = (-1)^{l(\pi)-1}.$$

PROOF. We easily check that

$$(x_1, x_2, ..., x_r) = (x_r, x_1)(x_{r-1}, x_1) \ ..., \ (x_3, x_1)(x_2, x_1).$$

The lemma is an immediate consequence of this identity. □

The lemma and our previous results imply

THEOREM 3.36. *Every permutation is a product of transpositions. The number of transpositions is even if and only if the permutation is.*

EXAMPLE 3.37. We have been studying

$$\pi = (1,3,5,7,9)(2,4,6)(8,10) = (1,9)(1,7)(1,5)(1,3)(2,6)(2,4)(8,10)$$

and thus

$$\pi^{-1} = (1,3)(1,5)(1,7)(1,9)(2,4)(2,6)(8,10).$$

REMARK 3.38. The last identity is a consequence of the fact that if

$$\pi = \tau_1\tau_2...\tau_k$$

is a decomposition of π as a product of transpositions, then

$$\pi^{-1} = \tau_k\tau_{k-1}...\tau_1;$$

which follows immediately from the fact that each 2-cycle is its own inverse.

EXERCISES

(1) What is $|A(1)|$?
(2) Determine the order and sign of
   - $(1,\ 2,\ 3,\ 4,\ 5)(10,\ 8,\ 6)(9,\ 11)$
   - $(1,\ 2,\ 3,\ 4,\ 5)(10,\ 5,\ 6)(9,\ 11)$
(3) Is every permutation of order 2 a transposition?
(4) Let $n \geq 2$. Show that every transposition is a product of transpositions of the form $(k, k+1)$, $1 \leq k \leq n-1$.
(5) Let $n \geq 3$.
   (a) Show that a product of two transposions in $S(n)$ is also a product of 3-cycles.
   (b) Show that the elements of $A(n)$ are products of 3-cycles.
   (c) Let $\pi \in A(n)$ be a k-cycle. Write π as a product of l 3-cycles. What is the minimum such l?

3. Definitions and more examples of groups

DEFINITION 3.39. Let X be a set. A *binary operation* or *product* on X is a map $* : X \times X \to X$; thus an assignment $x * y \in X$ to each ordered pair $(x, y) \in X \times X$. This property is also called *closure* of X under $*$.

DEFINITION 3.40. A *group* $(G, *)$ is a set G with a binary operation $*$ on G with the following properties.

- (Associativity) For all g, h and $k \in G$, $(g * h) * k = g * (h * k)$. (We say that the binary operation $*$ on G is *associative*.)
- (Existence of identity). There exists an *identity element* $e \in G$ such that $e * g = g * e = g$ for all $g \in G$.
- (Existence of inverses) For each $g \in G$, there exists an *inverse* $g^{-1} \in G$ such that $g^{-1} * g = g * g^{-1} = e$.

DEFINITION 3.41. A group $(G, *)$ is called *abelian* or *commutative* if $g * h = h * g$ for all g and $h \in G$. In this case we say that the binary operation $*$ on G is *commutative*.

NOTATION 3.42. *Some of the standard conventions are the following.*

- *We usually identify the group $(G, *)$ with the set G, and say the group G when the corresponding binary operation $*$ is understood from the context.*
- *The binary operation $*$ is many times written as $\cdot$ and also dropped from the notation completely. Thus xy, $x * y$ and $x \cdot y$ all stand for the product of x and y (in that order) in a group G.*
- *One never uses (interchangeably, for example) two different symbols (for example, $*$ and $\cdot$) for the same binary operation.*

- *For commutative groups, the binary operation is usually written as + and called a sum (rather than product), and an inverse of g will be denoted by $-g$.*

The definitions have some immediate consequences. Among them is

THEOREM 3.43. *The identity and inverses in groups are unique.*

PROOF. Let e and e' be identity elements of a group G. Then

$$e = ee' = e'.$$

The first equality uses the fact that e' is an identity element; the second, that e is. Now let $g \in G$ and assume it has h and k as inverses. Then

$$h = he = h(gk) = (hg)k = ek = k.$$

□

REMARK 3.44. For groups $(G, \cdot)$, the identity e is often written as 1; as 0, for abelian groups $(G, +)$. The identity element e of $(G, *)$ will be denoted by e_G when we need to emphasize which identity (group) is needed.

The next worksheet involves ideas from linear algebra and is preparation for an alternate discussion of Example (22) below.

WORKSHEET #4

Orthogonal affine transformations, a review.

(1) Let n be a positive integer. In this exercise we review affine orthogonal transformations of $\mathbb{R}^n$; with particular attention to the case $n = 2$. For this special case, **all claims appearing below should be verified**. One of the aims of this work sheet, is to explore the interplay between calculations and geometric ideas, between the Cartesian plane $\mathbb{R}^2$ and the complex plane $\mathbb{C}$.

(2) Recall that an $n \times n$ real matrix A is *orthogonal* iff $A^T A = \mathbf{I}$. An *affine orthogonal transformation* is a self-map of $\mathbb{R}^n$ defined by sending the column vector $v \in \mathbb{R}^n$ to the vector $Av + a$, where A is a fixed orthogonal $n \times n$ matrix and $a \in \mathbb{R}^n$ is fixed vector.

(3) Show that the determinant of a real orthogonal $n \times n$ matrix A must be either $+1$ or -1 by using the fact that for $n \times n$ matrices A and B,

$$\det AB = \det A \det B.$$

(4) Consider the case $n = 2$ and the real orthogonal matrix $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Conclude that the four real numbers a, b, c and d satisfy the three equations

$$a^2 + c^2 = 1,$$

$$b^2 + d^2 = 1$$

and

$$ab + cd = 0.$$

(5) The next task is to solve (simultaneously) the last three equations. The first of these equations tells us that the point $(a, c) \in \mathbb{R}^2$ lies on the circle with center at the origin and radius 1; hence $a = \cos\theta$ and $c = \sin\theta$ for a unique real number θ with $0 \leq \theta < 2\pi$.

Similarly the second equation tells us that $b = \cos\varphi$ and $d = \sin\varphi$ for some unique real number φ with $0 \leq \varphi < 2\pi$.

Conclude from the third equation that $\tan\theta\tan\varphi = -1$ and hence that $\varphi = \theta \pm \frac{\pi}{2}$. Hence also conclude that

$$A = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \text{ or } A = \begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix}.$$

Note that these two cases correspond to the two different possibilities for the sign of the determinant of A.

(6) Represent vectors in $\mathbb{R}^2$ as columns $X = \begin{bmatrix} x \\ y \end{bmatrix}$ with x and $y \in \mathbb{R}$. The orthogonal matrix A acts on $\mathbb{R}^2$ by sending the vector X to AX. In the two cases we have described we get

$$AX = \begin{bmatrix} x\cos\theta - y\sin\theta \\ x\sin\theta + y\cos\theta \end{bmatrix} \text{ and } AX = \begin{bmatrix} x\cos\theta + y\sin\theta \\ x\sin\theta - y\cos\theta \end{bmatrix},$$

respectively.

(7) A pair of real numbers (x, y) can be represented in rectangular coordinates by the single complex number $z = x + \imath y$. If $z \neq 0$, it can also be represented in polar coordinates by $re^{\imath\theta}$, where $r = \sqrt{x^2 + y^2}$ and $\theta = \sin^{-1}\frac{y}{r} = \cos^{-1}\frac{x}{r}$. We can in this context think of $e^{\imath\theta}$ as a short hand form of $\cos\theta + \imath\sin\theta$.

(8) In terms of complex numbers, our first map sends $z = x + \imath y$ to

$$(x\cos\theta - y\sin\theta) + \imath(x\sin\theta + y\cos\theta) = (\cos\theta - \imath\sin\theta)(x + \imath y) = e^{-\imath\theta}z$$

and in the second to

$$(x\cos\theta + y\sin\theta) + \imath(x\sin\theta - y\cos\theta) = (\cos\theta + \imath\sin\theta)(x - \imath y) = e^{\imath\theta}\bar{z} = \overline{e^{-\imath\theta}z}.$$

(9) Geometrically, the first case corresponds to a clockwise rotation of $\mathbb{C}$ about the origin by an angle θ. The second case, to complex conjugation followed by a counter-clockwise rotation by an angle θ or equivalently, a clockwise rotation by an angle θ followed by complex conjugation.

(10) The analysis of the case $n = 3$ is similar, but requires (much) more work.

EXAMPLES OF GROUPS

EXAMPLE 3.45. We have already encountered several groups. We list these as well as some new groups and some non-groups. We have grouped the examples under several categories. The reader should verify the axioms for the various groups and find the reason why other examples are not groups.

EXAMPLES BASED ON INTEGERS AND OTHER NUMBER SYSTEMS

(1) $(\mathbb{Z}, +)$ is an abelian group (and $|\mathbb{Z}| = \infty$).

(2) So is $(n\mathbb{Z}, +)$ for every integer n, where

$$n\mathbb{Z} = \{jn; j \in \mathbb{Z}\}$$

(and $|n\mathbb{Z}| = \infty$). In language to be developed, $n\mathbb{Z}$ is a *normal subgroup* of $\mathbb{Z}$.

(3) $(\mathbb{Z}_{\geq a}, +)$ is not a group for any $a \in \mathbb{Z}$ since the set is not closed under inverses.

(4) Neither is $(\mathbb{Z}, \cdot)$.

(5) For every positive integer n, $(\mathbb{Z}_n, +)$ is an abelian group and $|\mathbb{Z}_n| = n$. Its identity element is $[0]_n$.

(6) $(\{\pm 1\}, \cdot)$ is an abelian group with 2 elements. So is $(\mathbb{Z}_2, +)$. As we shall see later these are the same groups.

(7) For each $n \in \mathbb{Z}_{\geq 1}$, the n^{th} roots of unity (these are complex numbers of the form $e^{\frac{2\pi\imath k}{n}}$ with $k \in \mathbb{Z}$, $0 \leq k < n$), $\mathcal{U}_n$, form a commutative group of size n under multiplication.

(8) For $n \in \mathbb{Z}_{>0}$, $(\mathbb{Z}_n, \cdot)$ is not a group, but it has an identity element $[1]_n$. However, $(\mathbb{Z}_n^*, \cdot)$ is a group with $\varphi(n)$ members.

(9) The rationals $(\mathbb{Q})$, the reals $(\mathbb{R})$ and the complex numbers $(\mathbb{C})$ are each infinite abelian groups under addition. If we remove the zero element from these (obtaining $\mathbb{Q}^*$, $\mathbb{R}^*$ and $\mathbb{C}^*$), we obtain infinite abelian groups under multiplication.

(10) Complex numbers of absolute value 1 form an infinite abelian group under multiplication.

(11) We can use the complex numbers to construct another finite abelian group $\mathbb{C}_o$ under multiplication:

$$\mathbb{C}_o = \{\pm 1, \pm\imath\}$$

consisting of 4 elements. Its multiplication table is

The multiplication table for $\mathbb{C}_o$.

	1	-1	$\imath$	$-\imath$
1	1	-1	$\imath$	$-\imath$
-1	-1	1	$-\imath$	$\imath$
$\imath$	$\imath$	$-\imath$	-1	1
$-\imath$	$-\imath$	$\imath$	1	-1

.

(12) We now explore a less familiar example: a number system $\mathbb{H}$ known as the *quaternions*. We first consider three undefined new symbols $\imath$, $\jmath$ and κ. The set $\mathbb{H}$ is to consist of expressions of the form $a+b\imath+c\jmath+d\kappa$ with a, b c and $d \in \mathbb{R}$. (We are really considering 4 quantities 1, $\imath$, $\jmath$ and κ. The last formal sum is then $a1+b\imath+c\jmath+d\kappa$.) If we view 1, $\imath$, $\jmath$ and κ as basis elements of a real 4-dimensional vector spaces, we obtain the additive structure on the quaternions $(\mathbb{H}, +)$. In this structure

$$(a_1 1 + b_1\imath + c_1\jmath + d_1\kappa) + (a_2 1 + b_2\imath + c_2\jmath + d_2\kappa)$$

$$= (a_1 + a_2)1 + (b_1 + b_2)\imath + (c_1 + c_2)\jmath + (d_1 + d_2)\kappa.$$

To obtain a product structure for the quaternions, we must merely describe how to multiply the the 4 basis elements and then let the usual rules of arithmetic take over. We want 1 to be the identity element under the multiplication. So the 9 products among the other 3 basis elements must be specified. We require that

$$\imath^2 = \jmath^2 = \kappa^2 = -1, \imath\jmath = \kappa, \jmath\imath = -\kappa, \jmath\kappa = \imath, \kappa\jmath = -\imath, \kappa\imath = \jmath \text{ and } \imath\kappa = -\jmath.$$

Under these rules

$$(a_1 1 + b_1\imath + c_1\jmath + d_1\kappa)(a_2 1 + b_2\imath + c_2\jmath + d_2\kappa)$$

$$= (a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2)1 + (a_1b_2 + b_1a_2 + c_1d_2 + d_1c_2)\imath$$

$$+(a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2)\jmath + (a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2)\kappa.$$

We leave two questions for the reader to resolve. If we remove the zero element from $\mathbb{H}$, do we get a group under multiplication? An abelian group? The quaternions $\mathbb{H}$ contain a very interesting finite subset, the *quaternion* group consisting of 8 elements

$$\mathbb{H}_o = \{\pm 1, \pm\imath, \pm\jmath, \pm\kappa\}.$$

It is a tedious but routine matter to construct

The multiplication table for $\mathbb{H}_o$.

The entry in the i-th row, j-th column is the product of the i-th element with the j-th element (in this order).

	1	-1	$\imath$	$-\imath$	$\jmath$	$-\jmath$	κ	$-\kappa$
1	1	-1	$\imath$	$-\imath$	$\jmath$	$-\jmath$	κ	$-\kappa$
-1	-1	1	$-\imath$	$\imath$	$-\jmath$	$\jmath$	$-\kappa$	κ
$\imath$	$\imath$	$-\imath$	-1	1	κ	$-\kappa$	$-\jmath$	$\jmath$
$-\imath$	$-\imath$	$\imath$	1	-1	$-\kappa$	κ	$\jmath$	$-\jmath$
$\jmath$	$\jmath$	$-\jmath$	κ	$-\kappa$	1	-1	$\imath$	$-\imath$
$-\jmath$	$-\jmath$	$\jmath$	$-\kappa$	κ	-1	1	$-\imath$	$\imath$
κ	κ	$-\kappa$	$\jmath$	$-\jmath$	$-\imath$	$\imath$	-1	1
$-\kappa$	$-\kappa$	κ	$-\jmath$	$\jmath$	$\imath$	$-\imath$	1	-1

.

The entries in the above table are enough to convince us that all the group axioms except possibly associativity are satisfied. We will easily see that associativity holds too when we study Example (19), below. Is the group we have constructed abelian?

GROUPS OF PERMUTATIONS

(13) We have seen that for every non-empty set X, the set of permutations of X, $\mathrm{Perm}(X)$, forms a group under composition. This group is finite if and only if $|X|$ is finite and abelian if and only if $|X| \leq 2$.

(14) For every positive integer n, the sets $S(n)$ and $A(n)$ form groups under composition. In language to be established, $A(n)$ is a *normal subgroup* of $S(n)$. Here $|S(n)| = n!$ and for $n \geq 2$, $|A(n)| = \frac{n!}{2}$. If $n > 2$, $S(n)$ is not commutative; neither is $A(n)$ for $n > 3$.

(15) If we choose any $\pi \in S(n)$, then the powers of π

$$< \pi >= \{\pi^m; m \in \mathbb{Z}\}$$

form a group with $o(\pi)$ elements. There are many more groups of permutations. For example, the four elements of $S(n), n \geq 4$,

$$\mathrm{id}, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)$$

form, a group. The easiest way to verify the closure property is to construct

The multiplication table for G.

	id	$(1,2)(3,4)$	$(1,3)(2,4)$	$(1,4)(2,3)$
id	id	$(1,2)(3,4)$	$(1,3)(2,4)$	$(1,4)(2,3)$
$(1,2)(3,4)$	$(1,2)(3,4)$	id	$(1,4)(2,3)$	$(1,3)(2,4)$
$(1,3)(2,4)$	$(1,3)(2,4)$	$(1,4)(2,3)$	id	$(1,2)(3,4)$
$(1,4)(2,3)$	$(1,4)(2,3)$	$(1,3)(2,4)$	$(1,2)(3,4)$	id

.

We also note as a result of the last calculation that each element of G is its own inverse. Why is this not surprising?

GROUPS OF MATRICES

(16) Let n be a positive integer. Recall[5] that an $n \times n$ matrix is *invertible* if it has an inverse with respect to matrix multiplication. The set of invertible $n \times n$ matrices over the integers[6] ($\mathrm{GL}(n, \mathbb{Z})$), rationals ($\mathrm{GL}(n, \mathbb{Q})$), reals ($\mathrm{GL}(n, \mathbb{R})$), and complex numbers ($\mathrm{GL}(n, \mathbb{C})$) form a group under multiplication. The verification of the group axioms for these sets can be based on two facts from linear algebra. An $n \times n$ matrix with integer entries is invertible if and only if its determinant is ± 1; while in any of the other three cases, if and only if its determinant is $\neq 0$. Note that we have the proper inclusions

$$\mathrm{GL}(n, \mathbb{Z}) \subset \mathrm{GL}(n, \mathbb{Q}) \subset \mathrm{GL}(n, \mathbb{R}) \subset \mathrm{GL}(n, \mathbb{C}).$$

The reader unfamiliar with elementary matrix theory should verify the group axioms for $n = 2$.

(17) *Upper triangular* invertible matrices form a group under multiplication. An $n \times n$ matrix $A = [a_{ij}]$ is upper triangular if $a_{ij} = 0$ for all $i > j$.

(18) *Diagonal* invertible matrices form a group under multiplication. An $n \times n$ matrix $A = [a_{ij}]$ is diagonal if $a_{ij} = 0$ for all $i \neq j$.

(19) Let us define two 2×2 matrices

$$X = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \text{ and } Y = \begin{bmatrix} \imath & 0 \\ 0 & -\imath \end{bmatrix}.$$

As usual we note by $\mathbf{I}$ the 2×2, in this case, identity matrix: $\mathbf{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. Simple calculations show that

$$X^2 = Y^2 = -\mathbf{I} \text{ and } XY = -YX.$$

Define

$$Z = XY,$$

and calculate (once again) to see that

$$Z^2 = -\mathbf{I}, YZ = X, ZY = -X, ZX = Y \text{ and } XZ = -Y.$$

Thus the 8 matrices

$$\{\pm\mathbf{I}, \pm X, \pm Y, \pm Z\}$$

have the same multiplication as the quaternion group $\mathbb{H}_o$ (Example (12), above), with ± 1 in $\mathbb{H}_0$ corresponding to $\pm\mathbf{I}$ in this example; $\pm\imath$, to $\pm X$; $\pm\jmath$, to $\pm Y$ and $\pm\kappa$,

[5]From linear algebra courses.

[6]An $n \times n$ matrix A with integer entries may be invertible and still not belong to $\mathrm{GL}(n, \mathbb{Z})$. It belongs to $\mathrm{GL}(n, \mathbb{Z})$ if and only if so does A^{-1}.

to $\pm Z$. Since we know that matrix multiplication is associative, we conclude that so is the multiplication in $\mathbb{H}_0$.

(ASIDE TO THOSE WHO REMEMBER THE CONCEPT OF A LINEAR MAP.) If we send the quaternion $a + b\imath + c\jmath + d\kappa$ (here a, b, c and d are real numbers) to the 2×2 matrix $a\mathbf{I} + bX + cY + dZ$, then we have obtained an injective linear map from the quaternions (viewed as a real vector space) $\mathbb{H}$ into the 2×2 complex matrices, viewed as a real vector space.

(20) The set $\mathrm{SL}(2, \mathbb{Z})$ of 2×2 matrices with integer coefficient and determinant 1 forms a group under matrix multiplication. How does $\mathrm{SL}(2, \mathbb{Z})$ differ from $\mathrm{GL}(2, \mathbb{Z})$?

(21) Let p be a prime. An example closely related to the last one is the set $\mathrm{SL}(2, \mathbb{Z}_p)$ of 2×2 matrices whose entries are mod p congruence classes of integers and whose determinant is $[1]_p$. Thus an element of $\mathrm{SL}(2, \mathbb{Z}_p)$ is a matrix $A = \begin{bmatrix} [a]_p & [b]_p \\ [c]_p & [d]_p \end{bmatrix}$ with $[a]_p[d]_p - [b]_p[c]_p = [1]_p$. A number of routine calculations are needed to verify that $\mathrm{SL}(2, \mathbb{Z}_p)$ is a group under matrix multiplication. One shows, in particular that the inverse of the matrix A is $A^{-1} = \begin{bmatrix} [d]_p & [-b]_p \\ [-c]_p & [a]_p \end{bmatrix}$. We can view the elements of $\mathrm{SL}(2, \mathbb{Z}_p)$ as 2×2 integral matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with the integers a, b, c and d to be restricted to the values in $\{0, 1, ..., p-1\}$ and replacing all results of calculations by the mod p equivalent integer from this set. But despite the use of this notation $\mathrm{SL}(2, \mathbb{Z}_p)$ is NOT a *subgroup* of $\mathrm{SL}(2, \mathbb{Z})$.

GROUPS OF SYMMETRIES

These groups arise as *symmetries* of a geometric shape F; meaning orthogonal affine transformations of the plane $\mathbb{R}^2$ or 3-space $\mathbb{R}^3$ which leave invariant the fixed geometric figure F.

(22) (Rigid motions of an equilateral triangle.) We start with an equilateral triangle $\mathbf{T}$ and label its three vertices 1, 2 and 3, say in counter-clockwise order, to enable us to keep track of the motions we discuss. The three altitudes of $\mathbf{T}$ meet in a point O. Observe that any symmetry of $\mathbf{T}$ must maps vertices of $\mathbf{T}$ to vertices and sides of $\mathbf{T}$ to sides. Furthermore every symmetry of $\mathbf{T}$ is completely described by its action on the vertices this triangle.

The group of symmetries of $\mathbf{T}$ is often called $D(3)$. We proceed to describe it in detail. We define the first motion ρ as counter-clockwise rotation about O through an angle of $\frac{2\pi}{3}$. It is clear that this motion is a symmetry of $\mathbf{T}$. It is completely described (as a motion preserving $\mathbf{T}$) by its action on the vertices; hence by the permutation $(1, 2, 3) \in S(3)$ of these 3 points. A second motion R that we introduce is reflection in the perpendicular bisector of the side connecting the vertices 1 and 2 (this line passes through the mid-point of this side and the vertex

3). This motion is described by the transposition $(1,2) \in S(3)$. The figure $\mathbf{T}$ has, of course, many other symmetries. All of them will be described in terms of ρ, R and the identity map (id $\in S(3)$) that we denote by e. We introduce a multiplication on the set of symmetries of $\mathbf{T}$: if σ and τ are such symmetries, then $\sigma\tau$ is defined as the symmetry τ followed by the symmetry σ. (There is a good reason for this choice. We are viewing symmetries as maps and hence multiplication should correspond to composition. As a bonus, it also corresponds to multiplication of permutations.) This multiplication is associative. It is clear that the inverse of a symmetry is again a symmetry; it undoes what the original symmetry did. Let us observe that $\rho^3 = R^2 = e$ and start listing some of the symmetries we have:

$$\{e, \rho, \rho^2, R, \rho R \text{ and } \rho^2 R\}.$$

These six motions are distinct as can be seen by examining their action on the vertices of $\mathbf{T}$. There can be no other symmetries since there are at most 6 permutations of the vertices. Thus the last set coincides with $D(3)$ and is hence closed under multiplication. The construction of the multiplication table of $D(3)$ is simplified by the *relations*[7]

$$\rho^3 = e = R^2 \text{ and } \rho^2 R = R\rho. \tag{12}$$

The first two of these relations are obvious from the definitions. A geometric argument proves the last one. The reader is invited to provide one. The impatient reader could consult [**7**, pg. 186] or read the similar argument in the next example and adopt it to the current situation. We illustrate the calculation involved by considering two cases:

$$(\rho R)(\rho R) = \rho(R\rho)R = \rho(\rho^2 R)R = \rho^3 R^2 = e$$

and

$$(\rho^2 R)\rho^2 = (R\rho)\rho^2 = R\rho^3 = R.$$

The multiplication table for $D(3)$.

	e	ρ	ρ^2	R	ρR	$\rho^2 R$
e	e	ρ	ρ^2	R	ρR	$\rho^2 R$
ρ	ρ	ρ^2	e	ρR	$\rho^2 R$	R
ρ^2	ρ^2	e	ρ	$\rho^2 R$	R	ρR
R	R	$\rho^2 R$	ρR	e	ρ^2	ρ
ρR	ρR	R	$\rho^2 R$	ρ	e	ρ^2
$\rho^2 R$	$\rho^2 R$	ρR	R	ρ^2	ρ	e

If we place our triangle $\mathbf{T}$ on a coordinate system (a copy of $\mathbb{R}^2$ or $\mathbb{C}$) with center at O such that the base (for definiteness, take the base to be the side joining vertices 1 and 2) of $\mathbf{T}$ is parallel to the x-axis (the horizontal axis), then we can realize[8] the

[7] There are, of course, others. But all the relations in $D(3)$ are consequences of these three.

[8] As a consequence of the material in the last worksheet, for example.

motions ρ and R as orthogonal 2×2 matrices:

$$\rho = \begin{bmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{bmatrix} \text{ and } R = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}.$$

It is easier if we think of these as motions of $\mathbb{C}$:

$$z \mapsto e^{\frac{2\pi\imath}{3}} z \text{ and } z \mapsto -\bar{z}.$$

Even if we did not know how to derive these motions, we should easily be able to check that as self-maps of $\mathbb{C}$ or $\mathbb{R}^2$ they do the right thing. To do so we may scale our triangle so that its vertices lie on the unit circle and vertex 3 has complex coordinates $\imath = e^{\frac{\pi\imath}{2}}$. Thus vertices 1 and 2 must have coordinates $-\frac{\sqrt{3}}{2} - \frac{1}{2}\imath = e^{\frac{7\pi\imath}{6}}$ and $\frac{\sqrt{3}}{2} - \frac{1}{2}\imath = e^{\frac{-\pi\imath}{6}}$, respectively. Hence these two motions do act as expected on the vertices.

(23) (Rigid motions of a square.) Place a square $\mathbf{S}$ in the complex plane with vertices at $-1-\imath$ (labeled vertex 1), $1-\imath$ (labeled 2), $1+\imath$ (labeled 3) and $-1+\imath$ (labeled 4). Hence the center of $\mathbf{S}$ is at the origin O of the plane. We define the rigid motion ρ as rotation about O through an angle of $\frac{\pi}{2}$ (represented by the self map of $\mathbb{C}$ $z \mapsto \imath z$) and R as reflection in the perpendicular bisector of the edge joining the vertices 1 and 2 (represented by $z \mapsto -\imath\bar{z}$). The relations among these eight maps

$$\{e, \rho, \rho^2, \rho^3, R, \rho R, \rho^2 R, \rho^3 R\} \tag{13}$$

are

$$\rho^4 = e = R^2 \text{ and } \rho^3 R = R\rho, \tag{14}$$

as can easily be checked using the geometric interpretation of the symmetries. The multiplication table for the set of these 8 elements, that we call $D(4)$, is easily calculated, using only these relations, to be

The multiplication table for $D(4)$.

	e	ρ	ρ^2	ρ^3	R	ρR	$\rho^2 R$	$\rho^3 R$
e	e	ρ	ρ^2	ρ^3	R	ρR	$\rho^2 R$	$\rho^3 R$
ρ	ρ	ρ^2	ρ^3	e	ρR	$\rho^2 R$	$\rho^3 R$	R
ρ^2	ρ^2	ρ^3	e	ρ	$\rho^2 R$	$\rho^3 R$	R	ρR
ρ^3	ρ^3	e	ρ	ρ^2	$\rho^3 R$	R	ρR	$\rho^2 R$
R	R	$\rho^3 R$	$\rho^2 R$	ρR	e	ρ^3	ρ^2	ρ
ρR	ρR	R	$\rho^3 R$	$\rho^2 R$	ρ	e	ρ^3	ρ^2
$\rho^2 R$	$\rho^2 R$	ρR	R	$\rho^3 R$	ρ^2	ρ	e	ρ^3
$\rho^3 R$	$\rho^3 R$	$\rho^2 R$	ρR	R	ρ^3	ρ^2	ρ	e

The fact that these motions are closed under multiplication, as shown by the above table, proves that $D(4)$ is a group. As in the case of the triangle, the motions ρ and R can be represents as 2×2 matrices:

$$\rho = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \text{ and } R = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$$

and as (described above by the) self- maps of $\mathbb{C}$:

$$\rho : z \mapsto \imath z \text{ and } R : z \mapsto -\bar{z}. \tag{15}$$

These rigid motions can also be described as permutations of the vertices of $\mathbf{S}$:

Rigid motion	Permutation
e	id
ρ	$(1,2,3,4)$
ρ^2	$(1,3)(2,4)$
ρ^3	$(1,4,3,2)$
R	$(1,2)(3,4)$
$R\rho = \rho^3 R$	$(1,3)$
$R\rho^2 = \rho^2 R$	$(1,4)(2,3)$
$R\rho^3 = \rho R$	$(2,4)$

.

The second and and fifth lines of the above table determine the other six lines, of course. We see from the above table, that only 8 of the 24 permutations in $S(4)$ land in the group we have called $D(4)$. We claim that $D(4)$ is the full group of rigid motions of $\mathbf{S}$. There should be a reason why only $\frac{1}{3}$ of the elements of $S(4)$ correspond to motions of the square. To see why, consider the 6 lines joining the 4 vertices of $\mathbf{S}$. We label the (un-oriented) line joining the vertices a and b by ab. A rigid motion of $\mathbf{S}$ can send 13 to either 13 or 24, while an arbitrary permutation on 4 symbols can send 13 to any of the six lines. We conclude that $D(4)$ is the full group of rigid motions of the cube.

(24) (Rigid motions of a regular n-gon, $n \geq 2$.) A group can be defined by a set of *generators* (ρ (a different one in each case) and R (in some sense, the same in all cases) as in $D(3)$ and $D(4)$, the examples discussed above) subject to a set of *relations* satisfied by the generators (in the above two cases, (12) and (14)). To be specific, let $n \in \mathbb{Z}_{>1}$. We construct a group $D(n)$, the *dihedral n-group*, on generators ρ and R subject to the relations

$$\rho^n = e = R^2 \text{ and } \rho^{n-1}R = R\rho.$$

These relations are sufficient to construct the multiplication table for the group (it has $2n$ elements). Geometrically the group represents the rigid motions of a regular *n-gon* (a regular n sided polygon). The definitions for $n = 3$ and 4 agree, of courses. with our earlier definitions of the groups $D(3)$ and $D(4)$, respectively.

(25) (Rigid motions of a rectangle.) Let $\mathbf{R}$ be a rectangle which is not a square. To describe the symmetries of $\mathbf{R}$, we note that every element of this group must also be a symmetry of $\mathbf{S}$. So, we need to determine which of the eight elements of $D(4)$, fix $\mathbf{R}$. The motion ρ certainly does not. Only a little bit of thought is required to convince us that only the four motions

$$e, \rho^2, R, \rho^2 R$$

have the required property. The multiplication table for these motions is easily constructed. Observe that for each rigid motion r of $\mathbf{R}$, $r^2 = e$.

(26) Groups can also be associated with the study of solutions of equations of algebraic equations. We will discuss some of these after we describe some additional algebraic structures in §1 of Chapter 7.

EXERCISES

(1) Let X be a non-empty set. When is the group $\mathrm{Perm}(X)$ cyclic (see Definition 4.15 of Chapter 4)?
(2) Two of the rigid motions of the equilateral triangle were described as motions of $\mathbb{R}^2$ and then as motions of $\mathbb{C}$. Describe the other 4 as motions of these vector spaces, and then construct the multiplication table for these 6 motions in the two models. Show that you obtained (after relabeling) once again the multiplication table for $S(3)$ and $D(3)$.
(3) Verify that the multiplication (composition) table for the 8 self maps of $\mathbb{C}$ given in (13), where the maps ρ and R are defined by (15) is exactly the same as the multiplication table for $D(4)$.
(4) Verify that after relabeling of the elements, the multiplication table for $D(4)$ coincides with that for 8 permutations considered in the MAPLE program in §1.
(5) Use MAPLE or MATHEMATICA to construct the multiplication table for $D(5)$.
(6) Discuss the geometric realization of $D(2)$. What is the underlying geometric shape, the regular 2-gon? Can you identify $D(2)$ with another group?
(7) Identify the group of rigid motions of a rectangle (that is not a square) with a group encountered before.
(8) Explain why the rotation group of the octahedron is isomorphic to $S(4)$.
(9) What is the rotation group of the icosehedron?

CHAPTER 4

Group homomorphisms and isomorphisms.

The first two sections of the chapter are devoted to basic group theory. In the third section, we begin the study of homomorphisms, maps between groups that preserve the group structure. The fourth section is devoted to the study of groups of small order. The final section continues the study of homomorphisms.

1. Elementary group theory

This section deals with some of the elementary foundational results in group theory. The discussion parallels and generalizes part of our discussion of permutation groups.

THEOREM 4.1. *Let a and b be elements in a group G. There exist unique elements x and $y \in G$ such that $a = bx$ and $a = yb$.*

PROOF. It is easily seen that $x = b^{-1}a$ and $y = ab^{-1}$. □

REMARK 4.2. If G is abelian, then $x = y$, of course.

COROLLARY 4.3 (Cancellation law). *If g, h and b belong to a group G and $bg = bh$, then $g = h$. Similarly, if $gb = hb$, then $g = h$.*

PROOF. The first assertion follows from the uniqueness of x in the theorem. But this seems to be a rather torturous way to obtain the conclusion, which follows by multiplying each side of $bg = bh$ by b^{-1} on the left. The proof of the second assertion is similar. □

COROLLARY 4.4. *Let a and b be elements of a group G, then $(b^{-1})^{-1} = b$ and $(ab)^{-1} = b^{-1}a^{-1}$.*

PROOF. Take $a = e$ in the theorem and note that both b and $(b^{-1})^{-1}$ solve $e = b^{-1}x$. Again this assertion follows from the uniqueness of inverses as does the last claim in the statement of the corollary. □

The powers of an element g in a group G are defined exactly the way we defined the powers of a permutation $\pi \in S(n)$. We merely substitute g for each occurrence of π and G for each occurrence of $S(n)$ in Definition 3.13 of Chapter 3.

DEFINITION 4.5. Let g be an element of a group G. Set $g^0 = e$. For $k \in \mathbb{Z}_{>0}$, define inductively $g^k = gg^{k-1}$. Also define $g^{-k} = (g^{-1})^k$.

PROPOSITION 4.6. *Let g and h be elements in a group G and let r and s be integers. Then*

(1) $g^r g^s = g^{r+s}$,
(2) $(g^r)^s = g^{rs}$,
(3) $g^{-r} = (g^r)^{-1}$, *and*
(4) *if g and h commute, then $(gh)^r = g^r h^r$.*

PROOF. The required argument is identical to the one in the proof of Proposition 3.14 of Chapter 3. □

DEFINITION 4.7. An element g in a group G has *finite order* if there exists a positive integer m such that $g^m = e$ and the *order* of g is the smallest such m; we say that g has *infinite order* (or its order is ∞) if it does not have finite order. We let $o(g)$ be the order of g. Thus $o(g)$ is either a positive integer or ∞. The number of elements $|G|$ in a group G is also called its *order*, $o(G)$. So, $|G| = o(G) \in \mathbb{Z}_{>0} \cup \{\infty\}$.

REMARK 4.8. **1.** If n is a positive integer, then every $\pi \in S(n)$ has finite order in the above sense and its order as defined above agrees with its order as a permutation as defined in Chapter 3.

2. If the group G has finitely many elements (we shall say in this case that G is *a finite group*), then every one of its members has finite order.

3. The matrix $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ has infinite order in the group $\mathrm{SL}(2,\mathbb{Z})$. Since for every integer n, $A^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$.

4. As an element of the group $\mathrm{SL}(2,\mathbb{Z}_p)$, with p a prime, the matrix $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} [1]_p & [1]_p \\ [0]_p & [1]_p \end{bmatrix}$ has finite order p.

We now come to another key idea; the concept of a substructure.

DEFINITION 4.9. A non-empty subset H of a group $(G, *)$ is a *subgroup* (of G) if it is a group under the binary operation $*$ (restricted to $H \times H$). It is a *proper* subgroup if it is $\neq G$.

REMARK 4.10. **1.** A subgroup H of G always contains the identity $e \in G$. We verify this elementary fact. Since H is a group, it contains an identity element e'. Since $H \subseteq G$, $e' \in G$. Now $ee' = e'$ because $e' \in G$ and e is the identity in G, and $e'e' = e'$ because e' is the identity of H. Thus by the cancellation law (in G), $e = e'$.

2. Every group G has at least one subgroup; namely the *trivial* subgroup with one element; the identity element of G. All groups that contain more than one element have a second subgroup; namely the group G itself.

EXAMPLE 4.11. We have been discussing subgroups all along.

(1) The set of even integers $2\mathbb{Z}$ is a subgroup of $(\mathbb{Z}, +)$.
(2) Each of the following set-theoretic inclusions are subgroup inclusions (in the first set of inclusions the group operation is addition; multiplication, in the second)
$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$
and
$$\{\pm 1\} \subset \mathbb{Q}^* \subset \mathbb{R}^* \subset \mathbb{C}^*.$$
(3) $\mathrm{SL}(2,\mathbb{Z})$ is a subgroup of $\mathrm{SL}(2,\mathbb{R})$.
(4) But for any prime p, $\mathrm{SL}(2,\mathbb{Z}_p)$ is not a subgroup of $\mathrm{SL}(2,\mathbb{Z})$.

The next proposition gives easy tests for determining when susets of a group G are subgroups.

PROPOSITION 4.12. *Let H be a non-empty subset of a group G. The following conditions are equivalent:*
(a) *H is a subgroup of G.*
(b) *For all x and $y \in H$, x^{-1} and $xy \in H$.*
(c) *For all x and $y \in H$, $xy^{-1} \in H$.*

PROOF. Assume for the moment that H is closed under the multiplication it inherits from G. Since the product operation is the same for H and G; the multiplication in H is certainly associative. So in addition to closure, to show that H is a subgroup of G, we need to show that H contains the identity e of G and that the inverse of every element in H belongs to H. We are now ready to show that (a) $\Rightarrow$ (b) $\Rightarrow$ (c) $\Rightarrow$ (a). We start with (a). Hence (b) follows from the fact that H is a group. Now if (b) holds, then $y^{-1} \in H$ and hence so is xy^{-1}. So (b) implies (c). Finally if (c) is true, then there exists an $x \in H$ (since it is non-empty) and by taking $y = x$, we see that $e = xx^{-1} \in H$. To see that the inverse of every element $y \in H$ belongs to H, take $x = e$. To see that H is closed under multiplication of x by y (with both in H), observe that we already know that $y^{-1} \in H$ and thus $x(y^{-1})^{-1} \in H$. But $(y^{-1})^{-1} = y$. We conclude that (c) implies (a), □

The next two propositions provide methods for constructing subgroups of a given group.

PROPOSITION 4.13. *If H and K are subgroups of a group G, then so is $H \cap K$.*

PROOF. The set $H \cap K$ is not empty since it contains e. Now if x and $y \in H \cap K$, then these elements belong to both H and K and because these are subgroups, so does xy^{-1}; that says $xy^{-1} \in H \cap K$. □

PROPOSITION 4.14. *Let G be a group and x an element of order n in G. Then the distinct powers of x,*

$$< x >= \{x^m; m \in \mathbb{Z}\}$$

form a commutative subgroup of G containing n elements; called the cyclic subgroup of G generated by x.

PROOF. The set $< x >$ is not empty since it contains $e = x^0$. If r and $s \in \mathbb{Z}$ and x^r and $x^s \in < x >$, then so does $(x^r)(x^s)^{-1} = x^{r-s}$. □

To apply the above concept to abstract groups, rather than just subgroups of a given group, we introduce the next

DEFINITION 4.15. A group G is said to be *cyclic* with *generator* g if there exists an element $g \in G$ such that

$$G = \{g^m; m \in \mathbb{Z}\}.$$

In this case we write $G =< g >$ to indicate that the group G is generated by the element g. In general, we write

$$G =< g_1,\ g_2,\ ... >$$

to indicate that G is generated by the elements $g_1,\ g_2,$ ..., and

$$G =< g_1,\ g_2,\ ...\ ;\ R_1,\ R_2,\ ... >$$

to indicate that G is generated by the elements $g_1,\ g_2,$ ... subject to the relations $R_1,\ R_2,$ ....

EXERCISES

(1) Let G be a group and $g \in G$. If $o(g) = n \in \mathbb{Z}_{>0}$, show that for all $r \in \mathbb{N}$, $o(g^r) = \frac{n}{(n,r)}$.
(2) Is $\mathbb{Z}$ a group under subtraction?
(3) Is the intersection of two cyclic subgroups of a group also cyclic?

2. Lagrange's theorem

A remarkably simple way of decomposing groups will lead us to some surprisingly strong consequences. The key is a theorem due to Lagrange.

DEFINITION 4.16. Let H be a subgroup of G and let $a \in G$. We define a *left coset (of H in G)*

$$aH = \{ah; h \in H\}.$$

A *right coset* Ha is defined similarly.

REMARK 4.17. Several observations are in order.

(1) We restrict all remarks, propositions, theorems and examples to left cosets. Similar statements can of course be made for right cosets.
(2) Since $H = eH$, H is its own left coset.
(3) Since $a = ae$, $a \in aH$.
(4) If $b \in aH$, then $bH = aH$. Assume that $b = ah_o$ with $h_o \in H$. Then for all $h \in H$, $bh = ah_oh \in H$ and hence $bH \subseteq aH$. Conversely, for all $h \in H$, $ah = bh_o^{-1}h \in bH$ showing that $aH \subseteq bH$.
(5) aH is a subgroup of G if and only if $a \in H$. If $a \in H$, then $aH = H$ and thus aH is a subgroup. Conversely, if aH is a subgroup, then it contains e and thus $e = ah$ for some $h \in H$. Thus $a = h^{-1} \in H$.
(6) If we take $H = G$, we see that there is only one coset of G in G. If we take $H = \{e\}$, then we see that the coset of $a\{e\}$ of $\{e\}$ in G consists of the set with one element $\{a\}$.
(7) Since $a \in aH$,
$$\bigcup_{a \in G} aH = G.$$
(8) For commutative groups G, left and right cosets agree.

EXAMPLE 4.18. We have already encountered some cosets and we should examine some new ones.

(1) Let us fix a positive integer n. We know that $n\mathbb{Z}$ is a subgroup of $(\mathbb{Z}, +)$. Only a little thought is required to conclude that for all $a \in \mathbb{Z}$,
$$a + n\mathbb{Z} = [a]_n.$$
Why are we using additive notation $a + n\mathbb{Z}$ for the left coset? Does it differ from a right coset $n\mathbb{Z} + b$?
(2) Let $G = (\mathbb{Z}_6, +)$ and $H = \{[0]_6, [3]_6\}$, then
$$[1]_6 + H = \{[1]_6, [4]_6\} = [4]_6 + H$$
and in general
$$[a]_6 + H = [a + 3]_6 + H, \text{ for all } [a]_6 \in G.$$
Thus there are 3 left cosets of H in G.

(3) Let $G = S(3)$ and $H = \{\mathrm{id}, (1,2,3), (1,3,2)\}$. Then
$$(1,2)H = \{(1,2), (2,3), (1,3)\},$$
and there are only 2 left cosets of H in G. See also the next Proposition.

PROPOSITION 4.19. *Let a and b be elements of a group G and let H be a subgroup of G. Then either $aH = bH$ or $aH \cap bH = \emptyset$.*

PROOF. If $aH \cap bH \neq \emptyset$, then it contains an element, $c = ax = by$, where x and $y \in H$. Thus $b = axy^{-1}$ and it follows that $b \in aH$. By Item 4 of Remark 4.17, $aH = bH$. □

REMARK 4.20. A subgroup H of a group G introduces an equivalence relation R on G, where for x and $y \in G$, xRy if and only if $y^{-1}x \in H$.

PROPOSITION 4.21. *Let H be a subgroup of G and let $a \in G$. Then $|H| = |aH|$.*

PROOF. The map which sends $h \in H$ to $ah \in aH$ is a bijection. □

THEOREM 4.22 (Lagrange). *If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.*

PROOF. The group G can be decomposed as a finite union of disjoint cosets:
$$G = \bigcup_{i=1}^{m} a_i H.$$
Hence $|G| = m|H|$. □

COROLLARY 4.23. *Let g be an element of a finite group G, then $o(g)$ divides $|G|$.*

PROOF. The observation that $o(g) = | < g > |$ reduces the corollary to a special case of the theorem. □

DEFINITION 4.24. Let H be a subgroup of a finite group G. The *index* of H in G, $[G : H]$, is defined as the number of distinct cosets of H in G. In this language, Lagrange's theorem may be written as
$$o(G) = [G : H]o(H).$$

REMARK 4.25. Lagrange's theorem (its last corollary, in a more strict sense) is a generalization of two of our earlier results. We show that these earlier results follow from our last corollary.

- (Fermat) If p is a prime and $a \in \mathbb{Z}$ is not a multiple of p, then $a^{p-1} \equiv 1 \mod p$.

  PROOF. We use the group $(\mathbb{Z}_p^*, \cdot)$. It contains $p-1$ elements and since it contains $[a]_p$, $o([a]_p)$ divides $p-1$. □

- (Euler) For every positive integer n and all integers a that are relatively prime to n, $a^{\varphi(n)} \equiv 1 \mod n$.

  PROOF. We repeat the argument used above to prove Fermat. The group now is $(\mathbb{Z}_n^*, \cdot)$. It contains $\varphi(n)$ elements and since $[a]_n$ has a multiplicative inverse in $\mathbb{Z}_n$, it belongs to $\mathbb{Z}_n^*$. As before, $o([a]_p)$ divides the number of elements in the group $\mathbb{Z}_n^*$: $\varphi(n)$. □

- We see once again that Euler is a generalization of Fermat.

3. Homomorphisms

DEFINITION 4.26. A map $\theta : G \to H$ between groups is a *homomorphism* if

$$\theta(xy) = \theta(x)\theta(y) \text{ for all } x \text{ and } y \in G.$$

(That is, if it preserves the group structure. Multiplication on the left hand side of the last equation is in the group G; while the multiplication on the right hand side is in H.) The map θ is an *isomorphism* if it is also a bijection. In this case, $\theta^{-1} : H \to G$ is also an isomorphism. The groups G and H are *isomorphic* if there exists an isomorphism $\theta : G \to H$ between them and we then write $G \cong H$.

PROPOSITION 4.27. *If $\theta : G \to H$ is a homomorphism, then $\theta(e) = e$ and for all $x \in G$, $\theta(x^{-1}) = (\theta(x))^{-1}$.*

PROOF. In the first claim, the first e is the identity e_G of G and the second, e_H, of H, of course. To establish it, we note that $\theta(e_G) = \theta(e_G e_G) = \theta(e_G)\theta(e_G)$. If we multiply both sides of the last equation (ignoring the middle term) by $\theta(e_G)^{-1}$ on either the left or the right, we conclude that $e_H = \theta(e_G)$. For the second claim, we note that

$$e_H = \theta(e_G) = \theta(xx^{-1}) = \theta(x)\theta(x^{-1}) = \theta(x)(\theta(x))^{-1}$$

and

$$e_H = \theta(e_G) = \theta(x^{-1}x) = \theta(x^{-1})\theta(x) = (\theta(x))^{-1}\theta(x).$$

□

EXERCISE 4.28. Let n be a positive integer. *Reduction mod n* is the map

$$\text{red}_n : \mathbb{Z} \to \mathbb{Z}_n$$

that sends each an integer m to its congruence class modulo n. It is obviously a surjective group homomorphism with respect to the respective additive (abelian) group structures on $\mathbb{Z}$ and $\mathbb{Z}_n$.

PROPOSITION 4.29. *Let G be a group where every element other than e has order 2. Then G is abelian .*

PROOF. The hypothesis guarantees that for all $x \in G$, $x^{-1} = x$. Hence for all y and $x \in G$,

$$(xy)^{-1} = xy \text{ and } (xy)^{-1} = y^{-1}x^{-1} = yx.$$

□

THEOREM 4.30. *Let $n \in \mathbb{Z}_{>0}$. Every cyclic group of order n is isomorphic to $(\mathbb{Z}_n, +)$.*

PROOF. If g is the generator of a cyclic group G of order n, the isomporphism of G onto $\mathbb{Z}_n$ sends g to 1. □

EXERCISES

(1) Show that the relation R introduced in Remark 4.20 is an equivalence relation and then verify that for each $x \in G$, the equivalence class

$$[x] = \{y \in G; yRx\}$$

is the same as the left coset xH.

(2) Show that for each positive integer n, $(\mathbb{Z}_n, +)$ is a cyclic group of order n and that it is isomorphic to $(\mathcal{U}_n, \cdot)$ and to the group of permutations $< (1, 2, 3, ..., n) >$.
(3) Let n be a positive integer. Show that any two cyclic groups of order n are isomorphic. As a result of this fact, we use the symbol $\mathbb{Z}_n$ or $\mathbb{Z}_n =< 1 >$ to denote such a group when we use additive notation and $\mathcal{U}_n$ or $\mathcal{U}_n =< e^{\frac{2\pi\imath}{n}} >$ when we use multiplicative notation; in each case the second form also describes the generator of the group.
(4) Let $(G, \cdot)$ be a group.
- Show that the map that sends $x \in G$ to its square $x^2 = x \cdot x$ is a homomorphism of G into itself if and only if the group is abelian.
- Conclude that for abelian groups the elements that are their own inverses and the elements that are squares are each subgroups of G, H and K, respectively.
- Are either of the last two statements true for non abelian groups?
- What is the intersection of H and K?

4. Groups of small order

Let G be a finite group with n elements. In this section we describe all such groups with $n \leq 8$. We need some preliminary results that we proceed to establish. The first of these is the beginning of the classification theory of finite groups.

THEOREM 4.31. *A finite group G of prime order p is cyclic.*

PROOF. Let $e \neq g \in G$. Then

$$1 < o(g) \mid o(G) = p,$$

and thus $o(g) = p$. It follows that $< g >$ is a subgroup of G of order p and hence the inclusion of $< g;\ g^p = e >$ into G is an isomorphism. □

REMARK 4.32. $(\mathbb{Z}_p, +)$ is a good model (representative) for the isomorphism class of cyclic groups of order p. The convenient generator for $(\mathbb{Z}_p, +)$ is $[1]_p$ although $[a]_p$ will do as long as $a \in \mathbb{Z} - p\mathbb{Z}$.

THEOREM 4.33. *Let G be a group and a and b two of its members. Assume that a has finite order $n > 1$ and that $b^2 = a$. If n is odd assume further that $b \notin < a >$. Then $o(b) = 2o(a)$.*

PROOF. If $n = 2$, then $b \notin < a >$. For if $b \in < a >$, then $b = e$ or $b = a$. Both of these possibilities contradict the fact that $b^2 = a$.

Now $b^4 = a^2 = e$. Thus $o(b)|4$ and the only possibilities are $o(b) = 1$, 2 or 4. The first of these implies that $b = e$ which is impossible. The second implies that $b^2 = e$; which is also impossible since it would say that $a = e$. We conclude that $o(b) = 4$. We have established the theorem if $n = 2$. So assume that $n > 2$. We show first that if n is even, then (automatically) $b \notin < a >$. For if $b = a^r$ with $2 \leq r \leq (n-1)$ (note that as before, $b \neq e$ and $b \neq a$), then $a = b^2 = a^{2r}$. Thus $e = a^{2r-1}$ and $n|(2r-1)$. Since $3 \leq 2r - 1 \leq 2n - 3$, $r = n$ and it cannot be that $b^2 = a$. So in all cases, $b \notin < a >$. Now $b^{2n} = a^n = e$ and thus $o(b)|2n$. Let $s = o(b)$ (hence $b^s = e$). Thus $a^s = b^{2s} = e$ and hence $n|s$. We claim that $s \neq n$. This claim would imply that s must be at least $2n$ and hence $= 2n$. To verify the last claim, we assume (for contradiction) that $s = n$. If n is even (remember it is ≥ 4), then

$a^{\frac{n}{2}} = b^n = e$ which contradicts the fact that a has order n. If n is odd (remember it is ≥ 3), then $a^{\frac{n+1}{2}} = b^{n+1} = b$ which contradicts the fact that $b \notin < a >$. □

REMARK 4.34. If n is odd, then the assumption that $b \notin < a >$ is needed for the conclusion to hold. For in this case, we can choose $b = a^{\frac{n+1}{2}}$ and observe that

$$b^2 = a \text{ and } o(b) = o(a^{\frac{n+1}{2}}) = \frac{n}{(n, \frac{n+1}{2})} \leq n.$$

DEFINITION 4.35. Let $(G, *_1)$ and $(H, *_2)$ be groups. We introduce a binary operation $*$ on the direct product, $G \times H$, of G and H by the rule

$$(g_1, h_1) * (g_2, h_2) = (g_1 *_1 g_2, h_1 *_2 h_2), \text{ for } g_1 \text{ and } g_2 \in G, h_1 \text{ and } h_2 \in H.$$

PROPOSITION 4.36. *If G and H are groups, so is $G \times H$. For finite groups G and H,*

$$|G \times H| = |G| \ |H|.$$

PROOF. The group axioms are easily verified for $G \times H$. For example, the identity for $G \times H$ is (e_G, e_H) (which will be written as $e = (e, e)$) and the inverse of $(a, b) \in G \times H$ is (a^{-1}, b^{-1}). □

THEOREM 4.37. *If n and m are relatively prime positive integers, then*

$$\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm}.$$

PROOF. We make a few observation that should help the reader provide a proof of this result. Let a be a generator for $\mathbb{Z}_n$ and b for $\mathbb{Z}_m$. Thus $o(a) = n$ and $o(b) = m$. It follows that[1] $nm(a, b) = (m(na), n(bm)) = 0$. Thus $o(a, b)|nm$. Since for every positive integer k, $k(a, b) = (ka, kb)$ we conclude that $o(a, b)$ is a multiple of $o(a)$ and $o(b)$ and since these are relatively prime, a multiple of their product. □

REMARK 4.38. The above theorem is a special case of the Chinese remainder theorem ; see 5.40 which contains a proof of the above version.

EXAMPLE 4.39. The hypothesis in the last theorem that n and m be relatively prime is necessary. To see this we construct the

ADDITION TABLE FOR $\mathbb{Z}_4 \times \mathbb{Z}_2$

which we write additively since the group is abelian

	0	(1,0)	(2,0)	(3,0)	(0,1)	(1,1)	(2,1)	(3,1)
0	0	(1,0)	(2,0)	(3,0)	(0,1)	(1,1)	(2,1)	(3,1)
(1,0)	(1,0)	(2,0)	(3,0)	0	(1,1)	(2,1)	(3,1)	(0,1)
(2,0)	(2,0)	(3,0)	0	(0,1)	(2,1)	(3,1)	(0,1)	(1,1)
(3,0)	(3,0)	0	(1,0)	(2,0)	(3,1)	(0,1)	(1,1)	(2,1)
(0,1)	(0,1)	(1,1)	(2,1)	(3,1)	0	(1,0)	(2,0)	(3,0)
(1,1)	(1,1)	(2,1)	(3,1)	(0,1)	(1,0)	(2,0)	(3,0)	0
(2,1)	(2,1)	(3,1)	(0,1)	(1,1)	(2,0)	(3,0)	0	(1,0)
(3,1)	(3,1)	(0,1)	(1,1)	(2,1)	(3,0)	0	(1,0)	(2,0)

[1]We use additive notation because all the groups under consideration in this argument are abelian.

Using the table, we compute the orders of the elements of the group $\mathbb{Z}_4 \times \mathbb{Z}_2$.

element	0	$(1,0)$	$(2,0)$	$(3,0)$	$(0,1)$	$(1,1)$	$(2,1)$	$(3,1)$
order	1	4	2	4	2	4	2	4

If $\mathbb{Z}_4 \times \mathbb{Z}_2$ were cyclic, it would have order 8 (thus $\mathbb{Z}_8$) and hence contain an element of order 8. But none of its members have this order.

We proceed to describe all groups of order ≤ 8. We should keep in mind that $\mathbb{Z}_n \times \mathbb{Z}_m$ has order ≤ 8 as long as $nm \leq 8$.

4.1. $|G| = 1$**.** In this case $G =< e >= \{e\}$.

4.2. $|G| = 2$**, 3, 5, 7 and, in fact, all primes.** By Theorem 4.31, for each prime p there is only one (cyclic) group (up to isomorphisms) of size p (namely, $\mathbb{Z}_p$).

4.3. $|G| = 4$**.** If G has order 4, then its nontrivial elements can only have orders 4 and 2. If G has an element a of order 4, then it is cyclic and isomorphic to $\mathbb{Z}_4$. Otherwise all its elements, other than e, are of order 2 by Lagrange's theorem. By Proposition 4.29, G must be abelian. Choosing two distinct elements a and b in G of order 2, we conclude that

$$G = \{a, b;\ a^2 = e = b^2,\ ab = ba\},$$

and thus isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

4.4. $|G| = 6$**.** If G contains an element of order 6, then it is isomorphic to $(\mathbb{Z}_6, +)$. By Lagrange's theorem, the only other possibility is for all elements of G other that e to have orders 2 or 3.

So assume that G has no element of order 6. If G were also not to have an element of order 3, then it would have to be an abelian group by Proposition 4.29. Let a and b be two distinct elements of G of order 2. Then $\{a, b;\ a^2 = e = b^2,\ ab = ba\}$ would be a subgroup of G of order 4, contradicting Lagrange' theorem.

We conclude that G has an element a of order 3 and thus $H = \{e, a, a^2\}$ is a subgroup of G. Let $b \in G - H$. We consider the 6 elements of G: $\{e, a, a^2, b, ba, ba^2\}$; the first 4 of these are certainly distinct. If $ba = b$, then $a = e$, and if $ba = a^r$ for some $r \in \mathbb{Z}$, then $b = a^{r-1}$. We conclude that the first 5 elements in our last list are distinct. If $ba^2 = ba^s$ for $s = 1$ or 0, then $a^{2-s} = e$ which is impossible. Similarly if $ba^2 = a^r$ for some $r \in \mathbb{Z}$, then $b = a^{r-2}$. Thus the 6 elements in our list are distinct (hence this is the complete list of members of G) and we need only establish the multiplication table for these elements. The element b must have order 2 or 3. Let us try to compute b^2. If $b^2 \neq e$, it would have to be a^r with $r = 1$ or 2 or ba^s with $s = 0$, 1 or 2. If $b^2 = a$, then b has order 6; a contradiction. If $b^2 = a^2 \neq e$, then b cannot have order 2. Also $b^3 = ba^2 \neq e$; that is, b cannot have order 3; the last two statements yield a contradiction. Thus $b^2 \neq a^r$. If $b^2 = ba^s$, then $b = a^s$; which is also impossible. We have reached the conclusion that b has order 2. Let us see what we know at

this point about the multiplication table for G.

	e	a	a^2	b	ba	ba^2
e	e	a	a^2	b	ba	ba^2
a	a	a^2	e			
a^2	a^2	e	a			
b	b	ba	ba^2	e	a	a^2
ba	ba	ba^2	b			
ba^2	ba^2	b	ba			

We need to compute ab. There are only three possibilities $ab = ba^r$ with $r = 0$, 1 or 2. The first of these, $ab = b$, is impossible because it would imply that $a = e$. The second, $ab = ba$, would tell us that $(ab)^s = a^s b^s$ for all integers s and we would conclude that ab has order 6 (remember the only possibilities are 2, 3 and 6). Thus $ab = ba^2$. We now easily complete the multiplication table for G.

	e	a	a^2	b	ba	ba^2
e	e	a	a^2	b	ba	ba^2
a	a	a^2	e	ba^2	b	ba
a^2	a^2	e	a	ba	ba^2	b
b	b	ba	ba^2	e	a	a^2
ba	ba	ba^2	b	a^2	e	a
ba^2	ba^2	b	ba	a	a^2	e

A comparison of the above multiplication with the one for $S(3)$ shows that the group G is isomorphic to $S(3)$. An isomorphism $\theta : G \to S(3)$ can be chosen to satisfy

$$\theta(a) = (1,2,3) \text{ and } \theta(b) = (1,2).$$

It follows that

$$\begin{array}{lll} \theta(e) = \text{ id}, & \theta(a) = (1,2,3), & \theta(a^2) = (1,2,3)(1,2,3) = (1,3,2), \\ \theta(b) = (1,2), & \theta(ba) = (1,2)(1,2,3) = (2,3), & \theta(ba^2) = (1,2)(1,3,2) = (1,3) \end{array}.$$

We have shown that a group of order 6 is isomorphic to either $\mathbb{Z}_6$ or $S(3)$.

4.5. $|G| = 8$**.** We will see that in this case there are 5 groups up to isomorphisms: 3 abelian groups ($\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$ and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$) and 2 non-commutative groups ($D(4)$ and $\mathbb{H}_o$).

Let G be a group of order 8. If G contains an element g of order 8, then $G =< g >$ and is hence isomorphic to $\mathbb{Z}_8$. By Lagrange's theorem the only other possibility is for all the nontrivial ($\neq e$) elements of G to have orders 4 or 2.

We now assume that G does not contain an element of order 8 and assume for the moment that G is abelian . There are two cases to consider.

(a) If G has an element a of order 4, then $H =< e, a, a^2, a^3 >$ is a subgroup of order 4 of G and we may choose an element $c \in G - H$. Lagrange's theorem now tells us that $G = H \cup cH$. The element c has order 4 or order 2. If $o(c) = 2$, let $b = c$. If $o(c) = 4$, then $o(c^2) = 2$. If $c^2 \in G - H$, then we let $b = c^2$. If $c^2 \in H$, then because it has order 2, $c^2 = a^2$ and it follows that $o(ca) = 2$ and we let $b = ca$. We have shown that G contains an element $b \notin H$

of order 2. We thus conclude that $G = H \cup bH$. Because the group G is commutative, we have enough information to complete its multiplication table

	e	a	a^2	a^3	b	ba	ba^2	ba^3
e	e	a	a^2	a^3	b	ba	ba^2	ba^3
a	a	a^2	a^3	e	ba	ba^2	ba^3	b
a^2	a^2	a^3	e	a	ba^2	ba^3	b	ba
a^3	a^3	e	a	a^2	ba^3	b	ba	ba^2
b	b	ba	ba^2	ba^3	e	a	a^2	a^3
ba	ba	ba^2	ba^3	b	a	a^2	a^3	e
ba^2	ba^2	ba^3	b	ba	a^2	a^3	e	a
ba^3	ba^3	b	ba	ba^2	a^3	e	a	a^2

.

An analysis of the table shows that G is isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_2$; the isomorphism θ may be chosen to satisfy

$$\theta(a) = (1, 0) \text{ and } \theta(b) = (0, 1).$$

(b) We are left with the possibility that every nontrivial element of G has order 2. Let us choose two distinct elements of order 2 in G: a and b. We have already seen that the subgroup $H = \{e, a, b, ab\}$ of G of order 4 is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ (the case $|G| = 4$). So G must contain another element c of order 2 and $G = H \cup cH$. It now easy to construct the multiplication table for the group and conclude that it is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

It remains to consider non-abelian groups G of order 8. Such groups must contain elements of order 4 and choosing such an element a, we conclude that $H =< e, a, a^2, a^3 >$ is a subgroup of order 4 of G. We next choose an element $b \in G - H$. Then $o(b) = 4$ or $o(b) = 2$. In either case $G = H \cup bH$ and $ab \neq ba$; for if $ab = ba$, then $(a^r)(a^s) = (a^s)(a^r) = a^{r+s}$, $(a^r)(ba)^s = (ba)^s(a^r) = a^{r+s}b^s$ and $(ba)^r(ba)^s = (ba)^s(ba)^r = a^{r+s}b^{r+s}$ for all nonnegative integers r and s and G would be abelian . We consider separately the two cases.

(a) We first study the case where all the elements of $G - H$ have order 4. We need to compute b^2 and ab. Since b^2 has order 2 and such elements can be found only in H, we conclude that $b^2 = a^2$. We know that $ab \neq a^r$ (for all $r \in \mathbb{N}$) and $ab \neq ba$. Certainly, $ab \neq b$ Thus $ab = ba^r$ with $r = 2$ or 3. We show that $r = 2$ cannot occur. For if $ab = ba^2$, then $(ab)^2 = (ab)(ba^2) = a$ and since $ab \in H$, it must have order 8. This would imply that G is cyclic. Thus we are left with a group G generated by two elements a and b subject to the relations

$$a^4 = e,\ b^2 = a^2 \text{ and } ab = ba^3.$$

This suffices to construct the multiplication table for the group.

	e	a	a^2	a^3	b	ba	ba^2	ba^3
e	e	a	a^2	a^3	b	ba	ba^2	ba^3
a	a	a^2	a^3	e	ba^3	b	ba	ba^2
a^2	a^2	a^3	e	a	ba^2	ba^3	b	ba
a^3	a^3	e	a	a^2	ba	ba^2	ba^3	b
b	b	ba	ba^2	ba^3	a^2	a^3	e	a
ba	ba	ba^2	ba^3	b	a	a^2	a^3	e
ba^2	ba^2	ba^3	b	ba	e	a	a^2	a^3
ba^3	ba^3	b	ba	ba^2	a^3	e	a	a^2

.

An analysis of the table shows that G is isomorphic to the quaternion group $\mathbb{H}_o$; an isomorphism θ being defined by

$$\theta(a) = \imath \text{ and } \theta(b) = -\jmath.$$

(b) We are left to consider the possibility of the existence of an element $b \in G - H$ with $o(b) = 2$. We need only evaluate ab. As before $ab = ba^r$ with $r = 2$ or 3. Again, the case $r = 2$ is impossible; for if $ab = ba^2$, then $(ab)^2 = (ab)(ba^2) = a^3$ and we once again would be able to conclude that G is abelian. So in this case, the group is generated by two elements a and b subject to the relations

$$a^4 = e, b^2 = e \text{ and } ab = ba^3.$$

This suffices to conclude that the group is isomorphic to the group of symmetries of the square $D(4)$.

EXERCISES

(1) Construct an isomorphism from $S(3)$ to $D(3)$.
(2) The group $\mathbb{Z}_3 \times \mathbb{Z}_2$ has order 6. Hence it is isomorphic to either $\mathbb{Z}_6$ or $S(3)$. Which is it? Construct the isomorphism.
(3) Let G be the group of order 8 with the property that all its elements other than e have order 2. Compute its multiplication table and hence show that there is an isomorphism of G onto $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.
(4) Describe all possible groups of order 9.
(5) Describe all the subgroups of $S(4)$. Which of these are isomorphic?
(6) Let n be a positive integer. Describe the set of generators for $(\mathbb{Z}_n, +)$.
(7) Prove Theorem 4.37.

5. Homomorphisms and quotients

Homomorphisms and isomorphisms between groups $\theta : G \to H$ were defined (Definition 4.26) previously. An injective homomorphism is also called a *monomorphism*, and a surjective homomorphism, an *epimorphism*. Thus a homomorphism is an isomorphism if and only if it is both a monomorphism and an epimorphism. Homomorphisms preserve much of group structure; while isomorphisms are essentially relabellings of the "same" groups. An isomorphism of a group onto itself will be called an *automorphism* of the group.

Definition 4.40. Let G be a group. A subgroup $H \subset G$ is *normal* if $gHg^{-1} \subseteq H$ for all $g \in G$ (that is, $ghg^{-1} \in H$ for all $g \in G$ and all $h \in H$). Two elements f and f' of a group G are *conjugate* if there exists a $g \in G$ such that $f' = gfg^{-1}$.

Remark 4.41. The condition $gHg^{-1} \subseteq H$ is, of course equivalent to $H \subseteq g^{-1}Hg$. Hence H is a normal subgroup of G if and only if $gHg^{-1} = H$ for all $g \in G$.

Proposition 4.42. *Let $\theta : G \to H$ be a homomorphism between groups, then $\theta^{-1}(e)$ is a normal subgroup of G called the kernel of θ (in symbols* $\ker(\theta)$*). The image of θ,*

$$\mathrm{Im}(\theta) = \{h \in H; h = \theta(g) \text{ for some } g \in G\}$$

is a subgroup of H.

Proof. We know that $e \in \ker(\theta)$ and if g_1 and $g_2 \in \ker(\theta)$, then

$$\theta(g_1 g_2^{-1}) = \theta(g_1)\,(\theta(g_2))^{-1} = e.$$

Thus also $g_1 g_2^{-1} \in \ker(\theta)$. Hence $\ker(\theta)$ is a subgroup of G. If $g \in G$ and $h \in \ker(\theta)$, then

$$\theta\left(ghg^{-1}\right) = \theta(g)\theta(h)\theta\left(g^{-1}\right) = \theta(g)\ e\ \left(\theta(g)\right)^{-1} = e,$$

and thus $\ker(\theta)$ is a normal subgroup of G.

Certainly $e_H \in \mathrm{Im}(\theta)$. If h_1 and $h_2 \in \mathrm{Im}(\theta)$, then for $i = 1$ and 2, there exist $g_i \in G$ such that $h_i = \theta(g_i)$. Hence

$$h_1 h_2^{-1} = \theta(g_1)\theta(g_2^{-1}) \in \mathrm{Im}(\theta),$$

and $\mathrm{Im}(\theta)$ is a subgroup of H. □

REMARK 4.43.

- In general, for a fixed element g in a group G and a fixed subgroup $H \subseteq G$, the map

  $$\theta_g : h \mapsto ghg^{-1}$$

  is an isomorphism of H onto the subgroup $gHg^{-1} \subseteq G$, called *conjugation* (by g).

  PROOF. First we observe that gHg^{-1} is a subgroup (it certainly is a subset) of G. We note that for all h_1 and $h_2 \in H$,

  $$(gh_1g^{-1})(gh_2g^{-1})^{-1} = gh_1g^{-1}gh_2^{-1}g^{-1} = g(h_1h_2^{-1})g^{-1} \in gHg^{-1};$$

  thus gHg^{-1} is a subgroup of G. The map θ preserves multiplication since for h_1 and $h_2 \in H$,

  $$\theta(h_1h_2) = g(h_1h_2)g^{-1} = gh_1g^{-1}gh_2g^{-1} = (gh_1g^{-1})(gh_2g^{-1}) = \theta(h_1)\theta(h_2).$$

  If $ghg^{-1} = h'$, then $h = g^{-1}h'g^{-1}$. Thus $\theta(h) = e$ implies that $h = e$. It is clear that $\theta(H) = gHg^{-1}$. □

- We say that two subgroups H_1 and $H_2 \subseteq G$ are *conjugate* if there exists a $g \in G$ such that $H_2 = gH_1g^{-1}$.
- Let H be a subgroup of the group G. Then H is a normal if and only if $gH = Hg$ for all $g \in G$. Thus for a normal subgroup H, left and right cosets coincide.

  PROOF. Assume that H is normal in G. Fix $g \in G$. Define a map $\theta : gH \to Hg$ by $\theta(gh) = hg,\ h \in H$. This map is injective since $h_1g = h_2g$ for h_1 and $h_2 \in H$ implies that $gh_1gg^{-1} = gh_2gg^{-1}$ or $gh_1 = gh_2$. It is obviously surjective. Conversely, if $gH = Hg$ for all $g \in G$, then $gHg^{-1} = H$ for all $g \in G$ and hence H is a normal subgroup of G. □

- Every non-trivial group has at least two normal subgroups: the group itself and its trivial subgroup.
- All subgroups of an abelian group are normal.
- Every group of prime order has precisely two distinct subgroups; each is normal.
- The cyclic subgroup $< (1,2) >$ of $S(3)$ is NOT normal since

  $$(1,2,3)(1,2)(1,3,2) = (2,3).$$

The reason for introducing the concept of normality is explained by the next proposition and remark.

PROPOSITION 4.44. *Let H be a normal subgroup of the group G. The set of cosets*

$$G/H = \{gH;\ g \in G\}$$

has a natural group structure by defining the product

$$(g_1H)(g_2H) = (g_1g_2)H \text{ for } g_1 \text{ and } g_2 \in G.$$

The coset $H = eH$ is the identity element of this group known as the quotient group G modulo H. For all $g \in G$, the coset $g^{-1}H$ is the inverse of the coset gH.

PROOF. We are using left cosets; we could, of course use right cosets. The only issue is whether or not the multiplication is well defined. (Convince yourself that all the group axioms do indeed hold.) So what we have to prove is that if $g_1H = g_1'H$ and $g_2H = g_2'H$, then $(g_1g_2)H = (g_1'g_2')H$. The facts that $g_1H = g_1'H$ and $g_2H = g_2'H$ tell us, using only that H is a subgroup, that $g_1'g_1^{-1}$ and $g_2'g_2^{-1} \in H$. This alone is not enought to conclude that $(g_1'g_2')(g_1g_2)^{-1} = g_1'g_2'g_2^{-1}g_1^{-1} \in H$. We must use the fact that H is normal in G. Since $g_2'g_2^{-1} \in H$ and $g_1' \in G$ we conclude that $g_1'(g_2'g_2^{-1}){g_1'}^{-1} \in H$. Next because H is a group (we do not need normality for this step) and $g_1'g_1^{-1} \in H$, we also see that $g_1'g_2'g_2^{-1}{g_1'}^{-1}g_1'g_1^{-1} \in H$ as required. □

REMARK 4.45. Let H be a normal subgroup of the group G.

(1) The map that sends $g \in G$ to the coset gH is a surjective homomorphism of G onto G/H with kernel H. We call it the *canonical* homomorhism of G onto G/H.
(2) The simplest example shows that the normality assumption is needed. We use the fact that $H =< (1,2) >$ is not a normal subgroup of $G = S(3)$ to show that multiplication on $S(3)/ < (1,2) >$ is not well defined. We try to multiply $(1,3)H$ with $(2,3)H$; the result should be $(1,3,2)H$ if were to use $(1,3)$ as the representative for $(1,3)H$ and $(2,3)$ for $(2,3)H$, then we do get $(1,3,2)$ as the representative for $(1,3,2)H$. But we can use $(1,3)$ as the representative for $(1,3)H$ and $(2,3)(1,2) = (1,3,2)$ as representative for $(2,3)H$. If multiplication were well defined then $((1,3)H)((1,3,2)H) = (2,3)H = (1,3,2)H$; from which we would conclude the false statement that $(1,3,2)(2,3) = (1,3) \in H$.
(3) For all $g \in G$, the conjugation θ_g is an automorphism of H.
(4) For commutative groups $(G,+)$ the the multiplicative coset notation gH is replaced by the additive notation $g + H$. In this case G/H is also commutative.

REMARK 4.46. We discuss several examples fo group homomorphosms.

(1) The map the sends the complex number z to its absolute value $|z|$ is a homomorhism from $(\mathbb{C}^*, \cdot)$ onto $(\mathbb{R}_{>0}, \cdot)$ whose kernel consists of the complex numbers of absolute value 1.
(2) The exponential map that sends $x \in (\mathbb{R}, +)$ to $e^x \in (\mathbb{R}_{>0}, \cdot)$ is an isomorphism whose inverse is the logarithm map.
(3) More complicated is the complex exponential map that sends $z \in (\mathbb{C}, +)$ to $(\mathbb{C}^*, \cdot)$. It is a surjective homomorphism with kernel $2\pi\imath\mathbb{Z} \subset \mathbb{C}$.
(4) Let G be any group and $a \in G$. *Left translation by a*, T_a, is defined by

$$T_a(x) = ax \text{ for } x \in G.$$

Then $T_a \in$ Perm (G) and T defines an injective homomorphism from G to Perm (G). See the next section (Cayley's theorem) for a more complete discussion.

(5) Specialize the above situation with the two dimensional real vector space $G = (\mathbb{R}^2, +) = \mathbb{R} \times \mathbb{R}$.

(6) We construct one more group of homomorphisms (actually, a group of automorphisms). Let G be a group and $a \in G$. *Conjugation by* a, σ_a, is defined by

$$\sigma_a(x) = axa^{-1} \text{ for } x \in G.$$

Then $\sigma_a \in$ Perm (G) and since for all a, b and $x \in G$,

$$\sigma_a(\sigma_b(x)) = abxb^{-1}a^{-1},$$

the map σ that sends $a \in G$ to $\sigma_a \in$ Perm (G) is a group homomorphism. What is its kernel?

DEFINITION 4.47. An *exact sequence* of groups is a (perhaps infinite) collection of groups $\{G_i\}$ and homomorphisms $\theta_i : G_i \to G_{i+1}$:

$$\ldots G_{-1} \xrightarrow{\theta_{-1}} G_0 \xrightarrow{\theta_0} G_1 \xrightarrow{\theta_1} G_2 \xrightarrow{\theta_2} G_3 \xrightarrow{\theta_3} \ldots,$$

where
Im $(\theta_i) =$ ker (θ_{i+1}), or alternatively
the composite homomorphism $\theta_{i+1}\theta_i : G_i \to G_{i+2}$ is the trivial homomorphism (it sends every element of G_i to the identity element of G_{i+2}).

DEFINITION 4.48. A *short exact sequence* of groups is a diagram (a special case of the last definition that is most useful):

$$\{e\} \to G_1 \xrightarrow{\theta_1} G_2 \xrightarrow{\theta_2} G_3 \to \{e\},$$

where
the G_i for $i = 1,\ 2,\ 3$ are groups,
θ_1 and θ_2 are group homomorphisms,
θ_1 is a monomorphism (injective),
Im $(\theta_1) =$ ker (θ_2), and
θ_2 is an epimorphism (surjective).

We have seen that for every normal subgroup H of a group G,

$$\{e\} \to H \to G \to G/H \to \{e\}$$

is a short exact sequence.

EXERCISES

(1) Let $\mathcal{U}$ be the group of complex numbers of absolute value 1 under mutiplication. Show that $\theta(x) = e^{2\pi\imath x}$ defines a homomorphism of $(\mathbb{R}, +)$ onto $\mathcal{U}$. What is the kernel of this homomorphism?
(2) Show that $\mathbb{R}/\mathbb{Z}$ is isomorphic to $\mathcal{U}$.
(3) Do the powers of a three cycle in $S(3)$ form a normal subgroup of $S(3)$?
(4) Describe the kernel of the homomorphism σ.

6. Isomorphisms

In the abstract study of groups, a group and its isomorphic image are usually indistinguishable. We already saw, for example, that for each positive integer n, there is up to isomorphisms but one cyclic group $\mathbb{Z}_n$ of order n, that $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm}$ provided $(n, m) = 1$[2], and that $D(3) \cong S(3)$. One of the principal aims of this section is to properly place this last isomorphism within a more general theory as is done in the first subsection of this section.

6.1. Every group is a subgroup of a permutation group.

THEOREM 4.49. *(Cayley) Every group is isomorphic to a group of permutations.*

PROOF. Let G be a group. We must find a set X and a group G^* of permutations of X such that $G \cong G^*$ (thus we will have shown that G is isomorphic to a subgroup of $\mathrm{Perm}(X)$). There is very little besides G to work with. We set $X = G$. For $g \in G$, we define a self-map L_g of G by

$$L_g(x) = gx, x \in G$$

(L_g stands for multiplication on the left by g. It is obvious that L_g is a self-map of the set G. It is one-to-one since for x_1 and $x_2 \in G$, $gx_1 = gx_2$ implies that $x_1 = x_2$. The map is onto since for all $y \in G$, $g^{-1}y \in G$ and $L_g(g^{-1}y) = y$. Thus $L_g \in \mathrm{Perm}(G)$. We let $G^* = \{L_g; g \in G\}$. Obviously $G^* \subseteq \mathrm{Perm}(G)$. Since $\mathrm{Perm}(G)$ is a group under composition, composition is a binary operation on G^*, and to show that it is a subgroup of $\mathrm{Perm}(G)$, we must only establish the closure statement: for all g_1 and $g_2 \in G$, $L_{g_1} \circ (L_{g_2})^{-1} \in G^*$. This follows from the obvious identities

$$L_{g_1} \circ (L_{g_2})^{-1} = L_{g_1} \circ L_{g_2^{-1}} = L_{g_1 g_2^{-1}}.$$

These identities are verified in a straight forward manner. As an example we show that for all $g \in G$, $(L_g)^{-1} = L_{g^{-1}}$. This last equality means that $L_g \circ L_{g^{-1}} = L_{g^{-1}} \circ L_g = \mathrm{id}_G$; it follows from

$$L_g \circ L_{g^{-1}} = L_{gg^{-1}} = L_e = L_{g^{-1}g} = L_{g^{-1}} \circ L_g = \mathrm{id}_G$$

and $L_e = \mathrm{id}_G$.

We now have an obvious candidate for a homomorphism θ_L from G onto G^*: for $g \in G$, $\theta_L(g) = L_g$. The map θ_L is a homomorphism since for g_1 and $g_2 \in G$,

$$\theta_L(g_1 g_2) = L_{g_1 g_2} = L_{g_1} \circ L_{g_2} = \theta_L(g_1) \circ \theta_L(g_2).$$

The map θ_L is injective, since for $g \in G$, L_g is the identity map if and only if $g = e$; it is surjective by definition. □

DEFINITION 4.50. The isomorphism $\theta_L : G \to G^*$ is called the *left regular representation of* G.

REMARK 4.51. It should be recognized that the map $L_g, g \in G$ used in this section corresponds to (is the same as) the translation map map $T_a, a \in G$, used in the previous section.

[2]In the next section we generalize this result.

6.2. Solvable groups. In the study of the structure of groups, the following concept turns out to be extremely useful.

DEFINITION 4.52. Let G be a group. We say that G is *solvable* if there exists a finite sequence of subgroups $\{H_i\}$ of G:

$$G = H_0 \supset H_1 \supset H_2 \ ... \ \supset H_r = \{e\} \tag{16}$$

such that H_i is normal in H_{i-1} and the factor group H_{i-1}/H_i is abelian for $i = 1, \ ..., \ r$.

All abelian groups are obviously solvable. So are the groups $S(n)$ for $n = 2, 3$ or 4 (Exercise). We establish that for each $n \geq 5$, the permutation group $S(n)$ is not solvable. We need some preliminaries.

THEOREM 4.53. *Let H be a normal subgroup of G. Then G/H is abelian if and only if $aba^{-1}b^{-1} \in H$ for all a and $b \in G$.*

PROOF. Let $\theta : G \to G/H$ be the canonical homomorphism. Assume that G/H is abelian. For all a and $b \in G$,

$$\theta(aba^{-1}b^{-1}) = \theta(a)\theta(b)\theta(a^{-1})\theta(b^{-1}) = e_{G/H}.$$

Thus $aba^{-1}b^{-1} \in H$. Conversely, assume that $aba^{-1}b^{-1} \in H$ for all a and $b \in G$. Let A and $B \in G/H$. Since θ is surjective, there exists a and $b \in G$ such that $A = \theta(a)$ and $B = \theta(b)$. Thus

$$e_{G/H} = \theta(e_G) = \theta(aba^{-1}b^{-1}) = ABA^{-1}B^{-1};$$

from which it follows readily that $BA = AB$. □

PROPOSITION 4.54. *Let H and N be subgroups of $S(n)$ with $n \geq 5$ and N normal in H. If H contains every 3-cycle and H/N is abelian, then N contains every 3-cycle.*

PROOF. We take two 3-cycles in $S(n)$ with exactly one element in common, without loss of generality, $\sigma = (1, 2, 3)$ and $\tau = (3, 4, 5)$. By hypothesis both of these belong to H and since H/N is abelian, by the previous theorem, $(4, 3, 1) = \sigma\tau\sigma^{-1}\tau^{-1} \in N$. We have completed the argument. □

THEOREM 4.55. *For each $n \in \mathbb{Z}_{\geq 5}$, $S(n)$ is not solvable.*

PROOF. Using the notation of the definition of solvability, we conclude by induction that each H_i contains all 3-cycles which contradicts the fact that H_r is the trivial group. □

6.3. MORE sections to be included. Consider what we should have in this section.

EXERCISES

(1) The *right regular representation of the group G* is defined by the map $\theta_R : G \to G_*$, where

$$\theta_R(g) = R_g,$$
$$R_g(x) = xg^{-1} \text{ for } x \in G$$

and

$$G_* = \{R_g; g \in G\}.$$

Show that G_* is a subgroup of $\mathrm{Perm}(G)$ and that θ_R is an isomorphism of G onto G_*.

(2) Relate θ_L to θ_R.
(3) What can you conclude about θ_R of if we were to define R_g by $R_g(x) = xg, g \in G$?
(4) In this exercise we study the group $A(4)$.
    - What are the possible orders of the subgroups of $A(4)$?
    - Write an element $\pi \in A(4)$ as a disjoint product of cycles. Describe the products that can possibly appear.
    - Which of the following appear as isomorphic images of subgroups of $A(4)$: $(\mathbb{Z}_3, +)$, $\mathbb{Z}_2$, $\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$?
(5) Prove that $S(n)$ is solvable for $n = 2,\ 3$ and 4.
(6) Is $A(n)$, $n \geq 5$, solvable? Proof required.

CHAPTER 5

Algebraic structures

The main structures studied in this chapter are commutative rings and their ideals especially the ring integers and the ring of complex polynomials. We explore many of the similarities and some of the differences between these two structures.

1. A collection of algebraic structures

We start with a rather weak structure.

DEFINITION 5.1. A *semigroup* $(S, *)$ is a set S together with an associative binary operation $*$ on it. It has an *identity* if there is an element $e \in S$ such that $e * s = s = s * e$ for all $s \in S$.

EXAMPLE 5.2. We continue with some simple observations.

- Every group is a semigroup.
- The integers with multiplication $(\mathbb{Z}, \cdot)$ form a semigroup with identity element 1, but not a group.
- Let X be any set. The set $F(X)$ of all functions from X to itself is a semigroup under composition $\circ$ with identity id. If $|X| > 1$, then $(F(X), \circ)$ is not a group.

More interesting are the structures that are stronger than groups.

DEFINITION 5.3. A *ring* $(R, +, \cdot)$ is a set R together with two binary operations *addition* $+$ and *multiplication* $\cdot$ (usually dropped entirely from expressions) such that $(R, +)$ is an abelian group (thus the *(additive) identity* element of R is denoted by 0 and called *zero*) and

- multiplication is associative; that is, for all x, y and $z \in R$,
$$x(yz) = (xy)z,$$
and
- the the *distributivity* laws hold; that is, for all x, y and $z \in R$,
$$x(y + z) = xy + xz$$
and
$$(x + y)z = xy + yz.$$
- *has a multiplicative identity* 1; that is, there exists an $1 \neq 0$ in R such that $1x = x1 = x$ for all $x \in R$. [1]

The ring $(R, +, \cdot)$ is usually abbreviated by R. We need to specify various kinds of rings.

DEFINITION 5.4. A non-empty subset S of $(R, +, \cdot)$ is a *subring* of R if it a ring with respect to the ring operations $+$ and $\cdot$ of R.

[1] CAUTION: this axiom is not always required in the definition of rings.

It is easy to establish the following

PROPOSITION 5.5. *A non-empty subset S of $(R, +, \cdot)$ is a subring if and only if for all a and $b \in S$*
(a) $1 \in S$,
(b) $a - b \in$, *and*
(c) $ab \in S$.

DEFINITION 5.6. A ring $(R, +, \cdot)$

- is *commutative* if its multiplication is; that is, if $xy = yx$ for all x and $y \in R$.
- is an *integral domain* if it is a commutative ring without zero divisors. A *zero divisor* in the ring R is a non-zero $a \in R$ for which there exists a non-zero $b \in R$ such that $ab = 0$.
- is a *field* if it is a commutative ring in which every non-zero element has a multiplicative inverse; that is, for all $0 \neq x \in R$, there exists a $y \in R$ such that $xy = 1$.
- Let a and b be elements of the commutative ring R. It has been our practice to denote the additive inverse of b by $-b$ and $a + (-b)$ by $a - b$. Similarly if b has a multiplicative inverse b^{-1}, it is customary to denote ab^{-1} also by $\frac{a}{b}$

REMARK 5.7. In the setting of Proposition 5.5 we shall say that R is an *extension* of S. This will be particularly usefull language in our discussions of subfields of $\mathbb{C}$.

EXAMPLE 5.8. A discussion of various important examples follows.

(1) We studied in great detail the ring $(\mathbb{Z}, +, \cdot)$. It is an integral domain, but not a field. Under our definitions, $(2\mathbb{Z}, +, \cdot)$ certainly satisfies all the properties to be an integral domain, but it is not even a subring of $\mathbb{Z}$ because it does not contain a (mutiplicative) identity.
(2) The rationals $\mathbb{Q}$, reals $\mathbb{R}$, and complex numbers $\mathbb{C}$ are fields. Do the quaternions $\mathbb{H}$ form an integral domain or a field. Why? Each non-zero element of $\mathbb{H}$ has an inverse (see the exercise below).
(3) The set $M_2(\mathbb{Z})$ of 2×2 matrices with integer entries is a ring under matrix addition and multiplication with identity $\mathbf{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, but not an integral domain since
$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$
The ring is not commutative since, for example,
$$\begin{bmatrix} 2 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} \neq \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 2 \\ 0 & 1 \end{bmatrix}.$$
(4) Similar properties hold for the rings $M_2(\mathbb{Q})$, $M_2(\mathbb{R})$ and $M_2(\mathbb{C})$.
(5) For every integer, $n \geq 2$, $(\mathbb{Z}_n, +, \cdot)$ is a commutative ring with identity. It has zero divisors if n is composite and it is a field for for n prime (see next set of exercises).
(6) Define
$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2}; a, b \in \mathbb{Z}\} \subset \mathbb{R}$$
and endow it with the usual addition and multiplication it inherits as a subset of $\mathbb{R}$. Then $(\mathbb{Z}[\sqrt{2}], +, \cdot)$ is an integral domain with an identity.

(7) So is
$$\mathbb{Z}[\imath] = \{a + b\imath; a, b \in \mathbb{Z}\} \subset \mathbb{C}.$$
(8) The last two integral domains are not fields. We can enlarge them to get fields $\mathbb{Q}[\sqrt{2}]$ and $\mathbb{Q}[\imath]$:
$$\mathbb{Z}[\sqrt{2}] \subset \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2}; a, b \in \mathbb{Q}\} \subset \mathbb{R}$$
and
$$\mathbb{Z}[\imath] \subset \mathbb{Q}[\imath] = \{a + b\imath; a, b \in \mathbb{Q}\} \subset \mathbb{C}.$$
(9) The last set of examples is part of the story of the first appearance of fields in the study of mathematics – see Chapter 9. Let n be a positive integer and consider a *monic* polynomial[2] $P(x)$ of degree n
$$x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0$$
with rational coefficients a_i. The fundamental theorem of algebra[3] tells us that $P(x)$ has precisely n roots counting multiplicities; thus at most n distinct roots. There is smallest field F consisting of complex numbers and containing these roots. The study of the roots of $P(x)$ is facilitated by the field F. For degree one polynomials, $F = \mathbb{Q}$. For degree two polynomials, there are already infinitely many candidates for F (these fields can be divided however into finitely many classes). The examples $\mathbb{Q}[\sqrt{2}]$ and $\mathbb{Q}[\imath]$ belong to distinct classes and correspond to the polynomials $x^2 - 2$ and $x^2 + 1$, respectively.

Rings share many properties with the integers. An example is

PROPOSITION 5.9. *Let R be a ring. Then $x0 = 0 = 0x$ for all $x \in R$.*

PROOF. Using the axioms for rings
$$0x + 0x = (0 + 0)x = 0x.$$
Thus also
$$(0x + 0x) + (-0x) = 0x + (-0x) = 0.$$
But the left-hand side of the last equation is
$$0x + (0x + (-0x)) = 0x.$$
The proof that $x0 = 0$ is similar and left to the reader. □

DEFINITION 5.10. A map θ from a ring R to a ring S is a *(ring) homomorphism* if
(1) $\theta(a + b) = \theta(a) + \theta(b)$ and
(2) $\theta(ab) = \theta(a)\theta(b)$ for all a and $b \in R$.
(3) $\theta(1) = 1$.
(4) As usual, θ is an *isomorphism* if it both injective and surjective. An isomorphism of the ring R onto itself is an *automorphism* pf R.

We define two more general structures. The first of these should be familiar to most readers.

[2]See the next section for more information on polynomials.
[3]Its "easiest" proof uses complex analysis.

DEFINITION 5.11. Let K be a field.[4] A *vector space* V (*over the field* K) is an abelian group V (written additively) together with a *scalar multiplication* (of elements of V by elements of K); that is, an operation[5] that assigns to each *scalar* $\lambda \in K$ and each *vector* $v \in K$, a vector (written as) $\lambda v \in V$ such that

(1) for all $v \in V$, $1v = v$,
(2) for all λ and $\mu \in K$ and all $v \in V$, $(\lambda\mu)v = \lambda(\mu v)$,
(3) for all λ and $\mu \in K$ and all $v \in V$, $(\lambda + \mu)v = \lambda v + \mu v$, and[6]
(4) for all $\lambda \in K$ and all u and $v \in V$, $\lambda(u + v) = \lambda u + \lambda v$.

If V is also a ring (thus with a second multiplication operation which maps ordered pairs of vectors into their product; $V = (V, +, \cdot)$), then it is called a (K-)*algebra* provided the two multiplications (ring multiplication in V and scalar multiplication) are related by

$$\lambda(uv) = (\lambda u)v = u(\lambda v) \text{ for all } \lambda \in K \text{ and all } u \text{ and } v \in V.$$

EXAMPLE 5.12. Some examples that should be familiar to the reader as well as some examples that are not so familiar follow.

(1) Most elementary linear algebra courses (books) are devoted to a study of the vector spaces $\mathbb{R}^n$ over $\mathbb{R}$ consisting on n-tuples $(\lambda_1, ..., \lambda_n)$ of real numbers and the vector space $\mathbb{C}^n$ over $\mathbb{C}$ where the n-tuples $(\lambda_1, ..., \lambda_n)$ consist of complex numbers.
(2) Every vector space over $\mathbb{C}$ is automatically a vector space over $\mathbb{R}$. For $(\lambda_1, ..., \lambda_n) \in \mathbb{C}^n$, we can use the decomposition

$$\lambda_i = a_i + b_i\imath$$

of each component into its real an imaginary part, to construct a canonical identification

$$\mathbb{C}^n \ni (\lambda_1, ..., \lambda_n) \mapsto (a_1, ..., a_n, b_1, ..., b_n) \in \mathbb{R}^{2n}.$$

(3) Sets of polynomials form interesting vector spaces. They are studied in the next section.
(4) Let I be any interval in $\mathbb{R}$. The space $C_{\mathbb{R}}(I)$ of continuous real valued functions on I is an $\mathbb{R}$-algebra with the usual definitions of addition and multiplication of functions.
(5) The constructions and definitions of the last example also hold with $\mathbb{R}$ replaced by $\mathbb{Q}$ or $\mathbb{C}$. We can also replace I by any topological space – a space where the concept of continuity makes sense.
(6) We fix a prime p. The set $M_2(\mathbb{Z}_p)$ of 2×2 matrices with entries from the field $\mathbb{Z}_p$ with the usual matrix operations form a $\mathbb{Z}_p$-algebra.
(7) The set of 2×2 matrices of the form

$$a \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + b \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix},$$

[4]For most of the interesting examples K is $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$.

[5]Thus a map from $K \times V$ into V.

[6]Note that in the last and next equation, the + sign is used in a different sense on the two sides of the equal sign. The + sign on the left hand-side refers to scalar addition in the field K; while the + sign on the right hand-side refers to vector addition in V. Similarly the symbol 0 stands for both the additive identity in the field K and the identity in the group V.

with a and $b \in \mathbb{R}$ with the usual matrix operations form another model for the complex numbers $\mathbb{C}$; the matrices

$$\mathbf{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ and } Y = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

represent 1 (the identity) and $\imath$, respectively. In particular, a complex number $a+b\imath$ can also be considered as the real 2×2 matrix $\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$.

(8) Fix a positive integer n. The set of $n \times n$ matrices $M_n(\mathbb{Z})$, $M_n(\mathbb{Q})$, $M_n(\mathbb{R})$ and $M_n(\mathbb{C})$, with respectively, integer, rational, real and complex entries are much studied objects in many branches of theoretical and applicable mathematics.

REMARK 5.13. In the rest of this chapter we will use elementary properties of vector spaces and linear maps between them. In particular, we will use the following properties: Let $X = \{X_1,\ X_2, ...,\ X_n\}$ be a finite set of vectors in a vector space V over the field K.

- We say that the set X is a *spanning set* for V if every vector $v \in V$ is a linear combination of vectors in X; that is, there exists constants λ_i such that $v = \sum_{i=1}^{n} \lambda_i X_i$. In this case we say that the vector space is *finite dimensional*.
- The set X is *linearly independent* if a relation of the form $0 = \sum_{i=1}^{n} \lambda_i X_i$ with the constants $\lambda_i \in K$ implies that each $\lambda_i = 0$.
- For finite dimensional vector spaces, the dimension of the space can be defined as the minimum number of spanning vectors or the maximum number of linearly independent vectors in the space.

SOME MATERIAL ON DETERMINANTS AND DIAGONALIZATION OF MATRICES NEEDED FOR FUTURE CHAPTERS.

EXERCISES

(1) Show that the semigroup $(F(X), \circ)$ has the following weak form of the cancellation property. Let f, g and $h \in F(X)$. If $f \circ g = f \circ h$ and f is injective, then $g = h$. Show conversely that if for some fixed $f \in F(X)$, we have that for all g and $h \in F(X)$ $f \circ g = f \circ h$ implies that $g = h$, then f is injective.

Similarly show that $f \in F(X)$ is surjective if and only if for all g and $h \in F(X)$, $g \circ f = h \circ g$ implies that $g = h$.

(2) Show that every non-zero element in the quaternions $\mathbb{H}$ has a (multiplicative) inverse.

(3) We have seen that there is a map M that assigns to the complex number $c = a + b\imath$, with a and $b \in \mathbb{R}$, the real 2×2 matrix $\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$. Call this set of matrices $\mathbb{M}$.

- Show that $\mathbb{M}$ is a field with respect to matrix addition and multiplication.
- Show that for two complex numbers c_1 and c_2,

$$M(c_1 + c_2) = M(c_1) + M(c_2) \text{ and } M(c_1 c_2) = M(c_1)M(c_2).$$

- Show that Thus M is an isomorphism between $\mathbb{C}$ and $\mathbb{M}$.

(4) Prove that a finite integral domain must be field.

Most of our examples on rings will involve two cases: the integers $(\mathbb{Z}, +, \cdot)$ that were already studied in great detail and spaces of polynomials whose study is begun in the next section.

2. The algebra of polynomials

We begin with a

DEFINITION 5.14. A *(complex) polynomial* $p(x)$ is a formal expression in an *indeterminate* x and its powers of the form

$$p(x) = a_0 + a_1 x + ... + a_n x^n, \tag{17}$$

where $n \in \mathbb{Z}_{\geq 0}$ and $a_i \in \mathbb{C}$ for $i = 0, 1, ..., n$. For each non-negative integer k we view x^k as the k^{th} power of x and thus $x^0 = 1$. We denote the set of polynomials by $\mathbb{C}[x]$. If we restrict the domain of coefficients to be respectively the reals, rationals, integers, we get respectively the sets of *real polynomials*, *rational polynomials* and *integer polynomials*. With obvious notational conventions, we have the proper set inclusions

$$\mathbb{C}[x] \supset \mathbb{R}[x] \supset \mathbb{Q}[x] \supset \mathbb{Z}[x].$$

If $a_n \neq 0$, then we say the polynomial $p(x)$ has *degree* n and write $\deg p(x) = n$, and we call a_n the *leading coefficient of* of $p(x)$. The polynomial $p(x)$ is *monic* if $a_n = 1$.

REMARK 5.15.

(1) The degree has not been defined for the identically zero polynomial ($n = 0 = a_0$). It is covenient to define the degree of that polynomial, which will be denoted by 0, to be $-\infty$ and to regard $-\infty < d$ for all $d \in \mathbb{Z}_{\geq 0}$.
(2) The constants are a subset of the polynomials: $\mathbb{C} \subset \mathbb{C}[x]$. The non-zero constants $\mathbb{C}_{\neq 0}$ are precisely the polynomials of degree 0.
(3) We will work mostly with complex polynomials. The reader should decide what changes, if any, are required for more restrictive classes of polynomials. Because $\mathbb{Z}$ is not a field, the $\mathbb{Z}[x]$ theory is significantly different from the $\mathbb{C}[x]$ theory.
(4) The complex polynomial $p(x)$ can be regarded both as a formal expresssion in its own right and as a continuous (it has many more properties) self-map of $\mathbb{C}$. In this context, it is usually written as

$$p : \mathbb{C} \to \mathbb{C},$$

and $p(x)$ denotes the value of the function p at the point $x \in \mathbb{C}$. Real (rational, integral) polynomials define self maps of $\mathbb{R}$ ($\mathbb{Q}$, $\mathbb{Z}$). We can, of course, use results from calculus when considering element of $\mathbb{R}[x]$. We will use below at least one such result.

It is convenient to write

$$p(x) = \sum_{i=0}^{n} a_i x^i = \sum_{i=0}^{\infty} a_i x^i,$$

where in the last sum it is understood that $a_i = 0$ for all but finitely many indeces i. With this convention we introduce several binary operations:

addition of polynomials (on $\mathbb{C}[x] \times \mathbb{C}[x]$)

$$\sum_{i=0}^{\infty} a_i x^i + \sum_{i=0}^{\infty} b_i x^i = \sum_{i=0}^{\infty} (a_i + b_i) x^i,$$

multiplication of polynomials by scalars (on $\mathbb{C} \times \mathbb{C}[x]$)

$$\lambda \left(\sum_{i=0}^{\infty} a_i x^i \right) = \sum_{i=0}^{\infty} \lambda a_i x^i$$

and multiplication of polynomials (on $\mathbb{C}[x] \times \mathbb{C}[x]$)

$$\left(\sum_{i=0}^{\infty} a_i x^i \right) \left(\sum_{i=0}^{\infty} b_i x^i \right) = \sum_{i=0}^{\infty} \left(\sum_{j=0}^{i} a_j b_{i-j} \right) x^i.$$

Multiplication of polynomials by scalars is a special case of the binary operation of multiplication of polynomials. A tedious checking of the many axioms shows that $\mathbb{C}[x]$ with the above algebraic binary operations is a $\mathbb{C}$-algebra. Its dimension as a vector space over $\mathbb{C}$ is ∞. The reader should check that the above binary operations (especially multiplication of polynomials) are the ones familiar from high school algebra. As remarked earlier, the $\mathbb{C}$-algebra $\mathbb{C}[x]$ is a subalgebra of $C_{\mathbb{C}}(\mathbb{C})$ the space of continuous complex valued functions of a complex variable. As such its study is also a part of analysis. The reader should be convinced that the formal operations of addition and multiplication of polynomials, do agree with the corresponding concepts when the polynomials are viewed as functions.

The function degree is a map

$$\deg : \mathbb{C}[x] \to \mathbb{Z}_{\geq 0} \cup \{-\infty\}.$$

The most important, for our applications, properties of this map are summarized in

THEOREM 5.16. *Let $a(x)$ and $b(x) \in \mathbb{C}[x]$. Then*
(a) $\deg\,(a(x)+b(x)) \leq \max\{\deg\,(a(x)), \deg\,(b(x))\}$, *and*
(b) $\deg\,(a(x)b(x)) = \deg\,(a(x)) + \deg\,(b(x))$.

PROOF. The proof is completely straight forward and hence left to the reader. We remark that in the arithmetic for $(\mathbb{Z}_{\geq 0} \cup \{-\infty\}, +.\cdot)$ that we are using $-\infty + a = -\infty$ for all $a \in \mathbb{Z}_{\geq 0} \cup \{-\infty\}$. □

REMARK 5.17. In our study of the integers, the absolute value was a useful tool in determining the size of an integer (in existence arguments, for example). We shall see that we can use the degree to assign a size to a polynomial in many arguments.

For each non-negative integer n, we let $\mathbb{C}_n[x]$ denote the set of polynomials of degree $\leq n$. It is clear that $\mathbb{C}_n[x]$ is a vector subspace of $\mathbb{C}[x]$ of dimension $n+1$ and that for all n and $m \in \mathbb{Z}_{\geq 0}$, the multiplication map

$$M : \mathbb{C}_n[x] \times \mathbb{C}_m[x] \to \mathbb{C}_{n+m}[x] \tag{18}$$

which assigns to each ordered pair $(p(x), q(x)) \in \mathbb{C}_n[x] \times \mathbb{C}_m[x]$ its product $p(x)q(x) \in \mathbb{C}_{n+m}[x]$ is a surjection.

A useful alternate form of writing (17) is

$$p(x) = \lambda\,(x-\alpha_1)\,...\,(x-\alpha_n), \tag{19}$$

with λ and the collection of $\alpha_i \in \mathbb{C}$. It is quite easy to go from (19) to (17):

$$a_j = (-1)^{n-j}\lambda \sum_{i_1 < i_2 ... i_{n-j}} \alpha_{i_1}\alpha_{i_2}...\alpha_{i_{n-j}},\ j = 0,\ 1,\ ...,\ n.$$

It is particularly easy to conclude that

$$a_0 = (-1)^n \lambda \alpha_1 \alpha_2 ... \alpha_n,\ a_{n-1} = -\lambda(\alpha_1 + \alpha_2 + ... \alpha_n),\ a_n = \lambda;$$

equations that will be used many times in the sequel.

The journey from (17) to (19) is not so quick and requires some very non-trivial mathematics, the Fundamental theorem of algebra discussed in Chapter 7.

EXERCISES

(1) Show that the the map M of (18) is surjective. Let $p(x) \in \mathbb{C}_{n+m}[x]$. Describe $M^{-1}(p(x))$.
HINT: You may (and probably should) use the Fundamental theorem of algebra.
(2) Let $a(x)$ and $b(x) \in \mathbb{C}[x]$. What happens if you try to divide the polynomial $b(x)$ by the polynomial $a(x)$? Is there a different answer if you assume that $a(x)$ and $b(x) \in \mathbb{Z}[x]$?

2.1. The vector space of polynomials of degree n. We are assuming that the reader has some familiarity with the concepts of linear algebra and use it to study in detail the vector space $\mathbb{C}_n[x]$, here n is an arbitraty non-negative integer. As we already observed this vector space (over $\mathbb{C}$) has dimension $n+1$. A convenient basis for $\mathbb{C}_n[x]$ consists of the $n+1$ vectors

$$1,\ x,\ x^2,\ ...,\ x^n.$$

The polynomial (17) can be represented by the column vector ($(n+1) \times 1$ matrix) with entries $a_0,\ a_1,\ ...,\ a_n$, and a *linear operator*

$$T : C_n[x] \to \mathbb{C}_m[x]$$

can be represented with respect to such bases by the an $(m+1) \times (n+1)$ matrix M_T whose j^{th} row is the vector $(\alpha_1, \alpha_2,\ ...,\ \alpha_{m+1})$ provided that the the operator T sends the vector $x^{j-1} \in \mathbb{C}_n[x]$ to the vector $\sum_{i=1}^{m+1} \alpha_i x^{j-1} \in \mathbb{C}_m[x]$. Thus the vector of coefficients of the image of the vector of coefficients $v \in \mathbb{C}^{n+1}$ of the vector $p(x) \in \mathbb{C}_n[x]$ is the vector $M_T v \in \mathbb{C}^{m+1}$. Review *linear operator*, *kernel* or *null space of an operator* and *image of an operator* as well as the

THEOREM 5.18. *Let L be a linear operator from a vector space V to a vector space W. Then the dimension of V equals the dimension of the kernel of L plus the dimension of its image (the vector space $L(V) \subseteq W$).*

2.2. The Euclidean algorithm (for polynomials). We start with

DEFINITION 5.19. Let $a(x)$ and $b(x) \in \mathbb{C}[x]$. We say that $a(x)$ *divides* $b(x)$ and write $a(x)|b(x)$ if there exists a $q(x) \in \mathbb{C}[x]$ such that $b(x) = a(x)q(x)$. We write in this case $q(x) = \frac{b(x)}{a(x)}$.

THEOREM 5.20 (The division algorithm). *Let $a(x)$ and $b(x)$ be polynomials and assume that $a(x)$ is not the zero polynomial (thus* deg $a(x) > -\infty$*). There exist unique polynomials $q(x)$ and $r(x)$ such that*
(a) $b(x) = a(x)q(x) + r(x)$, *and*
(b) deg $r(x) <$ deg $a(x)$.

PROOF. The reader should note the similarities of the statement and proof to those of Theorem 1.13 of Chapter 1. In each case we are dividing one quantity by second quantity to obtain a quotient and a remainder. The remainder should be "smaller" than the second quantity. The measurement of smallness in the case of integers was obvious; for polynomials, it is measured by the degree. Just like in the case of integers, the proof has two parts.

Existence: If $a(x)$ divides $b(x)$, set $q(x) = \frac{b(x)}{a(x)}$ and $r(x) = 0$.

Assume now that $a(x)$ does not divide $b(x)$. This forces the degree of $a(x)$ to be positive, Let

$$D = \{\text{deg } (b(x) - a(x)k(x)); \quad k(x) \in \mathbb{C}[x]\}.$$

We claim that $D \subseteq \mathbb{Z}_{\geq 0}$. For if there existsts a $k(x) \in \mathbb{C}[x]$ such that $b(x) - a(x)k(x) = 0$, then $a(x)$ would divide $b(x)$. Let d be the greatest lower bound for D. Then there exists a polynomial $q(x) \in \mathbb{C}[x]$ such that $r(x) = b(x) - a(x)q(x)$ has degree d. If $d = 0$, then ceratainly $d = \text{deg } r(x) < \text{deg } a(x)$. We claim that also if $d > 0$, then $d < \text{deg } a(x)$. So assume that $d > 0$. If $d \geq \text{deg } a(x)$, we write

$$r(x) = \alpha_0 x^d + \alpha_1 x^{d-1} + ... + \alpha_d, \quad \alpha_0 \neq 0$$

and

$$a(x) = \beta_0 x^n + \beta_1 x^{n-1} + ... + \beta_n, \quad \beta_0 \neq 0, \quad d \geq n.$$

Since

$$b(x) - a(x)\left[q(x) + \frac{\alpha_0}{\beta_0}x^{d-n}\right] = r(x) - a(x)\left[\frac{\alpha_0}{\beta_0}x^{d-n}\right] = \gamma_0 x^{d-1} + ... + \gamma_{d-1}$$

has non-negative degree $\leq (d-1)$, we have reached a contradiction to the fact that d is the smallest element of D.

Uniqueness: Write $b(x) = a(x)q(x) + r(x) = a(x)q_1(x) + r_1(x)$, where $q(x)$, $q_1(x)$, $r(x)$ and $r_1(x) \in \mathbb{C}[x]$, and also deg $r(x) <$ deg $a(x) >$ deg $r_1(x)$. Then

$$a(x)[q(x) - q_1(x)] = r_1(x) - r(x).$$

If $q(x) \neq q_1(x)$, then

$$\text{deg } (a(x)[q(x) - q_1(x)]) \geq \text{deg } (a(x))$$

while

$$\text{deg } (r_1(x) - r(x)) \leq \max\{\text{deg } (r_1(x)), \text{deg } (r(x))\} < \text{deg } (a(x));$$

which is impossible. Thus $q(x) = q_1(x)$ and hence also $r(x) = r_1(x)$. □

THEOREM 5.21. *Let $a(x)$ and $b(x)$ be polynomials and assume that not both of these are the zero polynomial. There exists a unique monic polynomial $d(x) = (a(x), b(x)) = \gcd(a(x), b(x))$ of degree ≥ 0 such that*
(a) *$d(x)|a(x)$ and $d(x)|b(x)$, and*
(b) *whenever $c(x) \in \mathbb{C}[x]$ divides both $a(x)$ and $b(x)$, it also divides $d(x)$.*

PROOF. We are again modeling our proof on the corresponding theorem for the integers. Let

$$\mathcal{D} = \{a(x)s(x) + b(x)t(x); s(x) \text{ and } t(x) \in \mathbb{C}[x] \text{ and } a(x)s(x) + b(x)t(x) \neq 0\}.$$

The set $\mathcal{D}$ is not empty (it contains either $a(x)$ or $b(x)$). Let

$$D = \{d \in \mathbb{Z};\ d = \text{deg } (p(x)) \text{ for some } p(x) \in \mathcal{D}\}.$$

The set D is not empty because $\mathcal{D}$ is not and does not contain $-\infty$ because $0 \notin \mathcal{D}$. Hence D is a non-empty set of integers that is bounded from below (by 0). It hence contains a smallest (non-negative) element δ. We can thus find a monic polynomial $d(x) = a(x)s_o(x) + b(x)t_o(x) \in \mathcal{D}$ whose degree is δ ($d(x)$ cannot be the zero polynomial).

The proof of (b) is rather simple. We first note that $c(x) \neq 0$ as otherwise both $a(x) = 0 = b(x)$. Obviously $c(x)$ divides $d(x) = a(x)s_o(x) + b(x)t_o(x)$.

We proceed to the proof of (a). By the division algorithm $a(x) = d(x)q(x) + r(x)$ where $r(x)$ and $q(x) \in \mathbb{C}[x]$ with $\deg(r(x)) < \delta = \deg(d(x))$. Thus

$$r(x) = a(x) - d(x)q(x) = a(x) - q(x)[a(x)s_o(x) + b(x)t_o(x)]$$

$$= a(x)[1 - q(x)s_o(x)] + b(x)[-q(x)t_o(x)],$$

and if $r(x)$ were not the zero polynomial, it would certainly belongs to $\mathcal{D}$. Since the degree of $r(x)$ is smaller than δ (which is the minimum of the degrees of the polynomials in $\mathcal{D}$), $r(x) = 0$. This shows of course that $d(x)$ divides $a(x)$. The argument that $d(x)|b(x)$ is similar. We have established existence.

For uniqueness assume that the monic polynomial d_1 also satisfies conditions (a) and (b). We use (a) for $d_1(x)$ to conclude that it divides both $a(x)$ and $b(x)$. Now we use (b) for $d(x)$ with $c(x) = d_1(x)$ to conclude that $d_1(x)|d(x)$. Similarly $d(x)|d_1(x)$. Since both $d(x)$ and $d_1(x)$ are monic polynomials, we conclude that $d(x) = d_1(x)$. □

Definition 5.22. As with integers, we call $d(x)$, *the greatest common divisor (gcd)* of $a(x)$ and $b(x)$ and say that $a(x)$ and $b(x)$ are *relatively prime* if $d(x) = 1$. As with integers, we define $(0, 0) = 0$.

Corollary 5.23 (of proof). *For all $a(x)$ and $b(x) \in \mathbb{C}[x]$, $(a(x), b(x))$ is a linear combination of $a(x)$ and $b(x)$; that is, there exist $s(x)$ and $t(x) \in \mathbb{C}[x]$ such that*

$$(a(x), b(x)) = a(x)s(x) + b(x)t(x).$$

Remark 5.24. The above corollary does not tell us how to compute $(a(x), b(x))$ as a linear combination of $a(x)$ and $b(x)$. THE GCD ALGORITHM of section 3 of Chapter 1 works for complex polynomials

Instead of describing the general algorithm, we illustrate (using notation that is a straight forward translation of the algorithn for integers) with an example of two poynomials $a(x) = x^3 - 3x^2 + 2x$ and $b(x) = 2x^2 - 6x$. To give us confidence in our calculation, we use the fundamental theorem of algebra to factor the polynomials:

$$a(x) = x(x-1)(x-2), \quad b(x) = 2x(x-3).$$

The factored forms of the two polynomials tell us immediately that $(a(x), b(x)) = x$. The algorithm (without taking advantage of the factorization which is not needed) now reads

$$\left[\begin{array}{cc|c} 1 & 0 & x^3 - 3x^2 + 2x \\ 0 & 1 & 2x^2 - 6x \end{array}\right] \xrightarrow{\frac{1}{2}x} \left[\begin{array}{cc|c} 1 & -\frac{1}{2}x & 2x \\ 0 & 1 & 2x^2 - 6x \end{array}\right] \to \left[\begin{array}{cc|c} \frac{1}{2} & -\frac{1}{4}x & x \\ 0 & \frac{1}{2} & x^2 - 3x \end{array}\right].$$

As is the case with the earlier version of this algorithm, the arrows need not alternate between the rows of matrices; whereas it was convenient to use this alternating convention when dealing with integers, it may not be when dealing with polynomials – the aim in this case is to continue reducing the degrees of the polynomials appearing un the last columns of

the matrices. The meaning of the last arrow should be obvious to the reader. We conclude from the above calculations that

$$x = (a(x), b(x)) = \frac{1}{2}(x^3 - 3x^2 + 2x) - \frac{1}{4}x(2x^2 - 6x);$$

as can easily be checked. As we have pointed out, we need not the use the fundamental theorem of algebra to factor the polynomials nor do we need to know what the gcd is in order to compute it. We compute the gcd of a second set of two polynomials:

$$a(x) = x^3 - 3x^2 + 2x, \quad b(x) = x^4 - 5x^3 + 7x^2 - 3x.$$

It is completely obvious that $x|(a(x), b(x))$; but of course other monic polynomials of degree 1 may also divide $(a(x), b(x))$. The algorithm reads

$$\left[\begin{array}{cc|c} 1 & 0 & x^4 - 5x^3 + 7x^2 - 3x \\ 0 & 1 & x^3 - 3x^2 + 2x \end{array}\right] \stackrel{x}{\to} \left[\begin{array}{cc|c} 1 & -x & -2x^3 + 5x^2 - 3x \\ 0 & 1 & x^3 - 3x^2 + 2x \end{array}\right]$$

$$\stackrel{-2}{\to} \left[\begin{array}{cc|c} 1 & -x+2 & -x^2 + x \\ 0 & 1 & x^3 - 3x^2 + 2x \end{array}\right] \stackrel{-x}{\to} \left[\begin{array}{cc|c} 1 & -x+2 & -x^2 + x \\ x & -x^2 + 2x + 1 & -2x^2 + 2x \end{array}\right].$$

It is now easily concluded that

$$x(x-1) = (a(x), b(x)) = (-1)(x^4 - 5x^3 + 7x^2 - 3x) + (x-2)(x^3 - 3x^2 + 2x);$$

LEMMA 5.25. *Let $a(x)$ and $b(x) \in \mathbb{C}[x]$, and assume that $b(x) = a(x)q(x) + r(x)$ for some $q(x)$ and $r(x) \in \mathbb{C}[x]$. Then $(a(x), b(x)) = (a(x), r(x))$.*

PROOF. Let $d(x) = (a(x), b(x))$. If $d(x) = 0$, then $a(x) = 0 = b(x)$ and there is nothing to prove. So assume that $d(x) \neq 0$. In this case, $d(x)|r(x)$ and thus $d(x)|(a(x), r(x))$. But also $(a(x), r(x))|b(x)$ and $(a(x), r(x))|a(x)$; hence $(a(x), r(x))|d(x)$ and thus $(a(x), r(x)) = d(x)$. □

THEOREM 5.26 (The Euclidean algorithm). *Let $a(x)$ and $b(x) \in \mathbb{C}[x]$ with $a(x) \neq 0$. Then there exists a unique $n \in \mathbb{N}$, unique $r_1(x), r_2(x), ..., r_n(x) \in \mathbb{C}[x]$ and unique $q_1(x), q_2(x), ..., q_n(x), q_{n+1}(x) \in \mathbb{C}[x]$ such that*

$$\begin{aligned} b(x) &= a(x)q_1(x) + r_1(x), \ 0 \leq \deg\,(r_1(x)) < \deg\,(a(x)) \\ a(x) &= r_1(x)q_2(x) + r_2(x), \ 0 \leq \deg\,(r_2(x)) < \deg\,(r_1(x)) \\ r_1(x) &= r_2(x)q_3(x) + r_3(x), \ 0 \leq \deg\,(r_3(x)) < \deg\,(r_2(x)) \\ &\cdot \\ &\cdot \\ &\cdot \\ r_{n-2}(x) &= r_{n-1}(x)q_n(x) + r_n(x), \ 0 \leq \deg\,(r_n(x)) < \deg\,(r_{n-1}(x)) \\ r_{n-1}(x) &= r_n(x)q_{n+1}(x) \end{aligned}$$

and $(a(x), b(x)) = r_n(x)$.

PROOF. The existence and uniqueness of n, and the existence and properties of the collections of $r_i(x)$ and $q_i(x)$ follow from the division algorithm. The last lemma tells us that

$$(b(x), a(x)) = (a(x), r_1(x)) = (r_1(x), r_2(x)) = ... = (r_{n-2}(x), r_{n-1}(x)) = (r_{n-1}(x), r_n(x)) = r_n(x).$$

□

2.3. Differentiation.

DEFINITION 5.27. We define formally the *derivative*, $p'(x)$ of the polynomial $p(x)$ of (17) as the polynomial

$$p'(x) = a_1 + 2a_2x + ... + na_nx^{n-1}.$$

For each non-negative integer k, the k^{th} derivative $p^{(k)}(x)$ of the polynomial $p(x)$ is defined inductively by $p^{(0)}(x) = p(x)$ and $p^{(k+1)}(x)$ is the derivative of $p^{(k)}(x)$. Note that the n^{th} derivative of an n^{th} degree polynomial is a non-zero constant, while for each $m > n$, its m^{th} derivative is zero.

THEOREM 5.28 (Taylor series). *Let $p(x)$ be an n^{th} degree polynonial, then for all z_o and $\Delta \in \mathbb{C}$*

$$p(z_o + \Delta) = p(z_o) + p'(z_o)\Delta + \frac{p^{(2)}(z_o)}{2!}\Delta^2 + ... + \frac{p^{(n)}(z_o)}{n!}\Delta^n.$$

PROOF. The proof is a long calculation using the binomial theorem that is left to the reader. Note that we claim here that the proof is formal calculation that does not require any analysis. □

As an illustration of the power of formal calculations and because it will be needed in the section on multiple roots, we establish the following

THEOREM 5.29. *Let $p(x)$, $q(x)$ and $r(x)$ be three polynomials with $r(x) = p(x)q(x)$. Then*

$$r'(x) = p'(x)q(x) + p(x)q'(x).$$

PROOF. In the arguments that follow, we have ignored the indeces of summation, and coefficients indexed by a negative integer should be taken as zero. Let

$$p(x) = \sum_i a_i x^i,\ q(x) = \sum_i b_i x^i \text{ and } r(x) = \sum_i c_i x^i,$$

Then

$$p'(x) = \sum_i i a_i x^{i-1},\ q'(x) = \sum_i i b_i x^{i-1},\ r'(x) = \sum_i i c_i x^{i-1}$$

and

$$c_i = \sum_j a_j b_{i-j}.$$

Write

$$p'(x)q(x) + p(x)q'(x) = \sum_i d_i x_i.$$

We compute d_i. From the last equation, it follows that

$$d_i = \sum_j \left((j+1)a_{j+1}b_{i-j} + (i-j+1)a_j b_{i-j+1}\right). \tag{20}$$

We need to establish that

$$d_i = (i+1)c_{i+1} = (i+1)\sum_j a_j b_{i+1-j};$$

which follows upon rewriting (20) as

$$d_i = \sum_j (j+1)a_{j+1}b_{i-j} + \sum_j (i-j)a_{j+1}b_{i-j} = \sum_j (i+1)a_{j+1}b_{i-j} = (i+1)\sum_j a_j b_{i-(j-1)}.$$

□

EXERCISES

(1) Let n be a positive integer, and let $p(x)$, $p_1(x)$, ... $p_n(x)$ be a collection of $n+1$ polynomials with

$$p(x) = \prod_{i=1}^{n} p_i(x).$$

Show that

$$p'(x) = \sum_{j=1}^{n} \prod_{i=1}^{n} q_{ij}(x),$$

where

$$q_{ij}(x) = \begin{cases} p_i(x) \text{ for } i \neq j \\ p_i'(x) \text{ for } i = j \end{cases}.$$

(2) Let n be a positive integer. We study the *differential* operator

$$D : \mathbb{C}_{n+1}[x] \to \mathbb{C}_n[x]$$

defined by sending the polynomial $p(x)$ to the polynomial $p'(x)$, and the *integral* operator

$$I : \mathbb{C}_n[x] \to \mathbb{C}_{n+1}[x]$$

defined by sending the polynomial $a_n x^n + a_{n-1}x^{n-1} + ... + a_0$ to the polynomial $\frac{a_n}{n+1}x^{n+1} + \frac{a_{n-1}}{n}x^n + ... + a_0 x$.

- Show that D and I are linear operators.
- Show that D is surjective and that I is injective.
- Show that
$$I \circ D : \mathbb{C}_n[x] \to \mathbb{C}_n[x]$$
has a one dimensional kernel. What is the image of this operator?
- Show that
$$D \circ I : \mathbb{C}_n[x] \to \mathbb{C}_n[x]$$
is the identity operator.
- Does there exist a linear operator
$$T : \mathbb{C}_n[x] \to \mathbb{C}_{n+1}[x]$$
such that $T \circ D$ is the identity?

3. Ideals

3.1. Ideals in commutative rings. Let $(R, +, \cdot)$ be a commutative ring and $I \subseteq R$ a subring. We would like to give the additive cosets

$$R/I = \{a + I; a \in R\}$$

a *quotient* ring structure. Let a and $b \in R$. From our work on quotient groups, we know that R/I is an abelian group; addition is, of course, defined by

$$(a + I) + (b + I) = (a + b) + I.$$

We try to define multiplication anologously by

$$(a + I)(b + I) = (ab) + I.$$

We must verify that this is a well defined operation. Toward this end, let a' and $b' \in R$ be such that $a - a'$ and $b - b' \in I$. We need to verify that $a'b' - ab \in I$. We try to do so by observing that

$$a'b' - ab = a'b' - a'b + a'b - ab = a'(b' - b) + (a' - a)b.$$

We know that $(b' - b)$ and $(a' - a) \in I$. But since we only know that a' and $b \in R$ (not I), we are unable to conclude that $a'(b' - b)$ and $(a' - a)b \in I$ (which would conclude the proof that multiplication is well defined). Try as one might, there is no way out of this difficulty without some addtional assumption on I.

DEFINITION 5.30. A non-empty subset I of a commutative ring R is an *ideal* provided:
(a) for all a and $b \in I$, $(a - b) \in I$, and
(b) for all $a \in I$ and all $r \in R$, $ar \in I$.

REMARK 5.31.
- Every commutative ring R that contains 2 or more elements has two ideals: the *trivial* ideal $\{0\}$ and the *unit* ideal R. An ideal $I \subset R$ is called *proper*.
- Ideals need not be subrings since they need not contain 1.
- If an ideal I in R contains an invertible element (then it must also contain 1) of R, then $I = R$.
- If I is a proper ideal in the commutative ring R, then R/I is a commutative ring known as *quotient ring* .
- For every commutative ring R, $R/\{0\} = \{R\}$ and $R/R = \{0\} = \{0 + R\}$. The latter is, of course, not a ring in our definition since it does not contain 1.
- Ideal may also be defined for non-commutative rings. In this case one needs to distinguish three classes of ideals: left, right and two sided.
- If I_1 and I_2 are ideals in the commutative ring R, then so is

$$I_1 + I_2 = \{a \in R;\ a = a_1 + a_2 \text{ with } a_i \in I_i\}.$$

DEFINITION 5.32. Let R be a commutative ring and $a \in R$, the *principal* ideal *generated* by a is defined by

$$< a >= Ra = \{ra;\ r \in R\}.$$

More generally, assume that for some positive integer n, $a_1, ..., a_n \in R$. The ideal *generated* by $a_1, ..., a_n$ is

$$< a_1, ..., a_n >= a_1R + ... + a_nR = \{r_1a_1 + ... + r_na_n;\ r_i \in R \text{ for } i = 1, ..., n\}.$$

The proof that $a_1R + ... + a_nR$ is an ideal is elementary. Let $r_1a_1 + ... + r_na_n$ and $r'_1a_1 + ... + r'_na_n \in a_1R + ... + a_nR$. Then

$$(r_1a_1 + ... + r_na_n) - (r'_1a_1 + ... + r'_na_n) = (r_1 - r'_1)a_1 + ... + (r_n - r'_n)a_n \in a_1R + ... + a_nR$$

and if $r \in R$, then

$$r(r_1a_1 + ... + r_na_n) = (rr_1)a_1 + ... + (rr_n)a_n \in a_1R + ... + a_n.$$

PROPOSITION 5.33. *Let $\theta : R \to S$ be a ring homomorphism. Then*
(a) $\ker(\theta) = \{r \in R; \theta(r) = 0\}$ *is an ideal in R,*
(b) $\mathrm{Im}(\theta)$ *is a subring of S,*
(c) $\ker(\theta) = \{0\}$ *if and only if θ is injective, and*
(d) θ *is injective whenever R is a field.*

EXAMPLE 5.34. We discuss three important examples.

- $(\mathbb{Z}, +, \cdot)$ is a subring, hence a subgroup, of $(\mathbb{Z}[x], +\cdot)$, with respect to the additive structures. But the two groups are not isomorphic. In this case, we can determine all group homomorphisms $\theta : (\mathbb{Z}, +) \to (\mathbb{Z}[x], +)$. The group $\mathbb{Z}$ is cyclic with generator 1. Hence $\theta(\mathbb{Z})$ is cyclic with generator $\theta(1)$. But $\mathbb{Z}[x]$ is certainly not a cyclic group.
- $\mathbb{Z}$ is a subring of $\mathbb{Z}[\sqrt{2}]$, but not an ideal.
- Let $p(x)$ be a monic polynomial in $\mathbb{C}[x]$ of degree $n > 0$. Let I be the principal ideal $(p(x))$. Then the quotient ring $\mathbb{C}[x]/I$ is isomorphic as a vector space to $\mathbb{C}_{n-1}[x]$. Each equivalence class $Q(x) + I \in \mathbb{C}[x]/I$ has a canonical representative as a polynomial $q(x)$ of degree $\leq (n-1)$. To verify the last claim assume that the degree of $Q(x) = ax^m + ...$ is $m \geq n$, then $Q(x) - ax^{m-n}p(x)$ is equivalent to $Q(x)$ and has degree and most $m-1$. If $m - 1 < n$ we are done. Otherwise, we iterate the procedure and eventually find a plynomial $q(x)$ of degree at most $n-1$ that is equivalent to $Q(x)$. It is clear that two distinct polynomials of degree $\leq (n-1)$ cannot be equivalent modulo the ideal I (their difference cannot belong to I). This example introduces a multiplication structure on polynomials of degree $\leq (n-1)$ that is very different from the multiplicative stucture on $\mathbb{C}[x]$
- We continue with the last example with $p(x) = x^3 - 1$. Here the multiplication (in terms of canonical representatives for equivalence classes) yields

$$(a_0+a_1x+a_2x^2)(b_0+b_1x+b_2x^2) = (a_0b_0+a_1b_2a_2b_1)+(a_1b_0+a_0b_1+a_2b_2)x+(a_2b_0+a_1b_1+a_0b_2)x^2.$$

3.2. Ideals in $\mathbb{Z}$ and $\mathbb{C}[x]$.

PROPOSITION 5.35. *Every ideal I in $\mathbb{Z}$ is principal.*

PROOF. If I is the trivial ideal $(< 0 >)$ or the unit ideal $(< 1 >= \mathbb{Z})$, it is certainly principal. Assume now that I is not the trivial ideal. It thus contains an integer $a \neq 0$. If $a < 0$, then I also contains $(-1)a > 0$. Thus the set of integers $S = \{b \in I; b > 0\}$ is non-empty and bounded from below and hence contains a smallest element d. We claim that $I =< d >$. Because $d \in I$, it follows the $< d >= d\mathbb{Z} \subseteq I$. Conversely, if $c \in I$, then by the division algorithm $c = qd + r$ for some q and $r \in \mathbb{Z}$ with $0 \leq r < d$. Hence $r \in I$. If $r \neq 0$, then it would also belong to S which would contradict that d was the smallest element of S. We conclude that $c \in < d >$ and hence $I \subseteq < d >$. □

PROPOSITION 5.36. *Every ideal I in $\mathbb{C}[x]$ is principal.*

PROOF. If I is the trivial ideal $(< 0 >)$ or the unit ideal $(< 1 >= \mathbb{C}[x])$, it is certainly principal. Assume now that I is not the trivial ideal nor the unit ideal. Let D be the set of degrees of the non-zero elements of I. It is a non-empty subset of $\mathbb{N}$. It thus contains a smallest integer $d \neq 0$. If $d = 0$, then I would contain a non-zero constant and would hence be a the unit ideal. Thus there is a polynomial $d(x)$ of degree d in I. We claim that $I =< d(x) >$. Because $d(x) \in I$, it follows that $< d(x) >= d(x)\mathbb{C}[x] \subseteq I$. Conversely, if $p(x) \in I$, then by the division algorithm $p(x) = q(x)d(x)+r(x)$ for some $q(x)$ and $r(x) \in \mathbb{C}[x]$ with $r(x) = 0$ or $0 \leq \deg(r(x)) < d$. Now $r(x) \in I$. If $r(x) \neq 0$, then its degree would belong to D and would be smaller than d. This contradiction shows that $r(x) = 0$ and hence that $p(x) \in < d(x) >$. Thus $I \subseteq < d(x) >$. □

DEFINITION 5.37. A proper ideal I in a commutative ring R is a *prime* ideal if for all a and $b \in R$, $ab \in I$ implies that either a or $b \in I$, and is a *maximal* ideal if whenever N is another proper ideal with $I \subseteq N \subset R$, then $I = N$.

REMARK 5.38. The following assertions are easily established.

- An ideal I in a commutative ring R is maximal if and only if R/I is a field.
- An ideal I in R is prime if and only if R/I is an integral domain.

  PROOF. As an illustration, we provide a proof of this (and part of the next) assertion. Say I is a prime ideal . Let a and $b \in R$ if $(a+I)(b+I) = I$, then $ab \in I$ and hence either a or b must be in I and thus either $a+I$ or $b+I$ is the zero element of R/I. Conversely, if $ab \in I$, then either $a+I$ or $b+I$ is the zero element of R/I and hence either a or $b \in I$. □

- Every maximal ideal is prime. The converse is false.

  PROOF. We verify only the first claim. Let I be a maximal ideal in the ring R. Then R/I is a field, hence certainly an integral domain. Hence I is a prime ideal. □

THEOREM 5.39. (a) *An ideal* $< d >$ *in the integers* $\mathbb{Z}$ *is prime if and only if* d *or* $-d$ *is.*
(b) *An ideal* $< d(x) > \subset \mathbb{C}[x]$ *is prime if and only if* $d(x) = \alpha x + \beta$, *with* $\alpha \in \mathbb{C}_{\neq 0}$ *and* $\beta \in \mathbb{C}$.
(c) *An ideal* $I \subset \mathbb{Z}$ *or* $\subset \mathbb{C}[x]$ *is prime if and only if it is maximal .*

PROOF. *(a)* Without loss of generality, d is a positive integer. Assume that $< d >$ is a prime ideal. If d were not a prime integer, we could certainly find integers a and $b \in \mathbb{Z}$ such that d divides the product ab, but d does not divide either a or b. But then $ab \in I =< d >$ implies that either a or $b \in I$. Thus d divides either a or b. This contradiction establishes that d is a prime. We leave the proof of the converse as an exercise.
(b) We use the fundamental theorem of algebra (to be established in Chapter 7) to conclude that the principal ideal $< d(x) >$ is prime if and only if $d(x)$ is a polynomial of degree one.
(c) This is an imediate consequence of the fact that all ideals in either $\mathbb{Z}$ or $\mathbb{C}[x]$ are principal. □

EXERCISES

(1) Let d be a prime integer. Prove that $< d >$ is a prime ideal in $\mathbb{Z}$.
(2) Prove that an ideal in $\mathbb{Z}$ or in $\mathbb{C}[x]$ is prime if and only if it is maximal.
(3) Exhibit some of the differences between $\mathbb{Z}[x]$ and $\mathbb{C}[x]$.
(4) Prove that for every positive integer n, the quotient ring $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to the ring $\mathbb{Z}_n$.
(5) Compute the gcd of the polynomials $x^4 + 1$ and $x^3 + 1$.
(6) Let n be a positive integer. Define the gcd $d(x)$ of n polynomials $p_1(x)$, $p_2(x)$, ..., $p_n(x) \in \mathbb{C}[x]$ and show the that the ideal generated by these polynomials is the principal ideal generated by the gcd.
(7) Describe all homomorphisms θ from the integers $(\mathbb{Z}, +)$ to an arbitrary group. In particular, is $\theta(\mathbb{Z})$ cyclic and what are the possible orders of such groups?

4. CRT revisited

THEOREM 5.40 (The Chinese remainder theorem). *Let* $m_1,\ m_2,\ ...,\ m_r$ *be* $r > 0$ *relatively prime positive integers. The map*

$$\theta : \mathbb{Z}_{m_1 m_2 ... m_r} \to \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times ... \times \mathbb{Z}_{m_r}$$

defined by

$$\theta\left([a]_{m_1 m_2 ... m_r}\right) = \left([a]_{m_1}, [a]_{m_2},\ ...\ [a]_{m_r}\right)$$

is a ring isomorphism.

PROOF. We need to show that θ is well defined and a ring isomorphism. The map is well defined: if for a and $b \in \mathbb{Z}$, we have that $[a]_{m_1 m_2 \ldots m_r} = [b]_{m_1 m_2 \ldots m_r}$, then for each i, $[a]_{m_i} = [b]_{m_i}$. It is clear that θ preserves additive and multiplicative structures of the respective rings and is thus a ring homomorphism. The map θ is injective: if for a and $b \in \mathbb{Z}$ and for each i we have that $[a]_{m_i} = [b]_{m_i}$, then $(a-b)|m_i$ and hence $(a-b)|m_1 m_2 \ldots m_r$. The surjectivity of the map θ is a set theoretic consequence of two facts: (1) the map is injective and (2) $|\mathbb{Z}_{m_1 m_2 \ldots m_r}| = |\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \ldots \times \mathbb{Z}_{m_r}|$. □

REMARK 5.41. We discuss some connections to previous results (that such connections must exist is implied by the name of the theorem, for example).

- Unlike the earlier version of the Chinese remainder theorem (Theorem 1.70), the above proof produces the existence of the solution, but does not provide an algorithm for finding it.
- Recall Theorem 4.37.

EXERCISES

(1) Supply the details to show that the map θ of the last theorem preserves both the additive and multiplicative structures.
(2) Construct an inverse for the map θ.

5. Polynomials over more general fields

Throughout this section K is field that contains $\mathbb{Q}$ and is contained in $\mathbb{C}$. All of our work on $\mathbb{C}[x]$, in the previous sections, that does not involve the fundamental theorem of algebra applies to $K[x]$. In this section we explore some of the differences, especially concepts needed in Chapter 9. As usual, we start with a

DEFINITION 5.42. Let $p(x) \in K[x]$ have positive degree. We say that the polynomial $p(x)$ is *irreducible over* K if given a *factorization* $p(x) = f(x)g(x)$ with $f(x)$ and $g(x) \in K[x]$, then either $f(x)$ or $g(x) \in K$ (that is, at least one of them must have degree 0).

REMARK 5.43. The concept of irreducibility depends on the field K.

- Over $\mathbb{C}$, the only polynomials of positive degree that are irreducible are those of degree one (by the fundamental theorem of algebra).
- The polynomial of degree two $x^2 + 1$ is irreducible over $\mathbb{R}$.

THEOREM 5.44. *Every polynomial in $K[x]$ of positive degree can be expressed as a product of a constant $\lambda \in K$ and irreducible monic polynomials $p_1(x)$, ..., $p_r(x) \in K[x]$. In such a product, the constant and polynomials are uniquely determined up to rearrangement.*

DEFINITION 5.45. A field K is *algebraically closed* if every polynomial in $K[x]$ of positive degree has a root in K.

COROLLARY 5.46. *If K is algebraically closed, then every $p(x) \in K[x]$ of positive degree n has a factorization* (19). *The constant $\lambda \in K$ is unique; so are the roots α_i, up to rearrangement.*

REMARK 5.47.

- The field of complex numbers $\mathbb{C}$ is algebraically closed as a result of the fundamental theorem of algebra (discussed in Chapter 7), but $\mathbb{Q}$ and $\mathbb{R}$ are not.

- Finite dimensional vector spaces over the field with two elements $\mathbb{Z}_2$ will be important in our study of error correcting codes in Chapter 6.
- For an arbitrary commutative ring R, we can form its polynomial ring $R[x]$. It is easy to see that $R[x]$ is an integral domain whenever R is.

6. Fields of quotients and rings of rational functions

In Sub-section 5.1 of Chapter 1 we discussed the construction of the rationals from the integers. That construction is quite general.

DEFINITION 5.48. Let R be an integral domain. We introduce an equivalence relation $\equiv$ on $S = R \times R_{\neq 0}$ by declaring (a, b) to be *equivalent* to (α, β) provided $a\beta = b\alpha$; we write $\frac{a}{b}$ as a representative for the equivalence class of $(a, b) \in R \times R_{\neq 0}$. We let Q be the set of equivalence classes so obained and call it the *field of quotients* of R. Addition $+$ and multiplication $\cdot$ in Q are defined as in the construction of $\mathbb{Q}$ from $\mathbb{Z}$.

PROPOSITION 5.49. (a) $(Q, +, \cdot)$ *is a field.*
(b) *The map θ that sends $a \in R$ to $\frac{a}{1} \in Q$ is an injective ring homomorphism. We identify R with $\theta(R)$ and can hence view it as a subring of the field Q.*
(c) *If a and $b \in R$ with b invertible, then $\frac{a}{b} = ab^{-1}$.*

For an arbitrary commutatine ring R, we have defined a polynomial ring $R[x]$. We can also define the *ring of rational functions* $R(x)$ as the set of formal expressions $\rho(x) = \frac{p(x)}{q(x)}$ with $p(x)$ and $q(x) \in R[x]$ and $q(x) \neq 0$. We can define the binary operations $+$ and $\cdot$ on $R(x)$ that extend the corresponding operations on $R[x]$and turn $R(x)$ into a commutative ring. We can thus view $R[x]$ as a subring of $R(x)$ and also view ρ as a function from $R_{q(r)\neq 0}$ to R.

In the most interesting cases R is an integral domain and we can form the field of quotients Q_1 of the integral domain $R[x]$ as well as the field of quotients Q_2 of the integral domain $R(x)$. We can also construct the field of quotients Q of R and hence also $Q[x]$ and $Q(x)$. One checks at this point that the various constructions are related. In particular, the field of quotients of Q_1, Q_2 and $Q(x)$ are more or less the same object.

CHAPTER 6

Error correcting codes

We apply the material we have developed to study error detecting and error correcting codes.

1. ISBN

A code is just a number. We have discussed methods for transmitting codes that can not be deciphered by un-authorized listeners. We now turn to a different issue. How can the receiver be sure that the information received is identical with that sent? And if there is a transmission error, how can it be corrected? To what degree of certainty? We start with a discussion of

EXAMPLE 6.1. The International Standard Book Number (ISBN) is a sequence of nine integers $a_1a_2...a_8a_9$, where $0 \leq a_i \leq 9$, for each i, together with a *check digit* a (thus $a_1a_2...a_8a_9a$), where a is either an integer between 0 and 9 (inclusive) or the symbol X which stands for the integer 10. The inclusion of this 10-th digit gives a check on the other 9. It is constructed as the representative of the congruence class of

$$-(10a_1 + 9a_2 + ... + 3a_8 + 2a_9) = -\sum_{i=1}^{9}(11-i)a_i \mod 11$$

chosen, as usual (for us), between the integers 0 and 10 (inclusive). If a_i is erroneously transmitted as β instead of its correct value α, and all the other digits, including the check digit, are transmitted correctly, then the receiver computes as check digit $y = a - (11 - i)(\beta - \alpha) \mod 11$ and since 11 is prime and

$$11 - i \not\equiv 0 \mod 11 \text{ and } (\beta - \alpha) \not\equiv 0 \mod 11,$$

we see that also $(11 - i)(\beta - \alpha) \not\equiv 0 \mod 11$. Thus $y \neq a$ and the receiver knows that there is an error in the transmission. What the receiver does NOT know is which digit is wrong. It could, of course, be the check digit. Similarly, if the sender interchanges a_i with a_j and say that $1 \leq i, j \leq 9$, then the receiver computes $-(11 - i)a_j - (11 - j)a_i$ instead of $-(11 - i)a_i - (11 - j)a_j$ as the contribution of these two terms to the check digit. The difference

$$-(11-i)(a_j - a_i) - (11-j)(a_i - a_j) = (i-j)(a_j - a_i)$$

is congruent to $0 \mod 11$) if and only $a_i = a_j$, and again a single error is detected.

2. Groups and codes

Codes and information, in general, are usually transmitted in binary rather than decimal mode (notation). Thus a message is a finite set of zeros and ones; for example, 00011 or 10100.

DEFINITION 6.2. We fix a positive integer n. A *word of length* n is a point in $\mathbb{Z}_2^n$. We write such a word as $a = a_1a_2...a_n$, where each a_i is either 0 or 1.

REMARK 6.3. The simplest finite field with two elements $(\mathbb{Z}_2, +, \cdot)$ has lots of structure. We will denote from now on by $\mathbf{B}$. In particular, we fix a positive integer n and study $\mathbf{B}^n$ the abelian group (under addition) of order 2^n; it is also a vector space over $\mathbf{B}$ of dimension n. (We will not use this additional structure nor that it is a Boolean algebra[1].) The addition table for the group $\mathbf{B}^n$ is rather simple: if the element $b \in \mathbf{B}^n$ is the n-tuple $b_1b_2...b_n$, then $a + b$ is the n-tuple $c_1c_2...c_n$ where, $c_i = 0$ if and only if $a_i = b_i$. Thus each element of this group is its own inverse. The (scalar) product of the scalar $\lambda \in \mathbf{B}$ with the vector $w \in \mathbf{B}^n$ is also quite simple:

$$\lambda w = \begin{cases} 0 \text{ if } \lambda = 0 \\ w \text{ if } \lambda \neq 0 \end{cases} .$$

To formalize the concept of check-digits, we consider a word w of positive length m and transmit instead a *code word* $f(w)$ of length n which should have redundant information to enable us to detect and perhaps correct transmission errors. We thus are considering a *coding* function

$$f : \mathbf{B}^m \to \mathbf{B}^n.$$

Whenever necessary we have at our disposal a list of all possible code words.

In order for the coding function to enable us to recover the original word w from the code word $f(w)$, it is necessary that f be an injective mapping; in particular, that $n \geq m$. In practice we take $n > m$. WE ASSUME FROM NOW ON THAT f IS INJECTIVE AND THAT $n > m$. In practice there is a necessary trade off; the bigger n is, the more redundancy we have, the easier it should be to catch errors and correct mistakes, however, it is more expensive to transmit longer messages.

EXAMPLE 6.4. We begin by considering prototypes for the two simplest examples of coding functions.

- We take $n = m + 1$ and define $f(w) = wx$, where for $w = a_1a_2...a_m$, $x = \sum_{i=1}^{m} a_i$, where the sum is evaluated in $\mathbf{B}$. Thus the check digit x is 0 if the number of non-zero digits in the word w is even and 1 otherwise. If exactly one error is made in transmission, it will certainly be detected. But we cannot correct it, since we do not know where it is – it might be the check digit (so the message we receive, wx with x stripped from it) is correct although we cannot be sure of it[2]. In general this coding function will detect an odd number of transmission errors – but not an even number. How bad is this? Assume the probability p of a transmission error in any single digit is 1 in a 1000 (.001 or 10^{-3}). (In practice it is much smaller.) If our word w is of length five ($m = 5$), then the probability of precisely 2 transmission errors is $\begin{pmatrix} 6 \\ 2 \end{pmatrix} (.001)^2(.999)^4 = .0000149...$, much smaller than the probability of precisely one error $6(.001)(.999)^5 = .00597....$
- Let us now take $n = 3m$ and define $f(w) = www$. When we receive a code word (of length $3m$) we break it up into 3 words of length m: abc. If $a = b = c$ we can be fairly certain but not sure that $w = a$. Say that one mistake was made

[1]We have not defined this structure.

[2]Even if the check digit shows no obvious errors, there may be some.

in the transmission of a and then the same mistake was made in the transmission of b and c. What is the probability of this happening. Using the same set of values for m and p as in the previous example, we evaluate this probability as $5\left((.001)(.999)^4\right)^3 = .0000\ 0000\ 49...$; quite an unlikely event.

- We will use the next two examples in much of our subsequent development. We will hence refer to them in the sequel as *standard small examples* 1 and 2, respectively. We use $m = 4$ in the first of these and add a check digit before transmitting the word. The transition from word to code word in the second example will be explained later. For these examples, we consider the maps $f : \mathbf{B}^4 \to \mathbf{B}^5$ and $g : \mathbf{B}^3 \to \mathbf{B}^6$ defined by the following two tables.

x	$f(x)$
0000	00000
0001	00011
0010	00101
0011	00110
0100	01001
0101	01010
0110	01100
0111	01111
1000	10001
1001	10010
1010	10100
1011	10111
1100	11000
1101	11011
1110	11101
1111	11110

and

x	$g(x)$
000	000000
001	001111
010	010101
011	011010
100	100111
101	101000
110	110010
111	111101

.

The list of elements $x \in \mathbf{B}^4$ and $\mathbf{B}^3$ appearing in the first columns of the above tables are shown in *lexicographic* (dictionary) ordering. The reader should check that the table for f represents the first of our examples with $m = 4$. We will see below that these two examples are special cases of a family of codes.

We introduce some preliminaries in order to discuss more efficient codes than the next to last example.

DEFINITION 6.5. We define the *weight* of a word $w = a_1a_2...a_m \in \mathbf{B}^m$ as

$$\mathrm{wt}(w) = \sum_{i=1}^{m} a_i,$$

where the sum is in $\mathbb{Z}$; thus the weight of a word is the number of ones in its binary expansion, and

$$0 \leq \mathrm{wt}(w) \leq m$$

with equality $0 = \mathrm{wt}(w)$ if and only if $w = 0$. We thus have a map

$$\mathrm{wt} : \mathbf{B}^m \to \mathbb{Z}.$$

The *distance* $d(v, w)$ between words v and $w \in \mathbf{B}^m$ is

$$d(v, w) = \mathrm{wt}(v - w) = \mathrm{wt}(v + w);$$

thus the distance between these words $v = b_1 b_2 ... b_m$ and w is precisely the number of places where they differ (that is,

$$d(v, w) = |\{i = 1, 2, ..., m; a_i \neq b_i\}| = \sum_{i=1}^{m} |a_i - b_i|,$$

where the last sum is again in $\mathbb{Z}$). As in the case of weights, $d(w, v) = 0$ if and only if $w = v$.

Remark 6.6. The distance function provides us with a map

$$d : \mathbf{B}^m \times \mathbf{B}^m \to \mathbb{Z}_{\geq 0}$$

that satisfies the usual properties of distance functions studied in analysis: For all u, v and $w \in \mathbf{B}^m$,

- $d(w, v) = 0$ if and only if $w = v$.
- $d(w, v) = d(v, w)$.
- $d(u, w) \leq d(u, v) + d(v, w)$.

Its values land in $\mathbb{Z}_{\geq 0}$, a subset of $\mathbb{R}_{\geq 0}$, where the "normal" distance functions of analysis take their values. The distance function d is *translation invariant*: that is,

$$d(u - v, w - v) = d(u, w).$$

Theorem 6.7. *Let k be a positive integer. A coding function $f : \mathbf{B}^m \to \mathbf{B}^n$ detects k or fewer errors if and only if the minimum distance between distinct code words is at least $k + 1$.*

Proof. Say we have received a message $w \in \mathbf{B}^n$, whereas $v \in \mathbf{B}^n$ was the intended (correct) message. The code word v is in our list of possible code words. We need to know, of course, that such a list exists. If there are k or fewer errors in our message, then $d(v, w) \leq k$. So unless $v = w$, w is not in our list of code words and we have detected an error if and only if the minimum distance between code words is $\geq (k + 1)$. □

Theorem 6.8. *Let k be a positive integer. A coding function $f : \mathbf{B}^m \to \mathbf{B}^n$ allows the correction of k or fewer errors if and only if the minimum distance between distinct code words is at least $2k + 1$.*

Proof. If the distance between distinct code words is at least $2k + 1$, then by the previous theorem, we can detect up to and including $2k$ transmission errors. But even if we had as few as $k + 1$ transmission errors, there may be two distinct code words in $\mathbf{B}^n$ that are are within distance $k + 1$ to the erroneous message we received, so we cannot be sure how to correct the error. However, there is at most one code word within distance k of the erroneous message. So if the transmission had at most k errors, there is precisely one code word within distance k of the message. □

Example 6.9. For our standard small example 1, an examination of the differences between code words shows that the minimum distance between distinct code words is 2. (This involves computing $15 + 14 + ... + 1 = 120$ differences and then checking their weights.) Hence this coding function can detect one error, but cannot correct it. For small example 2, the minimum distance between distinct code words is also 2.

DEFINITION 6.10. Let $f : \mathbf{B}^m \to \mathbf{B}^n$ be a coding function. We say that f is a *group* or *linear code* if $f(\mathbf{B}^m)$ is a subgroup of $\mathbf{B}^n$.

REMARK 6.11. If $f : \mathbf{B}^m \to \mathbf{B}^n$ is a group homomorphism, then it certainly is a linear code.

THEOREM 6.12. *If $f : \mathbf{B}^m \to \mathbf{B}^n$ is a linear code, the minimum distance between distinct code words is minimum of the weights of non-zero code words.*

PROOF. Let d and d' be the minima of the distances between distinct code words and of the weights of non-zero code words, respectively; that is,

$$d = \min \{d(v, w); v \text{ and } w \in f(\mathbf{B}^m), v \neq w\}$$

and

$$d' = \min \{\mathrm{wt}(v); v \in f(\mathbf{B}^m), v \neq 0\}.$$

Both d and d' exist (and belong to $\mathbb{Z}_{>0}$) since they are minima of non-empty (finite[3]) sets of positive integers. Since f is a linear code, $0 \in f(\mathbf{B}^m)$, and thus we conclude from the fact that for all $v \in f(\mathbf{B}^m)$, $wt(v) = d(v, 0)$, that

$$d \leq d'.$$

Also there exist code words u and $v \in f(\mathbf{B}^m)$ (hence also $u + v \in f(\mathbf{B}^m)$) such that $u \neq v$ and

$$d = d(u, v) = \mathrm{wt}(u - v) = \mathrm{wt}(u + v) \geq d'.$$

□

EXAMPLE 6.13. Standard small examples 1 and 2 are linear codes. The first set of code words is the group generated by the words 00011, 00101, 01001 and 10001; the second by 001111, 010101 and 100111. For linear codes, the last theorem certainly simplifies the calculations of the minimal distances between code words. For our standard small example 1, we need to examine only 15 words (instead of 120 differences between words).

We describe a useful method for producing group codes f as group homomorphisms.

DEFINITION 6.14. Let m and n be positive integers with $m < n$. An $m \times n$ matrix (thus with m rows and n columns) G with entries in $\mathbf{B}$ is a *generator* matrix if its first m columns form the $m \times m$ identity matrix $\mathbf{I} = \mathbf{I}_m$. Thus $G = [\mathbf{I}_m, A]$ where A is a $m \times (n - m)$ matrix of zeros and ones.

EXAMPLE 6.15. Examples of generator matrices with $m = 1, 2, 3, 4$ and $n = m + 1$ are

$$\begin{bmatrix} 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

Another generator matrix is

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

[3]This extra fact is not needed.

DEFINITION 6.16. View the elements of $\mathbf{B}^m$ as $1 \times m$ matrices (row vectors). An $m \times n$ generator matrix G defines, using matrix multiplication, the group code (homomorphism[4])

$$f_G : \mathbf{B}^m \ni w \mapsto wG \in \mathbf{B}^n.$$

We will say that G is the *generator matrix for the code* f_G.

EXAMPLE 6.17. The last two matrices are generator matrices for our two standard small examples.

REMARK 6.18. A basis (over $\mathbf{B}$) of the vector space $\mathbf{B}^m$ consists of the m-row vectors v_i, $i = 1, 2, ..., m$, consisting of a one in the i-th column and $m-1$ zeros (in the other columns, of course). The image $f_G(v_i)$ of v_i under the map f_G is the i-th row of the matrix G. The vector subspace $f_G(\mathbf{B}^m)$ of $\mathbf{B}^n$ is hence spanned by the n rows of the matrix G. We also observe that for each $w \in \mathbf{B}^m$, the first m letters of the code word $f_G(w)$ consist of the word w; thus $f_G(w) = wv$, where $v \in \mathbf{B}^{n-m}$ constitutes a set of *check digits* and f_G is injective. The property of group homomorphisms (or equivalently of linear maps between vector spaces) that we find most useful is

$$f_G(v + w) = f_G(v) + f_G(w) \text{ for all } v \text{ and } w \in \mathbf{B}^m.$$

THEOREM 6.19. *Let $\theta : \mathbf{B}^m \to \mathbf{B}^n$ be an arbitrary homomorphism. Then there exists an $(m \times n)$ generator matrix G such that $\theta = f_G$.*

PROOF. (This theorem is really a standard result from linear algebra.) We may of course view θ as a $\mathbf{B}$-linear map from the vector space (over $\mathbf{B}$) $\mathbf{B}^m$ to the vector space $\mathbf{B}^n$. The vectors v_i form a basis for $\mathbf{B}^m$. The i-th row of the matrix G is then $\theta(v_i) \in \mathbf{B}^n$. □

EXAMPLE 6.20. The last three matrices in Example 6.15 are the generator matrices for the codes f and g described in the third set of codes in Example 6.4.

We describe a useful way to proceed with an error detection and correction procedure. Assume that we are using a group code $f : \mathbf{B}^m \to \mathbf{B}^n$, not necessarily given as a group homomorphism. We let $W \subset \mathbf{B}^n$ be the set of code words; a subgroup of $\mathbf{B}^n$. Let d be the minimum of the distances between code words in W. Suppose we receive a word $v \in \mathbf{B}^n$ with a single error in it. It differs from a word $w \in W$, by a basis element $v_i \in \mathbf{B}^n$. So instead of receiving a word $w \in W$, we have received the word $v_i + w$ in the coset $v_i + W$. Similarly, if we receive a word with precisely two errors, then a code word in the group W has been transformed by mistake into a word in the coset $v_i + v_j + W$ with $i \neq j$. In general a word with precisely k transmission errors involves replacing W by $v_{i_1} + v_{i_2} + ... + v_{i_k} + W$, where the integers i_j may be assumed to satisfy $1 \leq i_1 < i_2 < ... < i_k \leq n$.

Assume that we receive a word v. If it is a code word, we can be fairly certain that it is error free. It could of course contain transmission errors, necessarily more than one if we have check digits, that transforms one code word to another. If the minimum distance[5] between code words is $(d =)$ 7, then we would need at least 7 errors to change one code word to another – a very unlikely possibility. Say v is not a code word. Thus it contains at least one error. We want to correct the error, without requesting that the word be resent.

[4]The map f_G is also $\mathbf{B}$-linear (a stronger property); that is, a linear map from the vector space $\mathbf{B}^m$ to the vector space $\mathbf{B}^n$.

[5]We will be making parenthetical remarks about such an example as we go along.

It turns out that we cannot be absolutely sure that we are correcting the erroneous word to the correct code word. However, in practice, the probability that we have corrected an error is very close to 1. We use what is known as the *maximum likelihood decoding* procedure. We replace v by a code word closest to it. To do so, we compute the set of distances $d(v, w)$ for all $w \in W$ and choose as our replacement word w_o as one that minimizes these set of distances; if there is more than one such w_o, choose one arbitrarily. (In our example, w_o is unique if v has fewer than 4 transmission errors.)

Instead of constructing a w_o for each v we receive, we can calculate in advance a *decoding table* as follows.

We start with a coding function $f : \mathbf{B}^m \to \mathbf{B}^n$ for which the code words form a subgroup W of $\mathbf{B}^n$.

- The decoding table T is a $2^{n-m} \times 2^m$ matrix (thus consisting of $2^n = o(\mathbf{B}^n)$ entries; each of these entries is a word in $\mathbf{B}^n$).
- We list in a single row the 2^m elements in the group W, starting with the identity[6] $\mathbf{0} = 000...000$ of W. This is the first row of the matrix T. It is convenient to label $\mathbf{0} = x_1$.
- Find a word x_2 in $\mathbf{B}^n - W$ of minimal weight (there will, in general, be more than one of these; choose one). Add x_2 to (equivalently, subtract x_2 from) the entries in the first row of T to obtain its second row. Observe that above each word in the second row is the word in the first row that is closest to it. The entries in the second row of T hence list the elements in the coset $x_2 + W$. Of course, $W \cap (x_2 + W) = \emptyset$.
- Find a word x_3 in $\mathbf{B}^n - W - (x_2 + W)$ of minimal weight. The third row in the matrix T is constructed as the coset $x_3 + W$. We now observe that, in addition to $W \cap (x_3 + W) = \emptyset$, we also have that $(x_2 + W) \cap (x_3 + W) = \emptyset$; for if $v \in (x_2 + W) \cap (x_3 + W)$, then $v = x_2 + w_2 = x_3 + w_3$ for some w_2 and $w_3 \in W$ and it follows that $x_3 = x_2 + (w_2 - w_3) \in x_2 + W$; contrary to our choice of x_3.
- We keep repeating the above procedure.
- After r steps, we have used $2^m r$ elements of $\mathbf{B}^n$, arranged into r rows, the r-th row consisting of the coset $x_r + W$. We observe that

$$(x_j + W) \cap (x_r + W) = \emptyset, \text{ for } j = 1, ..., r - 1.$$

  We have listed all the elements of $\mathbf{B}^n$ after 2^{n-m} steps and at this point we have completed the construction of the decoding table T.
- We call the words x_i, $i = 1, ..., 2^{n-m}$, the *coset leaders* of the decoding table; they are the entries in the first column of the matrix T.
- We receive a word v. It certainly is an element of $\mathbf{B}^n$; hence in our decoding table T. Say the word v is the (i, j) entry of the matrix T. The code word (in W) nearest to v that we use is then the $(1, j)$ entry of T.

We illustrate the above construction for the group code $f_G : \mathbf{B}^4 \to \mathbf{B}^7$ defined by the generator matrix

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

[6] It is convenient but not necessary to do so.

The lengthy calculations are best performed on a computer. A sample (not simple) MAPLE program is shown below. We follow the program with some explanatory notes.

MAPLE SESSION #10

```
> with(linalg):  dirprod:=proc(A::{list,set},B::{list,set})
  local AxB,Ai, Bi, i,j;
  AxB:=[];
  for i from 1 to nops(A) do
  Ai:=op(A[i]);
  for j from 1 to nops(B) do
  Bi:=op(B[j]);
  AxB := [op(AxB), [ Ai, Bi ]];
  od;
  od;
  end:
  selfprod:=proc(S::{list},n::posint)
  local A,m;
  if (n=1) then
  return(S);
  fi;
  if (modp(n,2)=0) then
  return( selfprod(dirprod(S,S),n/2));
  else
  return( dirprod(S,selfprod(S,n-1)));
  fi;
  end:
> listA := selfprod([0,1],4):
> listB := selfprod([0,1],7):
> G :=
  matrix([[1,0,0,0,0,1,1],[0,1,0,0,1,1,0],[0,0,1,0,1,1,1],[0,0,0,1,1,1,1
  ]]);
```

$$G := \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

```
> g := x -> multiply(x,G): list1 := map(g,listA): mod2 := x ->
  modp(x,2):  listmod2 := l -> map(mod2,l):  gpW := map(listmod2,list1):
> SetMinus:=(A,B)->remove(x->inlist(x,B),A):
> inlist:=proc(x,L)
  local i;
  for i from 1 to nops(L) do
  if (equal(L[i],x)) then return(true) fi;
  od;
  false;
  end:
> list2 := SetMinus(listB,gpW): nops(listB); nops(list2);
                                  128
                                  112
> wt := x -> sum(x[k],k=1..7):  listwtgpW := map(wt,gpW);
```

$$listwtgpW := [0,\ 4,\ 4,\ 2,\ 3,\ 3,\ 3,\ 5,\ 3,\ 3,\ 3,\ 5,\ 4,\ 4,\ 4,\ 6]$$

```
> lowestwt:=proc(L) local result, i; result := L[1]; for i from 2 to
  nops(L) do if (wt(L[i]) < wt(result)) then result := L[i] fi; od;
  eval(result); end proc:
> x2 := lowestwt(list2):
> addvect:=proc(x,L) local fcn, preres; fcn := y -> matadd(x,y); preres
  := map(fcn,L); map(listmod2,preres) end proc:
> coset2 := addvect(x2,gpW):
> list3 := SetMinus(list2,coset2):
> x3 := lowestwt(list3):
> coset3 := addvect(x3,gpW):
> list4 := SetMinus(list3,coset3):
> x4 := lowestwt(list4):
> coset4 := addvect(x4,gpW):
> list5 := SetMinus(list4,coset4):
> x5 := lowestwt(list5):
> coset5 := addvect(x5,gpW):
> list6 := SetMinus(list5,coset5):
> x6 := lowestwt(list6):
> coset6 := addvect(x6,gpW):
> list7 := SetMinus(list6,coset6):
> x7 := lowestwt(list7):  coset7 := addvect(x7,gpW):
> list8 := SetMinus(list7,coset7):  x8 := lowestwt(list8):  coset8 :=
  addvect(x8,gpW):
> nops(SetMinus(list8,coset8));
```

$$0$$

```
> decodingmatrix := array(1..8,1..16,[gpW, coset2, coset3,coset4,
  coset5, coset6, coset7, coset8]);
```

$$\begin{bmatrix}
0000000 & 0001111 & 0010111 & 0011000 & 0100110 & 0101001 & 0110001 & 0111110 & 1000011 & 1001100 & 1010100 & 1011011 \\
0000001 & 0001110 & 0010110 & 0011001 & 0100111 & 0101000 & 0110000 & 0111111 & 1000010 & 1001101 & 1010101 & 1011010 \\
0000010 & 0001101 & 0010101 & 0011010 & 0100100 & 0101011 & 0110011 & 0111100 & 1000001 & 1001110 & 1010110 & 1011001 \\
0000100 & 0001011 & 0010011 & 0011100 & 0100010 & 0101101 & 0110101 & 0111010 & 1000111 & 1001000 & 1010000 & 1011111 \\
0001000 & 0000111 & 0011111 & 0010000 & 0101110 & 0100001 & 0111001 & 0110110 & 1001011 & 1000100 & 1011100 & 1010011 \\
0100000 & 0101111 & 0110111 & 0111000 & 0000110 & 0001001 & 0010001 & 0011110 & 1100011 & 1101100 & 1110100 & 1111011 \\
1000000 & 1001111 & 1010111 & 1011000 & 1100110 & 1101001 & 1110001 & 1111110 & 0000011 & 0001100 & 0010100 & 0011011 \\
0000101 & 0001010 & 0010010 & 0011101 & 0100011 & 0101100 & 0110100 & 0111011 & 1000110 & 1001001 & 1010001 & 1011110
\end{bmatrix}$$

```
> H
  :=matrix([[0,1,1],[1,1,0],[1,1,1],[1,1,1],[1,0,0],[0,1,0],[0,0,1]]);
```

$$H := \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

```
> result := array(1..8,1..2):  for k to 8 do for l to 2 do if (l = 2)
then result[k,l] := eval(decodingmatrix[k,1]) else result[k,l] :=
listmod2(eval(multiply(decodingmatrix[k,1],H))) end if end do end do:
print(result);
```

$$\begin{bmatrix} 000 & 0000000 \\ 001 & 0000001 \\ 010 & 0000010 \\ 100 & 0000100 \\ 111 & 0001000 \\ 110 & 0100000 \\ 011 & 1000000 \\ 101 & 0000101 \end{bmatrix}$$

END MAPLE PROGRAM

- The first item in the program consists of two parts; the first computes the Cartesian product of two sets or lists and the second uses this procedure to compute the n-th Cartesian product of a list.
- The second and third commands compute $\mathbf{B}^4$ and $\mathbf{B}^7$, respectively.
- The next step enters the matrix G.
- The next set of instructions execute the mod 2 multiplication of matrices to obtain the group W. We have suppressed the printing of W as well as the cosets of W in $\mathbf{B}^7$ in the subsequent commands because they appear as the rows of the decoding matrix.
- The next two sets of commands compute the relative complement of one list with respect to another. The standard MAPLE set difference command is inappropriate for our purposes.
- The computations of the cosets of W in $\mathbf{B}^7$ need several preliminaries. One needs to compute relative differences of sets (the `listn` entries), minimal weights of sets of words, and finally the cosets. This is done in the subsequent set of commands. As a check on our work, we have computed the cardinality of `listB` and `list2` using the `nops` command.
- We have displayed the weights of the code words W. Since the lowest non-zero weight of elements of W is 2, the coding function will detect 1 error, but will correct none.
- The eight `xi` are the coset leaders.
- The lists `list8` and `coset8` contain the same words in a different order; this fact is verified by the `nops(SetMinus(list8,coset8))` command.
- We have shown only 12 of the 16 columns of the decoding matrix.

- The role of the last two commands should be obvious after we develop a little more theory.

We now proceed to a discussion of correcting errors with less information than a complete decoding table.

DEFINITION 6.21. Let $G = [\mathbf{I}_m, A]$ be an $m \times n$ generator matrix. The *corresponding parity-check* matrix is the $n \times (n-m)$ matrix $H = \begin{bmatrix} A \\ \mathbf{I}_{n-m} \end{bmatrix}$. The *syndrome* of a word $w \in \mathbf{B}^n$ is the word $wH \in \mathbf{B}^{n-m}$.

PROPOSITION 6.22. *Let H be a parity-check matrix corresponding to the generator matrix G. Then $w \in \mathbf{B}^n$ is a code word if and only if $wH = \mathbf{0}$.*

PROOF. A word $w \in \mathbf{B}^n$ is a code word if and only if $w = sG = s[\mathbf{I}_m, A]$ for some $s \in \mathbf{B}^m$ if and only if $w = uv$ with $u \in \mathbf{B}^m$ and $v = uA$. We rewrite the last equation as

$$\mathbf{0} = uA - v\mathbf{I}_{n-m} = uA + v\mathbf{I}_{n-m} = (uv)H = wH$$

showing that w is a code word if and only if $\mathbf{0} = wH$. □

COROLLARY 6.23. *Two words are in the same row of the coset decoding table if and only if they have the same syndrome.*

PROOF. Two words u and $v \in \mathbf{B}^n$ are in the same row of the decoding table (in the same coset of the code group W) if and only if they differ by a code word $w \in W$; that is, if and only if $w = u - v$ if and only if $\mathbf{0} = wH = uH - vH$ or if and only if $uH = vH$. □

REMARK 6.24. A parity-check matrix H defines a linear mapping

$$H : \mathbf{B}^n \ni v \mapsto vH \in \mathbf{B}^{n-m}.$$

This linear mapping need not be injective nor surjective. If H is the parity-check matrix corresponding to the generator matrix G, then we also have the injective (not surjective) linear mapping (we called it f_G before)

$$G : \mathbf{B}^m \ni w \mapsto wG \in \mathbf{B}^n.$$

The last proposition shows that $H \circ G$ is the zero map.

We can now expand the decoding table for a group code by adding an extra column, say at the left, that records the syndrome of each row. Thus the first two entries of the first row of the expanded decoding table T, which is now a $2^{n-m} \times (2^m + 1)$ matrix, start with $\mathbf{0} \in \mathbf{B}^{n-m}$ and $\mathbf{0} \in \mathbf{B}^n$. We can dispense with all but the first two columns of this expanded decoding table and label the resulting $2^{n-m} \times 2$ matrix $\mathbf{T}$. If we receive a word v, we first compute its syndrome vH, which we find in the first of our two column matrix $\mathbf{T}$. In the next column, in the same row as vH, is the coset leader u of the row in the full decoding table T where v is found. Adding u to v we obtain $u + v$, a code word closest to the word v that we received. Stripping away the last $n - m$ digits from the word $u + v$ we obtain the maximum likelihood candidate for the word w that we believe was intended.

EXERCISES

(1) If $f : \mathbf{B}^m \to \mathbf{B}^n$ is a linear code, must it also be a group homomorphism?

(2) Show that $\mathrm{wt} : \mathbf{B}^m \to \mathbb{Z}$ is not a group homomorphism but that

$$\mathrm{red}_2 \circ \mathrm{wt} : \mathbf{B}^m \to \mathbb{Z}_2$$

is.

(3) In this section words were considered as row vectors of length m and hence the coding function f for a group code was a map $w \mapsto wG$ for some some generator matrix G. How would you define a generator matrix and the corresponding parity-check matrix if words were viewed as column vectors of length m?

CHAPTER 7

Roots of polynomials

Among the main purposes of this chapter is to discuss unified approaches (formulae) for solving polynomial equation of degree ≤ 4. We outline several approaches to establishing a key result: the fundamental theorem of algebra. Along the way we continue the study of the ring of polynomials; emphasising once again that it shares many properties with the ring of integers. For this chapter, we assume that the reader is familiar with some basic linear algebra; for example, the contents of [**2**]. THE MATERIAL IN THIS CHAPTER IS IN PRELIMINARY FORM.

1. Roots of polynomials

The main results of this subsection is the next theorem, the fundamental theorem of algebra. We present several proofs. Each of them requires some analysis.

THEOREM 7.1 (The fundamental theorem of algebra, FTA). *For all $n \in \mathbb{Z}_{>0}$, an n^{th} degree complex polynomial $p(x)$ has precisely n complex roots counting multiplicities; thus there exist constants $0 \neq \lambda$ and $\beta_1, ..., \beta_n \in \mathbb{C}$ such that*

$$p(x) = \lambda(x - \beta_1)...(x - \beta_n).$$

We start with

DEFINITION 7.2. A *zero* or *root* of a polynomial $p(x)$ of positive degree is a complex number α such that $p(\alpha) = 0$.

It is an immediate consequence of the Euclidean algorithm that if α is a root of the polynomial $p(x)$ of degree $n > 0$, then there exists a unique polynomial $q(x)$ of degree $n - 1$ such that

$$p(x) = (x - \alpha)q(x).$$

1.0.1. *A linear algebra approach.* We outline a recent argument due to H. Derksen [**4**], based mostly on linear algebra. While this approach requires considerable algebraic tools (which our outlined without proof), it depends on very little analysis (complete details provided).

LEMMA 7.3. *Every real polynomial $p(x)$ of odd degree has a real zero.*

PROOF. This standard fact is proved in most calculus courses. The argument goes as follows. It involves no loss of generality to assume that $p(x)$ is monic. Thus

$$\lim_{x\to\infty} p(x) = \infty \text{ and } \lim_{x\to-\infty} p(x) = -\infty.$$

it follows that there exists an $R > 0$ such that

$$p(R) > 0 \text{ and } p(-R) < 0.$$

By the intermediate value theorem there exists a λ in the open interval $(-R, R)$ such that $p(\lambda) = 0$. □

LEMMA 7.4. *Every complex number $z = \alpha + \beta\imath$, α and $\beta \in \mathbb{R}$, has a square root.*

PROOF. Put $\gamma = \sqrt{\alpha^2 + \beta^2} = |z|$. The existence of square roots of non-negative real numbers is a basic property of the real number system; a fact from calculus. Then

$$\left(\sqrt{\frac{\gamma+\alpha}{2}} + \sqrt{\frac{\gamma-\alpha}{2}}\imath\right)^2 = \alpha + \beta\imath.$$

□

We begin an outline the the algebraic tolls needed in this approach.

DEFINITION 7.5. Let K be a field and V a K-vector space. A K-linear self map L of V is called an *endomorphism* of V. A scalar $\lambda \in K$ is an *eigenvalue* of L if there exists a vector $x \in V$, $x \neq 0$, called an *eigenvector* of λ or of L, such that $L(x) = \lambda x$.

We introduce a statement $\mathcal{P}(K, d, r)$ for a field K and positive integers d and r: *Any r commuting endomorphisms of a K-vector space V of dimension n such that d does not divide n have a common eigenvector.*

LEMMA 7.6. *If $\mathcal{P}(K, d, 1)$ holds, then so does $\mathcal{P}(K, d, r)$ for all positive integers r.*

LEMMA 7.7. *$\mathcal{P}(\mathbb{R}, 2, r)$ holds for all positive integers r; that is, any collection A_1, A_2, ..., A_r of commuting endomorphisms of an odd dimensional real vector space have a common eigenvector.*

LEMMA 7.8. *$\mathcal{P}(\mathbb{C}, 2, 1)$ holds; that is, every endomorphism of an odd dimensional complex vector has an eigenvector.*

LEMMA 7.9. *$\mathcal{P}(\mathbb{C}, 2^k, r)$ holds for all positive integers k and r.*

The above series of technical results lead to a theorem that is of interest in its own right.

THEOREM 7.10. *Let r be a positive integer. If A_1, A_2, ..., A_r are commuting endomorphisms of non-trivial finite dimensional $\mathbb{C}$-vector space V, then they have a common eigenvector.*

As a consequence (corollary in some sense) of the last theorem, we can now establish the fundamental theorem of algebra in the following form:

COROLLARY 7.11 (The fundamental theorem of algebra). *If $p(x)$ is a non-constant polynomial with complex coefficients, then there exists a $\beta \in \mathbb{C}$ such that $p(\beta) = 0$.*

PROOF. It suffices to assume that $p(x)$ is a monic polynomial of degree $n \geq 1$:

$$p(x) = x^n + a_1 x^{n-1} + ... + a_n. \tag{21}$$

We claim that $p(x) = \det(x\mathbf{I} - A)$, where A is the *companion* matrix of $p(x)$:

$$A = \begin{bmatrix} 0 & 0 & ... & 0 & -a_n \\ 1 & 0 & & 0 & -a_{n-1} \\ 0 & 1 & & 0 & -a_{n-2} \\ . & & & . & \\ . & & & . & \\ . & & & . & \\ 0 & 0 & ... & 1 & -a_1 \end{bmatrix}.$$

We use induction on n to verify that

$$x^n + a_1 x^{n-1} + ... + a_n = \det \begin{bmatrix} x & 0 & 0 & ... & 0 & 0 & a_n \\ -1 & x & 0 & & 0 & 0 & a_{n-1} \\ 0 & -1 & x & & 0 & 0 & a_{n-2} \\ . & & & & & & . \\ . & & & & & & . \\ . & & & & & & . \\ 0 & 0 & 0 & ... & -1 & x & a_2 \\ 0 & 0 & 0 & ... & 0 & -1 & x + a_1 \end{bmatrix}.$$

The formula for the base case $n = 1$ reads

$$x + a_1 = \det [x + a_1],$$

which is obviously true. We assume now that $n > 1$. Expanding in terms of minors, we see that

$$\det \begin{bmatrix} x & 0 & 0 & ... & 0 & 0 & a_n \\ -1 & x & 0 & & 0 & 0 & a_{n-1} \\ 0 & -1 & x & & 0 & 0 & a_{n-2} \\ . & & & & & & . \\ . & & & & & & . \\ . & & & & & & . \\ 0 & 0 & 0 & ... & -1 & x & a_2 \\ 0 & 0 & 0 & ... & 0 & -1 & x + a_1 \end{bmatrix}$$

$$= x \det \begin{bmatrix} x & 0 & & 0 & 0 & a_{n-1} \\ -1 & x & & 0 & 0 & a_{n-2} \\ . & & & & & . \\ . & & & & & . \\ . & & & & & . \\ 0 & 0 & ... & -1 & x & a_2 \\ 0 & 0 & ... & 0 & -1 & x + a_1 \end{bmatrix} + \det \begin{bmatrix} 0 & 0 & & 0 & 0 & a_n \\ -1 & x & & 0 & 0 & a_{n-2} \\ . & & & & & . \\ . & & & & & . \\ . & & & & & . \\ 0 & 0 & ... & -1 & x & a_2 \\ 0 & 0 & ... & 0 & -1 & x + a_1 \end{bmatrix}.$$

The induction hypothesis tells us that

$$\det \begin{bmatrix} x & 0 & & 0 & 0 & a_{n-1} \\ -1 & x & & 0 & 0 & a_{n-2} \\ . & & & & & . \\ . & & & & & . \\ . & & & & & . \\ 0 & 0 & ... & -1 & x & a_2 \\ 0 & 0 & ... & 0 & -1 & x + a_1 \end{bmatrix} = x^{n-1} + a_1 x^{n-2} + ... + a_{n-1};$$

while another expansion in terms of minors and the fact that the determinant of an upper triangular matrix is the product of the diagonal elements yields

$$\det \begin{bmatrix} 0 & 0 & & 0 & 0 & a_n \\ -1 & x & & 0 & 0 & a_{n-2} \\ . & & & & & . \\ . & & & & & . \\ . & & & & & . \\ 0 & 0 & ... & -1 & x & a_2 \\ 0 & 0 & ... & 0 & -1 & x+a_1 \end{bmatrix} = (-1)^{n-2} a_n \det \begin{bmatrix} -1 & x & & 0 & 0 \\ . & & & & . \\ . & & & & . \\ . & & & & . \\ 0 & 0 & ... & -1 & x \\ 0 & 0 & ... & 0 & -1 \end{bmatrix} = a_n.$$

The last two equalities finish the induction argument. The last theorem tells that A has an eigenvalue; that is, there exists a $\beta \in \mathbb{C}$ such that $p(\beta) = 0$. □

REMARK 7.12. The above corollary implies Theorem 7.1 by induction on $n \in \mathbb{Z}_{>0}$. The base case $n = 1$ holds. So if $n > 1$ and $p(x)$ is a polynomial of degree n, then by our last corollary, there is a $\beta_n \in \mathbb{C}$ such that $p(\beta_n) = 0$. By the division algorithm,

$$p(x) = (x - \beta_n)q(x) + r(x),$$

where $q(x)$ is a complex polynomial of degree $n-1$ and $r(x) \in \mathbb{C}$. Since $p(\beta_n) = 0$, $r(x) = 0$. The induction hypothesis tell us that $q(x)$ factors as required.

1.0.2. *A topological (real analysis) approach.*

LEMMA 7.13 (d'Alembert). *If $p(x)$ is a non-constant polynomial and $p(z_0) \neq 0$, then any ball about z_0 contains a point z_1 with $|p(z_1)| < |p(z_0)|$.*

PROOF. We use the Taylor series (with z_0 replacing x_o) for the polynomial $p(x)$. Since the polynomial is not constant, there exists a smallest integer k, $1 \leq k \leq n$ such that $p^{(k)} \neq 0$. Thus (as a polynomial in Δ)

$$p(z_0 + \Delta) = p(z_0) + \alpha\Delta^k + \epsilon\Delta^{k+1},$$

where α is a non-zero complex number and ϵ is a polynomial in Δ of degree $n - k - 1$ (if $n = k$, then $n - k - 1$ should be interpreted as $-\infty$). Now let us think of Δ as a complex number of small (certainly much less than 1) absolute value – which can be made even smaller as our argument proceeds. By choosing Δ sufficiently small we can certainly make $\left|\epsilon\Delta^{k+1}\right| < \frac{1}{4}|p(z_0)|$. By making $|Delta|$ even smaller, if necessary, we can also make sure that $|\alpha\Delta^k| < \frac{1}{2}|p(z_0)|$. It readily follows that $0 < |p(z_0 + \Delta)| < 2|p(z_0)|$. We would like to eliminate the 2 from the last equation. We have one more degree of freedom at our disposal: CHANGING THE ARGUMENT OF THE COMPLEX NUMBER Δ. So let θ_0, θ and θ_1 be the initial arguments of $p(z_0)$, Δ and $\alpha\Delta^k + \epsilon\Delta^{k+1}$, respectively; chosen to lie in the interval $[0, 2\pi)$. As we crank up the argument of Δ from θ to $\theta + 2\pi$, the argument of $\alpha\Delta^k + \epsilon\Delta^{k+1}$ changes *continuously* from θ_1 to $\theta_1 + 2\pi n$ for some positive integer n. (This is not obvious – an analysis proof is needed.) By the intermediate value theorem there is a $\varphi \in [0, 2\pi n]$ so that if we choose Δ to have argument φ, the complex number $\alpha\Delta^k + \epsilon\Delta^{k+1}$ will have argument $-\theta_0$. This means that the vectors $p(z_0)$ and $\alpha\Delta^k + \epsilon\Delta^{k+1}$ point in opposite directions and hence (TO BE CONTINUED)¿ □

We are once again ready to prove

THEOREM 7.14 (FTA). *Every non-constant polynomial has a root.*

PROOF. NEED ARGUMENT HERE. □

REMARK 7.15. Another proof of FTA using some analytic steps, similar to those used above, can be found in [**9**].

1.0.3. *A complex analysis approach.* By far the most elegant proof of FTA is through complex analysis. See for example [**6**].

EXERCISES

(1) Let F_1 and F_2 be subfields of $\mathbb{C}$ that contain $\mathbb{Q}$. Show that $F_1 \cap F_2$ is also a subfield of $\mathbb{C}$ that contains $\mathbb{Q}$. Conclude that if ζ_1, ζ_2, ..., ζ_n, is an arbitrary finite collection of complex numbers, then there exists a unique smallest (by inclusion) subfield $F \subset \mathbb{C}$ that contains each ζ_i, $i = 1, 2, ..., n$.
(2) Let $p(x)$ be a monic polynomial of degree $n \geq 1$. Let ζ_i, $i = 1, 2, ..., n$ be the roots of $p(x)$.
   (a) Show that there exists a unique field $F \subset \mathbb{C}$ that contains $\mathbb{Q}$ and ζ_i for $i = 1, 2, ..., n$.
   (b) Does F contain the coefficients of the polynomial $p(x)$?
(3) Let n be a positive integer and let $p(x)$ of (21) be a monic real polynomial of degree n. Let
$$a = |a_1| + ... + |a_n| + 1.$$
Show that $p(a) > 0$ and $p(-a) < 0$. Hence there exists a real number $\lambda \in (-a, a)$ such that $p(\lambda) = 0$.

1.1. Derivatives and multiple roots. SECTION TO BE COMPLETED LATER.

2. Circulant matrices

Fix a positive integer $n \geq 2$, and let
$$v = (v_0,\ v_1, \ldots, v_{n-1})$$
be a row vector in $\mathbb{C}^n$. Define a *shift* operator $T : \mathbb{C}^n \to \mathbb{C}^n$ by
$$T(v_0,\ v_1, \ldots, v_{n-1}) = (v_{n-1},\ v_0, \ldots, v_{n-2})\,.$$
The *circulant matrix* associated to v is the $n \times n$ matrix whose rows are given by iterations of the shift operator acting on v, that is to say, the matrix whose k-th row is given by $T^{k-1}v$, $k = 1, \ldots, n$. Such a matrix will be denoted by
$$V = \mathrm{circ}\{v\} = \mathrm{circ}\{v_0, v_1, \ldots, v_{n-1}\}\,. \tag{22}$$

THEOREM 7.16. *Let $v = (v_0, v_1, \ldots, v_{n-1})$ be a vector in $\mathbb{C}^n$, and $V = \mathrm{circ}\{v\}$. If ϵ is a primitive n-th root of unity, then*
$$\det V = \det \begin{bmatrix} v_0 & v_1 & \cdots & v_{n-2} & v_{n-1} \\ v_{n-1} & v_0 & \cdots & v_{n-3} & v_{n-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ v_2 & v_3 & \cdots & v_0 & v_1 \\ v_1 & v_2 & \cdots & v_{n-1} & v_0 \end{bmatrix} = \prod_{l=0}^{n-1} \left(\sum_{j=0}^{n-1} \epsilon^{jl} v_j \right). \tag{23}$$

PROOF. We view the matrix $V = \text{circ}\{v_0, v_1, \ldots, v_{n-1}\}$ as a self map (linear operator) of $\mathbb{C}^n$. For each integer l, $0 \le l \le n-1$, let $x_l \in \mathbb{C}^n$ be the transpose of the row vector $\frac{1}{\sqrt{n}}(1, \epsilon^l, \epsilon^{2l}, \ldots, \epsilon^{(n-1)l})$ and[1]

$$\lambda_l = v_0 + \epsilon^l v_1 + \cdots + \epsilon^{(n-1)l} v_{n-1}. \tag{24}$$

A calculation shows that

$$\begin{bmatrix} v_0 & v_1 & \cdots & v_{n-2} & v_{n-1} \\ v_{n-1} & v_0 & \cdots & v_{n-3} & v_{n-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ v_2 & v_3 & \cdots & v_0 & v_1 \\ v_1 & v_2 & \cdots & v_{n-1} & v_0 \end{bmatrix} \begin{bmatrix} 1 \\ \epsilon^l \\ \epsilon^{2l} \\ \vdots \\ \epsilon^{(n-1)l} \end{bmatrix} = \lambda_l \begin{bmatrix} 1 \\ \epsilon^l \\ \epsilon^{2l} \\ \vdots \\ \epsilon^{(n-1)l} \end{bmatrix}.$$

Thus λ_l is an eigenvalue of V with normalized eigenvector x_l. Since the n vectors $x_0, x_1, \ldots, x_{n-1}$ are linearly independent, they form a basis for $\mathbb{C}^n$. We conclude, by a standard result from linear algebra, that the matrix V is diagonalizable and that

$$\det V = \prod_{l=0}^{n-1} \lambda_l \,.$$

□

Let D_V be the diagonal matrix with diagonal entries λ_0, λ_1, …, λ_{n-2}, λ_{n-1}, respectively. Then there exists[2] an $n \times n$ invertible matrix C such that

$$C^{-1} V C = D_V. \tag{25}$$

Thus the matrices

$$V = \text{circ}\{v_0, v_1, \ldots, v_{n-1}\} \text{ and } D_V = \text{diag}(\lambda_0, \lambda_1, \ldots, \lambda_{n-1})$$

are conjugate[3].

REMARK 7.17. It is possible to always use $\epsilon = e^{\frac{2\pi\imath}{n}}$. The $\varphi(n)$ distinct primitive n-th roots of unity are then $\{\epsilon^k;\ k \in \mathbb{Z},\ 1 \le k \le n,\ (n,k) = 1\}$.

DEFINITION 7.18. For $\epsilon = e^{\frac{2\pi\imath}{n}}$, we call the set $\{\lambda_0, ..., \lambda_{n-1}\}$ defined by (24), the *ordered eigenvalues* of the circulant matrix (22).

COROLLARY 7.19. *The characteristic polynomial of V is*

$$p_V(x) = \det(xI - V) = \prod_{l=0}^{n-1} (x - \lambda_l).$$

COROLLARY 7.20. *We have $\sum_{l=0}^{n-1} \lambda_l = n v_0$.*

[1]We reserve the symbols λ_l and x_l for this eigenvalue and eigenvector throughout this chapter. We use the convention that, unless otherwise specified, all vectors are column matrices. To avoid too many empty spaces, we will often write them as row matrices without mentioning that we are considering the transpose of the column vector. This identification should not cause any confusion. In a sense, it was already used in defining the shift operator T. In line with this convention, matrices, when viewed as linear operators, multiply column vectors on the left.

[2]We will describe this matrix shortly.

[3]The diagonal matrix with entries a_1, a_2, …, a_{n-1}, a_n is denoted by $\text{diag}(a_1, a_2, \ldots, a_{n-1}, a_n)$.

PROOF. Since

$$\sum_{l=0}^{n-1} e^{il} = \begin{cases} n & \text{for } i = 0 \\ 0 & \text{for } i = 1, ..., n-1 \end{cases},$$

we see that

$$\sum_{l=0}^{n-1} \lambda_l = \sum_{l=0}^{n-1} \sum_{i=0}^{n-1} e^{li} v_i = \sum_{i=0}^{n-1} \left(\sum_{l=0}^{n-1} e^{li} \right) v_i = n v_0.$$

□

REMARK 7.21. The trace of a square matrix is the sum of its diagonal entries. Since the trace is a conjugacy class invariant, the last corollary also follows from the identity $\sum_{l=0}^{n-1} \lambda_l = \operatorname{trace} V$, since the sum is the trace of D_V.

DEFINITION 7.22. Let $\mathrm{Circ}(n)$ and $\mathrm{Diag}(n)$ be the sets of all $n \times n$ complex circulant and diagonal matrices, respectively, viewed as subsets of $M_n(\mathbb{C})$, the algebra of $n \times n$ complex matrices with the usual matrix operations of addition and multiplication and scalar multiplication (by complex numbers).

$\mathrm{Diag}(n)$ is an n-dimensional commutative subalgebra of $M_n(\mathbb{C})$. Furthermore, transposes of diagonal matrices and inverses of nonsingular (a diagonal matrix is nonsingular if and only if the product of its diagonal entries (which equals its determinant) is not zero) diagonal matrices are also diagonal. We record a number of consequences of the last theorem that show that $\mathrm{Circ}(n)$ has many similar properties. As a matter of fact, we will show that $\mathrm{Diag}(n)$ and $\mathrm{Circ}(n)$ are isomorphic algebras.

COROLLARY 7.23. $\mathrm{Circ}(n)$ *is an* n*-dimensional commutative subalgebra of* $M_n(\mathbb{C})$*. Furthermore, complex conjugates and transposes of circulant matrices and inverses of nonsingular circulant matrices are also circulant. All elements of* $\mathrm{Circ}(n)$ *are simultaneously diagonalized by the same unitary matrix.*

PROOF. Our first observation is that $\mathrm{Circ}(n)$ is an n-dimensional vector space over the complex numbers $\mathbb{C}$. Let C be the $n \times n$ matrix that represents the linear transformation sending the l-th unit vector e_l (this is the vector $(0, ..., 0, 1, 0, ..., 0)$ with the 1 in the l-th slot) to x_l:

$$C = \frac{1}{\sqrt{n}} \begin{bmatrix} 1 & 1 & \cdots & 1 & 1 \\ 1 & \epsilon & \cdots & \epsilon^{n-2} & \epsilon^{n-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & \epsilon^{n-2} & \cdots & \epsilon^{(n-2)^2} & \epsilon^{(n-1)(n-2)} \\ 1 & \epsilon^{n-1} & \cdots & \epsilon^{(n-2)(n-1)} & \epsilon^{(n-1)^2} \end{bmatrix}. \tag{26}$$

Observe that C is *symmetric* (its own *transpose*) and that C^*, the transpose of the conjugate of C, equals C^{-1}, the inverse of C. Thus C is a symmetric *unitary* matrix. A lengthy but routine calculation shows that (25) holds. This calculation can be avoided if we use the definitions and results on eigenvalues at our disposal:

$$C^{-1} V C(e_l) = C^{-1} V(x_l) = C^{-1}(\lambda_l x_l) = \lambda_l C^{-1}(x_l) = \lambda_l e_l = D_V(e_l).$$

Thus the unitary matrix C, that depends only on n, diagonalizes each circulant matrix. It is convenient to fix the matrix C and study the map

$$C^* : \ \mathrm{Circ}(n) \ni V \mapsto C^{-1} V C \in \mathrm{Diag}(n).$$

For U and $V \in M_n(\mathbb{C})$,

$$C^{-1}VC = U \text{ iff } V = CUC^{-1}. \tag{27}$$

Since for all V_1 and $V_2 \in \mathrm{Circ}(n)$ and all $c \in \mathbb{C}$,

$$C^*(V_1 + cV_2) = C^*(V_1) + cC^*(V_2)$$

and as a result of (27) for $V \in \mathrm{Circ}(n)$,

$$C^*(V) = \mathbf{O} \text{ iff } V = \mathbf{O},$$

we conclude that C^* is a $\mathbb{C}$-linear injection of $\mathrm{Circ}(n)$ into $\mathrm{Diag}(n)$. Since

$$\dim(\mathrm{Circ}(n)) = n = \dim(\mathrm{Diag}(n)),$$

we conclude that C^* is surjective; that is, $C^*(\mathrm{Circ}(n)) = (\mathrm{Diag}(n))$ and hence that $\mathrm{Circ}(n)$ and $\mathrm{Diag}(n)$ are isomorphic as vector spaces over $\mathbb{C}$ and $(C^*)^{-1} = C \cdot C^{-1}$ maps $\mathrm{Diag}(n)$ onto $\mathrm{Circ}(n)$. Since for two diagonal matrices D_1 and D_2,

$$(C^*)^{-1}(D_1D_2) = CD_1D_2C^{-1} = (CD_1C^{-1})(CD_2C^{-1}) = (C^*)^{-1}(D_1)(C^*)^{-1}(D_2),$$

we conclude that $\mathrm{Circ}(n)$ is closed under matrix multiplication. Since $\mathrm{Diag}(n)$ is closed under complex conjugation, transposes and inverses (of nonsingular matrices that it contains), so is $\mathrm{Circ}(n)$ by an argument similar to the one used to show that $\mathrm{Circ}(n)$ is closed under matrix multiplication. □

COROLLARY 7.24 (of proof). $\mathrm{Circ}(n)$ *and* $\mathrm{Diag}(n)$ *are isomorphic subalgebras of* $M_n(\mathbb{C})$.

We proceed to describe another algebra that is isomorphic to $\mathrm{Circ}(n)$. If we let

$$W = \mathrm{circ}\{0, 1, 0, \ldots, 0\},$$

then it is easily seen that

$$\mathrm{circ}\{v_0, v_1, \ldots, v_{n-1}\} = \sum_{i=0}^{n-1} v_i W^i.$$

REMARK 7.25. With respect to the standard basis of $\mathbb{C}^n$, the shift operator T is represented by the transpose of the matrix W; that is, by $\mathrm{circ}\{0, 0, \ldots, 0, 1\}$.

COROLLARY 7.26. *The map that sends* W *to the indeterminate* X *establishes an isomorphism of algebras between* $\mathrm{Circ}(n)$ *and the algebra* $\mathbb{C}[X]/(X^n - 1)$.

DEFINITION 7.27. Given a circulant matrix $V = \mathrm{circ}\{v_0, v_1, \ldots, v_{n-1}\}$, we define its *representer* as the polynomial $P_V(X) = \sum_{i=0}^{n-1} v_i X^i$.

COROLLARY 7.28. *For* $l = 0, \ldots, n-1$, *we have that* $\lambda_l = P_V\left(e^{\frac{2\pi\imath}{n}l}\right)$.

We know that a matrix cannot be recovered from its collection of eigenvalues, not even from an ordered set of eigenvalues. However, given an ordered set of n eigenvalues: $\{\lambda_l,\ l = 0, 1, ..., n-1\}$, there exists a unique diagonal matrix D with entry λ_l in the l-th slot. Thus CDC^{-1} is the unique circulant matrix with this set of ordered eigenvalues.

EXERCISES

(1) A complex $n \times n$ matrix V is *Hermetian* if and only if $V^t = \bar{V}$.

(a) What is the dimension over $\mathbb{R}$ of the vector space of $n \times n$ complex Hermetian matrices?
(b) What is the dimension over $\mathbb{R}$ of the vector space of $n \times n$ complex Hermetian circulant matrices?

(2) Let $\mathbf{v} \in \mathbb{C}^n$ be the row vector

$$\mathbf{v} = (v_0, v_1, ..., v_{n-1}).$$

We have associated with $\mathbf{v}$ several other algebraic quantities: a circulant matrix

$$\mathbf{V} = \text{circ}\{\mathbf{v}\} \in \text{Circ}(n),$$

an ordered set of eigenvalues

$$\lambda_{\mathbf{V}} = \{\lambda_0, \lambda_1, ...\lambda_{n-1}\} \in \mathbb{C}^n,$$

the characteristic polynomial of $\mathbf{V}$

$$p_{\mathbf{V}}(x) = \det(xI - \mathbf{V}) = \prod_{l=0}^{n-1}(x - \lambda_l) = x^n + \sum_{k=0}^{n-1} a_k x^k,$$

hence also a vector

$$\mathbf{a} = \{a_0, a_1, ...a_{n-1}\} \in \mathbb{C}^n \text{ with } a_{n-1} = -nv_0,$$

and the representer of $\mathbf{V}$

$$P_{\mathbf{V}}(x) = \sum_{k=0}^{n-1} v_k x^k.$$

Let $\mathbf{J} \in \mathbb{C}^n$ and $\mathbf{K} \in \text{Circ}(n)$ be respectively the vector and matrix with all entries equal to 1 (thus $\mathbf{K} = \text{circ}\{\mathbf{J}\}$). Let

$$\mathbf{v}' = (0, v_1 - v_0, ..., v_{n-1} - v_0) = \mathbf{v} - v_0\mathbf{J},$$

and denote by symbols with primes the associated quantities for $\mathbf{v}'$. Show that

(a) $\mathbf{V}' = \mathbf{V} - v_0\mathbf{K}$.
(b) $\lambda_{\mathbf{V}'} = \{\lambda_0 - nv_0, \lambda_1, ...\lambda_{n-1}\} = \{-\sum_{l=1}^{n-1}\lambda_l, \lambda_1, ...\lambda_{n-1}\}$.
(c) $p_{\mathbf{V}'}(x) = \left(x + \sum_{l=1}^{n-1}\lambda_l\right)\prod_{l=1}^{n-1}(x - \lambda_l)$.
(d) $\mathbf{a}' = \{a'_0, a'_1, ...a'_{n-2}, 0\}$
(e) $P_{\mathbf{V}'}(x) = \sum_{k=1}^{n-1}(v_k - v_0)x^k$.
(f) $P_{\mathbf{V}'}\left(e^{\frac{2\pi\imath}{n}l}\right) = \begin{cases} \lambda_0 - nv_0 & \text{for } l = 0 \\ \lambda_l & \text{for } l = 1, 2, ..., n-1 \end{cases}$.
(g) $\text{trace}(\mathbf{V}') = 0$.

(3) Show that the $n \times n$ circulant matrices with trace 0 form a $(n-1)$-dimensional subspace of $\text{Circ}(n)$.

(4) Let $\alpha \in \mathbb{C}$. Show that there exists a

$$\mathbf{v}'' = (v''_0, v''_1, ..., v''_{n-1}) \in \mathbb{C}^n$$

such that (with notation as in the first exercise)

$$\lambda_{\mathbf{V}''} = \{\lambda_0 - \alpha, \lambda_1 - \alpha, ...\lambda_{n-1} - \alpha\} = \lambda_{\mathbf{V}} - \alpha\mathbf{J}.$$

Show that

(a) $p_{\mathbf{V}''}(x) = p_{\mathbf{V}}(x + \alpha) = \det((x + \alpha)I - \mathbf{V})$.

(b) $\text{trace}(\mathbf{V}'') = \text{trace}(\mathbf{V}) - n\alpha$ and hence that for $\alpha = v_0$, $\text{trace}(\mathbf{V}'') = 0$.
(c) $\mathbf{a}'' = \{a_0'', a_1'', ...a_{n-2}'', 0\}$.
(d) $P_{\mathbf{V}''}\left(e^{\frac{2\pi\imath}{n}l}\right) = \lambda_l - \alpha$ for $l = 0, 1, ..., n-1$.

3. Roots of polynomials of small degree

The last corollary and the interplay between the characteristic polynomial p_V of a circulant matrix V and its representer P_V leads us to a method for finding roots of (monic) polynomials of degree less than or equal to 4.

The roots of the characteristic polynomial of an arbitrary $n \times n$ matrix V (these are the eigenvalues of the matrix V) are obtained by solving a monic n-degree polynomial equation. However, in the case of circulant matrices V, the roots of p_V are easily calculated using the *auxiliary companion* polynomial P_V, the representer of V. Thus if a given polynomial p is known to be the characteristic polynomial of a KNOWN circulant matrix V, its zeros can be readily found. This remark is the basis the method we will describe for solving polynomials of low degree. It is thus of considerable interest to determine which monic polynomials are characteristic polynomials of circulant matrices. Further, if we are given that $p = p_V$ for some circulant matrix V, can we determine V, or equivalently P_V, directly from p?

We can obviously recover V from its representer. If $\lambda = \{\lambda_0, \ldots, \lambda_{n-1}\}$ is an ordered set of eigenvalues (viewed in (28) as a column vector in $\mathbb{C}^n$), then there is a unique circulant matrix $V = \text{circ}\{v\} = \text{circ}\{v_0, v_1, \ldots, v_{n-1}\}$ whose ordered eigenvalues are λ:

$$v = \sqrt{n}C^{-1}\lambda\,. \tag{28}$$

If the eigenvalues are distinct, then there are precisely $n!$ ordered sets of eigenvalues producing the same characteristic polynomial. In this case, there are $n!$ circulant matrices V with characteristic polynomial p_V. Corollary 7.20 tells us that for each such circulant matrix $V = \text{circ}\{v_0, ..., v_{n-1}\}$, $v_0 = \frac{1}{n}\sum_{l=0}^{n-1}\lambda_l$ is independent of the ordering of the eigenvalues; however, the v_i for $1 < i < n$ do depend on the ordering. If k is the number of distinct roots of the characteristic polynomial, then there are of course at least $k!$ circulant matrices with the given characteristic polynomial. In particular, every monic polynomial p is the characteristic polynomial of some circulant matrix V.

Definition 7.29. Let n be a positive integer, p be a monic n-th degree polynomial, and V an $n \times n$ circulant matrix. We say that V *adheres* to p or V is the *adhering* circulant matrix to p if $p = p_V$ (that is if p is the characteristic polynomial of V).

But the above argument avoids completely the issue of finding the roots of p, as the given construction of V from p started by assuming we had the roots of the polynomial. So the more difficult question is the construction of V (or equivalently, it representer P_V) in terms of the coefficients of the polynomial p.

We are now ready to state and try to solve the problem of interest. Let us consider a monic n-th degree polynomial p:

$$p(x) = x^n + \alpha_{n-1}x^{n-1} + \alpha_{n-2}x^{n-2} + ... + \alpha_1 x + \alpha_0, \tag{29}$$

where $\alpha_i \in \mathbb{C}$. A basic result in complex analysis (which we now use) tells us that the polynomial has precisely n roots, counting multiplicities. Thus there exist complex numbers β_i such that

$$p(x) = (x - \beta_1)(x - \beta_2)...(x - \beta_n).$$

The task is to find these roots β_i. Since

$$\alpha_{n-1} = -\sum_{i=1}^{n} \beta_i,$$

the substitution $y = x + \frac{\alpha_{n-1}}{n}$ eliminates the term of degree $n-1$; that is, it changes (29) to

$$q(y) = p\left(y - \frac{\alpha_{n-1}}{n}\right) = y^n + \gamma_{n-2}x^{n-2} + ... + \gamma_1 y + \gamma_0, \tag{30}$$

where the constants γ_j are easily computed in terms of the α_i. If we can solve equation (30), then we can certainly also solve (29) since

$$q(y) = \left(y - \beta_1 - \frac{\alpha_{n-1}}{n}\right)\left(y - \beta_2 - \frac{\alpha_{n-1}}{n}\right) ... \left(y - \beta_n - \frac{\alpha_{n-1}}{n}\right).$$

In the notation of the last set of exercises, if $p = p_{\mathbf{V}}$, then $q = p_{\mathbf{V}''}$, where we use $\alpha = \frac{\alpha_{n-1}}{n}$ in the definition of $\mathbf{V}''$.

3.1. Roots of linear and quadratic polynomials. The solution of the linear monic equation

$$x + \alpha_0$$

does not present any problems; so we proceed to the quadratic monic equation (still only a warm-up exercise)

$$x^2 + \alpha_1 x + \alpha_0. \tag{31}$$

The classical solution of the last equation is based on completing the square; rewriting it as

$$x^2 + \alpha_1 x + \left(\frac{\alpha_1}{2}\right)^2 + \alpha_0 - \frac{\alpha_1^2}{4} = \left(x + \frac{\alpha_1}{2}\right)^2 + \alpha_0 - \frac{\alpha_1^2}{4};$$

thus its roots are

$$x = -\frac{\alpha_1}{2} \pm \sqrt{\frac{\alpha_1^2}{4} - \alpha_0}.$$

As a warm-up exercise we use circulant matrices to solve for the roots of (31). We are looking for a circulant 2×2 matrix

$$V = \begin{bmatrix} a & b \\ b & a \end{bmatrix}$$

whose characteristic polynomial

$$p_V(x) = \det \begin{bmatrix} x-a & -b \\ -b & x-a \end{bmatrix} = x^2 - 2ax + a^2 - b^2$$

equals (31). We are thus required to solve

$$\begin{array}{rcl} -2a & = & \alpha_1 \\ a^2 - b^2 & = & \alpha_0 \end{array}.$$

The solution is easily seen to be

$$a = -\frac{\alpha_1}{2} \text{ and } b = \sqrt{\frac{\alpha_1^2}{4} - \alpha_0}.$$

There are in general, of course, two square roots of the complex number $\frac{\alpha_1^2}{4} - \alpha_0$, we choose one of them. The representer for V is hence the polynomial

$$P_V(x) = \left(\sqrt{\frac{\alpha_1^2}{4} - \alpha_0} \right) x - \frac{\alpha_1}{2}.$$

Thus the roots of the original quadratic polynomial (31) (which is also p_V) are

$$P_V(1) = -\frac{\alpha_1}{2} + \sqrt{\frac{\alpha_1^2}{4} - \alpha_0}$$

and

$$P_V(-1) = -\frac{\alpha_1}{2} - \sqrt{\frac{\alpha_1^2}{4} - \alpha_0}.$$

We observe, as expected, that a our choice of the square root of $\frac{\alpha_1^2}{4} - \alpha_0$ only affected the order of the roots we found.

We leave it to the reader to recast the above discussion in terms of 2×2 circulant matrices of trace 0.

3.2. The general case. We are now given the monic n-th degree polynomial p of (29) and we are trying to find a circulant matrix $V = \text{circ}\{v\} = \text{circ}\{v_0, v_1, \ldots, v_{n-1}\}$ whose characteristic polynomial

$$p_V(x) = \det(xI - V) = \det \begin{bmatrix} x - v_0 & -v_1 & \cdots & -v_{n-2} & -v_{n-1} \\ -v_{n-1} & x - v_0 & \cdots & -v_{n-3} & -v_{n-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ -v_2 & -v_3 & \cdots & x - v_0 & -v_1 \\ -v_1 & -v_2 & \cdots & -v_{n-1} & x - v_0 \end{bmatrix}$$

$$= x^n - \left(\sum_{i=0}^{n-1} v_i \right) x^{n-1} + \ldots$$

is equal to p, the polynomial whose roots we are trying to find. We are thus attempting to solve for the n unknown v_i in n-equations; the first of these is

$$\alpha_{n-1} = \sum_{i=0}^{n-1} v_i = \text{ trace}(V).$$

We have already seen that we can make a simple change of variable to eliminate the term of degree $n-1$ in the equation (29) and hence solve for the roots of (30). We are thus looking for a traceless circulant matrix V; the first equation to be solved is now

$$0 = \sum_{i=0}^{n-1} v_i = \text{ trace}(V).$$

We will use this reduction in the next two subsections.

3.3. Roots of cubics. We start with the normalized[4] monic cubic

$$q(y) = y^3 + \beta y + \gamma$$

and look for a traceless circulant matrix

$$C = \begin{bmatrix} 0 & b & c \\ c & 0 & b \\ b & c & 0 \end{bmatrix}$$

whose characteristic polynomial

$$\det(yI - C) = \begin{bmatrix} y & -b & -c \\ -c & y & -b \\ -b & -c & y \end{bmatrix} = y^3 - 3bcy - (b^3 + c^3)$$

equals $q(y)$. The equations to be solved for b and c are

$$b^3 + c^3 = -\gamma \text{ and } 3bc = -\beta.$$

Cubing the last equation we solve for b^3 and c^3 in

$$b^3 + c^3 = -\gamma \text{ and } 27b^3c^3 = -\beta^3.$$

Replacing, as is permitted by the second equation, for example, c^3 by $-\frac{\beta^3}{27b^3}$ in the first of these equations and then using the quadratic formula we conclude that

$$b^3 = \frac{-\gamma \pm \sqrt{\gamma^2 + \frac{4\beta^3}{27}}}{2}.$$

The same formula holds for c^3, however we must choose square roots consistently. Thus having chosen one square root

$$b^3 = \frac{-\gamma + \sqrt{\gamma^2 + \frac{4\beta^3}{27}}}{2},\ c^3 = \frac{-\gamma - \sqrt{\gamma^2 + \frac{4\beta^3}{27}}}{2}.$$

We must use a little care, as suggested by the last displayed equation, because we are working with complex numbers. We choose one of the six[5] possible values of

$$b = \left(\frac{-\gamma \pm \sqrt{\gamma^2 + \frac{4\beta^3}{27}}}{2} \right)^{\frac{1}{3}}.$$

We then set

$$c = \frac{-\beta}{3b}.$$

To keep track of what is going on, let us write

$$2b^3 = -\gamma + \delta,\ \delta^2 = \gamma^2 + \frac{4\beta^3}{27},$$

[4]To have 0 as the coefficient of its quadratic term.

[5]In the generic case.

and observe that the definition of δ involves a choice of a square root and that the resulting δ may be replaced by $-\delta$ and the resulting two values of b may each be replaced by $\omega^j b$ with $\omega = e^{\frac{2\pi\imath}{3}}$ and $j = 1$ or 2. The values of b and c are described by

$$b = \left(\frac{-\gamma+\delta}{2}\right)^{\frac{1}{3}} \text{ and } c = \left(\frac{-\gamma-\delta}{2}\right)^{\frac{1}{3}};$$

it follows from these equations that $3bc = -(\beta^3)^{\frac{1}{3}}$. Having chosen a cube root in the formula for b, the correct cube root must be chosen in the formula for c so that the last equation becomes $3bc = -\beta$. With these conventions in mind, the three roots of q can now be written as $P(\omega^j)$ with $j = 0, 1, 2$ where

$$P(y) = by + cy^2.$$

Thus the roots are

$$r_1 = b + c = \left(\frac{-\gamma+\delta}{2}\right)^{\frac{1}{3}} + \left(\frac{-\gamma-\delta}{2}\right)^{\frac{1}{3}},$$

$$r_2 = b\omega + c\omega^2 = \omega\left(\frac{-\gamma+\delta}{2}\right)^{\frac{1}{3}} + \omega^2\left(\frac{-\gamma-\delta}{2}\right)^{\frac{1}{3}}$$

and

$$r_3 = b\omega^2 + c\omega = \omega^2\left(\frac{-\gamma+\delta}{2}\right)^{\frac{1}{3}} + \omega\left(\frac{-\gamma-\delta}{2}\right)^{\frac{1}{3}}.$$

We can determine the effect of the various choices made on the values of the roots. Replacing δ by $-\delta$, certainly interchanges b and c. Hence r_1 is fixed while r_2 and r_3 are permuted. Keeping δ fixed and replacing a cube root choice, say b by ωb (the only other possibility is $\omega^2 b$ results in the replacement of say c by $\omega^2 c$. Thus r_1 is replaced by r_2, r_2 by r_3 and hence (without the need of a calculation) r_3 by r_1. In general, the various choices made correspond to the action of the symmetric group $S(3)$ on the roots of the monic cubic polynomial.

If we start with the general monic cubic

$$p(x) = x^3 + \alpha_2 x^2 + \alpha_1 x + \alpha_0,$$

then the change of variable $y = x - \frac{\alpha_2}{3}$ reduces us to the normalized case with

$$\beta = -\frac{1}{3}\alpha_2^2 + \alpha_1 \text{ and } \gamma = \frac{2}{27}\alpha_2^3 - \frac{1}{3}\alpha_2\alpha_1 + \alpha_0.$$

3.4. Roots of quartics. To find the roots of the normalized monic quartic

$$q(y) = y^4 + \beta y^2 + \gamma y + \delta$$

we look for a traceless 4×4 circulant matrix

$$C = \begin{bmatrix} 0 & b & c & d \\ d & 0 & b & c \\ c & d & 0 & b \\ b & c & d & 0 \end{bmatrix}$$

whose characteristic polynomial

$$\det(yI-C) = \begin{bmatrix} y & -b & -c & -d \\ -d & y & -b & -c \\ -c & -d & y & -b \\ -b & -c & -d & y \end{bmatrix} = y^4-(4bd+2c^2)y^2-4c(b^2+d^2)y+c^4-b^4-d^4-4bc^2d+2b^2d^2$$

equals $q(y)$. We thus have to solve for b, c and d the system

$$\begin{array}{rcl} 4bd + 2c^2 &=& -\beta \\ 4c(b^2 + d^2) &=& -\gamma \\ c^4 - b^4 - d^4 - 4bc^2d + 2b^2d^2 &=& \delta \end{array} . \tag{32}$$

Assume for the moment that $c \neq 0$. In this case, the first and second equations of (32) can be rewritten as

$$bd = -\frac{\beta + 2c^2}{4} \text{ and } b^2 + d^2 = -\frac{\gamma}{4c}, \tag{33}$$

they determine bd and $b^2 + d^2$ in terms of c. This suggests that the third equation of (32) be rewritten as

$$c^4 - 4bdc^2 - (b^2 + d^2)^2 + 4(bd)^2 = \delta.$$

Substitution of (33) into this equation and clearing fractions leads us to

$$c^6 + \frac{\beta}{2}c^4 + \left(\frac{\beta^2}{16} - \frac{\delta}{4}\right)c^2 - \frac{\gamma^2}{64} = 0; \tag{34}$$

a monic (not normalized) cubic in c^2 that can be solved by the methods of the previous subsection. Choose one non-zero root c of (34). This is possible since 0 is a root of (34) if and only if $\gamma = 0$; while all the roots of this equation are 0 if and only if $\beta = 0 = \delta = \gamma$. Using this value of c, we solve for b and d in (33). The roots of $q(x)$ are then the values at 1, $\imath$, -1 and $-\imath$ of the representer

$$P(y) = by + cy^2 + dy^3$$

of the circulant matrix C. If $\gamma = 0$, we can of course use $c = 0$ and solve for b and d in

$$4bd = -\beta \text{ and } b^2 - d^2 = \sqrt{-\delta}.$$

The various choices made lead to an action of $S(4)$ on the roots of q. We illustrate the various ideas encountered with a MAPLE program to solve the equation

$$x^4 - 10x^3 + 35x^2 - 50x + 24 = 0.$$

MAPLE SESSION #xx

```
> p := x -> x^4 - 10 * x^3 + 35 * x^2 - 50 * x + 24;
```

$$p := x \to x^4 - 10\,x^3 + 35\,x^2 - 50\,x + 24$$

```
> solve(p(x) = 0,x);
```

$$1,\ 2,\ 3,\ 4$$

```
> q := y -> p(y + 5/2);
```

$$q := y \to \mathrm{p}(y + \frac{5}{2})$$

```
> expand(q(y));
```

$$y^4 - \frac{5}{2}y^2 + \frac{9}{16}$$

```
> solve(z^2 - 5/2 * z + 9/16 = 0,z);
```

$$\frac{9}{4}, \frac{1}{4}$$

```
> beta := - 5/2:  gama := 0:  delta := 9/16:
> solve(t^3 + (beta/2) * t^2 + (beta^2/16 - delta/4) * t - gama^2/64 =
  0,t);
```

$$0,\ 1,\ \frac{1}{4}$$

```
> c := 0;
```

$$c := 0$$

```
> solve({4 * b * d = -beta, b^2 - d^2 = sqrt(-delta)},{b,d});
```

$$\{d = \frac{-1}{4} + \frac{3}{4}I,\ b = \frac{-1}{4} - \frac{3}{4}I\},\ \{d = \frac{1}{4} - \frac{3}{4}I,\ b = \frac{1}{4} + \frac{3}{4}I\},\ \{d = \frac{-3}{4} + \frac{1}{4}I,\ b = \frac{-3}{4} - \frac{1}{4}I\},$$
$$\{d = \frac{3}{4} - \frac{1}{4}I,\ b = \frac{3}{4} + \frac{1}{4}I\}$$

```
> b := -1/4 -3/4 * I: d := -1/4 + 3/4 * I:
> P := t -> b * t + c * t^2 + d * t^3;
```

$$P := t \to b\,t + c\,t^2 + d\,t^3$$

```
> P(1) + 5/2, P(I) + 5/2, P(-1) + 5/2, P(- I) + 5/2;
```

$$2,\ 4,\ 3,\ 1$$

END MAPLE PROGRAM

We describe the various steps of the above program.

(1) The first line of the program introduces the polynomial $p(x)$ to be solved.
(2) The second line uses the internal MAPLE command to solve this equation (as a check on our work).
(3) The third and fourth lines change the polynomial $p(x)$ to its normal form $q(x)$. We note that the roots of $p(x)$ are the roots of $q(x)$ plus $\frac{5}{2}$.
(4) The next line (again a check on our work) uses MAPLE to solve the normalized polynomial $q(x)$ – because it is a quadratic in y^2.
(5) Next, the constants defining the $q(x)$ are entered.
(6) We solve for the possible values of c and use $c = 0$. Thus we will use a circulant matrix of the form $V = \mathrm{circ}\{0, b, 0, d\}$.
(7) We proceed to solve for the possible values of b and d, and choose a solution set (out of the 4 possibilities).
(8) The last two commands calculate the roots of $p(x)$ using the representer $P(y)$ of V.

3.5. Real roots and roots of absolute value 1. We fix throughout this subsection an $n \in \mathbb{Z}_{>0}$, a monic n-th degree polynomial p and an $n \times n$ matrix $V \in \mathrm{Circ}(n)$ that adheres

to p. We are interested in learning what properties of p are reflected in V. Recall that in the case under study p is the characteristic polynomial of V.

THEOREM 7.30. *The monic polynomial p has only real roots if and only if its adhering circulant matrix V is Hermetian.*

PROOF. It is easy to see that a monic polynomial $p \in \mathbb{C}[x]$ with only real roots must belong to $\mathbb{R}[x]$ (that is, it must have real coefficients). A matrix V is Hermetian iff $V = \overline{V^t}$. We know from linear algebra that the eigenvalues of a Hermetian matrix are real. Thus if V is Hermetian, p has real roots. Conversely, if p has real roots, then V has real eigenvalues. Thus there exists an $n \times n$ real diagonal matrix D with $V = CD\overline{C^t}$ and C is defined by (26) (in particular, $C^{-1} = \overline{C^t}$). We now compute

$$\overline{V^t} = \overline{(CD\overline{C^t})^t} = \overline{\overline{C}DC^t} = CD\overline{C^t} = V;$$

thus V is Hermetian. □

Many other properties of $p(x)$ can be read off from V. We record some of these in

THEOREM 7.31. *Let p be a monic polynomial with adhering circulant matrix V. Then*
(a) *the roots of $p(x)$ are real if and only if V is Hermetian ($V = \overline{V^t}$),*
(b) *the roots of $p(x)$ have absolute value 1 if and only if V is unitary ($V^{-1} = \overline{V^t}$), and*
(c) *the roots of $p(x)$ are purely imaginary if and only if V is skew-Hermetian ($V = -\overline{V^t}$).*

3.6. What goes wrong for polynomials of higher degree? Will the method described in subsections 3.3 and 3.4 work on polynomials of degree ≥ 5? The answer to this question is a resounding NO, but that is a topic for an entirely different chapter of mathematics.

EXERCISES

(1) Using circulant matrices find the roots of each of the following polynomials.
   (a) $1 + 2x + x^3$.
   (b) $1 + 2x + x^2 + 3x^3$.
   (c) $1 + x + 2x^2 + x^4$.
   (d) $1 + x + 2x^2 + 3x^3 + x^4$.

(2) Complete the solution of the example worked out by the MAPLE program by choosing a value $c \neq 0$. What is the formula for the representer $P(y)$ in this case? What element of $S(4)$ is represented by permutation that changes the MAPLE solution to your solution?

(3) (a) Prove parts (b) and (c) of Theorem 7.31 using the ideas in the proof of Theorem 7.30 (part (a) of Theorem 7.30).
   (b) Deduce part (c) of Theorem 7.31 from Theorem 7.30 and the observation that a monic polynomial $p(x)$ of degree n has purely imaginary roots if and only if the monic polynomial $\frac{p(ix)}{i^n}$ has only real roots. Describe an adhering circulant matrix V for $p(x)$ in terms of one for $\frac{p(ix)}{i^n}$.

CHAPTER 8

Moduli for polynomials

Preliminary version of chapter. Written in a form that should be accessible to most high school mathematics teachers. Certain results from previous chapters are repeated here to make the presentation more self contained.

1. Polynomials in three guises

Let n be a positive integer. We will be dealing with expressions of the form

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_0, \tag{35}$$

or alternatively just the expression

$$a_n x^n + a_{n-1} x^{n-1} + ... + a_0, \tag{36}$$

where x is an *indeterminate* or *independent variable*, each a_i is a real number (or more generally, a complex number) and $a_n \neq 0$.

We call (36) an *n-th degree polynomial (with real or complex coefficients)*. Polynomials with real (complex) coefficients will be referred to as *real (complex)* polynomials. At times there are significant differences between the two cases. Polynomials can be manipulated using the usual rules of arithmetic; for example, replaceing x by $\alpha x + \beta$ with $\alpha \neq 0$ and β real or complex numbers transforms it into another n-th degree polynomial. An algebraist would say that (36) is an element of the integral domain $\mathbb{R}[x]$ or $\mathbb{C}[x]$.

It is quite clear that (36) and (35) are more or less the same object. The introduction of the extra symbol $p(x)$ or p in (35) reminds us that we may also think of a polynomial as a function

$$p : \mathbb{R} \to \mathbb{R} \text{ or } p : \mathbb{C} \to \mathbb{C},$$

with $p(x)$ denoting the value of this function at $x \in \mathbb{R}$ or $\mathbb{C}$, respectively. When viewed as a function from $\mathbb{C}$ to itself a real polynomial has the added feature of assuming real values at the real points in $\mathbb{C}$. The symbol p is the *dependent* variable and y is another common letter used to represent it. Associated to any funnction $f : \mathbb{R} \to \mathbb{R}$ is its *graph*; the set

$$\left\{(x, y) \in \mathbb{R}^2 \text{ such that } y = f(x)\right\}.$$

This set is often identified with the function f.

When discussing roots of the polynomail (36) or (35) we are looking for those x (usually in $\mathbb{C}$) that satisfy the equation

$$0 = a_n x^n + a_{n-1} x^{n-1} + ... + a_0.$$

2. An example from high school math: the quadratic polynomial

The study of first degree polynomials

$$l(x) = ax + b$$

with complex coefficients (a and b are complex numbers and $a \neq 0$) is certainly trivial for all high school mathematics teachers. The quadratic polynomial

$$y(x) = ax^2 + bx + c \tag{37}$$

with complex coefficients (a, b and c are complex numbers and $a \neq 0$) is only slightly more challenging. We present a treatment that is much more concise than the one found in many high school texts (for example in [**5**]). The graph of the *standard form of the real quadratic polynomial* $y(x) = x^2$ (the special case $a = 1$, $b = 0 = c$) is certainly familiar to every reader. By completing squares and applying elementary algebraic manipulations one easily concludes from (37) that

$$\frac{y}{a} = \left(x + \frac{b}{2a}\right)^2 + \left(\frac{c}{a} - \frac{b^2}{4a^2}\right). \tag{38}$$

This tells the complete story for quadratic polynomials:

- Every quadratic polynomial has two, perhaps complex, roots counting multiplicities.
- The roots of (37) are easily obtained from its equivalent form (38); they are
$$-\frac{b}{2a} \pm \frac{\sqrt{b^2 - 4ac}}{2a}.$$
- For real quadratic polynomials, the roots are real and distinct if the *discriminant* $b^2 - 4ac$ of the polynomial is positive.
- There is one double real root if the discriminant vanishes.
- There is a pair of conjugate complex roots if the discriminant is negative.
- The linear change of coordinates
$$X = x + \frac{b}{2a} \text{ and } Y = \frac{y}{a} + \frac{b^2 - 4ac}{4a^2}$$
transforms (37) (and (38), of course) to standard form $Y = X^2$.

Up to change of coordinates, this is all there is to quadratic polynomials; that is, the general quadratic polynomial $ax^2 + bx + c$ is obtained from the standard quadratic x^2 by first pre-composing with the affine map $x \mapsto x + \frac{b}{2a}$ and then post-composing with the affine map $x \mapsto ax + c - \frac{b^2}{4a}$. We illustrate the concept of change of coordinates in Figure 1 with an example that hints at the important equivalence relation we are about to introduce.

We do not claim this approach is the way an excellent teacher would present the quadratic to a high school audience, but rather that every competent high school mathematics teacher should be aware of this elegant and short treatment.

3. An equivalence relation

If we start, in general, with a polynomial $y = y(x)$ in the independent variable x and use the linear change of both independent and dependent variables

$$X = ax + b, \quad Y = cy + d,$$

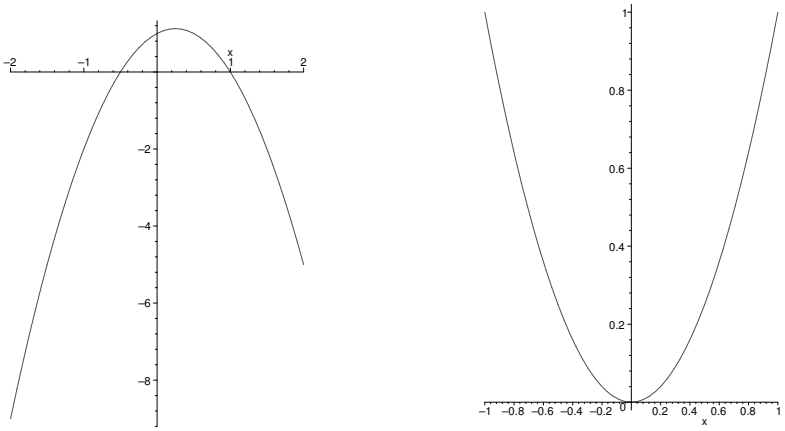


FIGURE 1. On the left is the graph of $y = -2x^2 + x + 1$. Apply the change of coordinates $X = x - \frac{1}{4},\ Y = \frac{y}{2} + \frac{9}{16}$ to get the standard form $Y = X^2$ graphed on the right.

where a, b, c and d are complex constants with $ac \neq 0$, we obtain a polynomial $Y = Y(X)$ in a new independent variable X. Notice we can write $Y(X) = Y(ax + b) = cy(ax + b) + d$. We consider these two polynomials to be *equivalent*. Of course, equivalent polynomials share many properties. Most importantly, the real or complex number $x = r$ is a *root* of y (so $y(r) = 0$) if and only if the polynomial Y evaluated at $X = ar + b$ equals d. In particular, if the dependent variable is not subject to a translation (that is, if $d = 0$), then r is a root of $y(x)$ if and only if $ar + b$ is a root of $Y(X)$, or equivalently, $\frac{r-b}{a}$ is a root of $Y(ax + b)$.

We emphasize that our changes of coordinates allow translations, resizing, and sign changes in both the independent and dependent variables. We may consider only real polynomials and work only with real affine maps. Let us examine the situation in a more formal way.

First degree polynomials are also called *affine maps* of the complex plane $\mathbb{C}$. They form a group under composition (composing two affine maps generates a third one). We denote by $L^{-1}(x)$ the inverse of the affine map $L(x)$ in this group[1]. Our equivalence relation (which we will denote by the symbol $\equiv$) is actually independent of the dependent variable y: The polynomial $p(x)$ is *equivalent* to the polynomial $q(x)$ if $q(x)$ can be obtained from $p(x)$ by pre-composition and post-composition with affine maps; that is, if and only if there exist affine maps $L_1(x)$ and $L_2(x)$ such that

$$q(x) = L_2(p(L_1(x))). \tag{39}$$

We note that every polynomial $p(x)$ is equivalent to itself since the identity map is affine. If $p(x) \equiv q(x)$, then there existaffine maps L_1 and L_2 such that (39) holds, and thus

$$p(x) = L_2^{-1}\left(q\left(L_1^{-1}(x)\right)\right);$$

or $q(x) \equiv p(x)$. Finally, if $p_1(x) \equiv p_2(x)$ and $p_2(x) \equiv p_3(x)$, then there exist affine maps L_i, $i = 1,\ 2,\ 3,\ 4$ such that

$$p_2(x) = L_2(p_1(L_1(x))) \text{ and } p_3(x) = L_4(p_2(L_3(x))).$$

[1]The notation is meant to emphasize the fact affine maps are polynomials of degree one.

Thus

$$p_3(x) = L_4(L_2(p_1(L_1(L_3(x)))))$$

or $p_1(x) \equiv p_3(x)$.

4. An example all high school math teachers should know: the cubic polynomial

To understand what is going on with quadratic polynomials, one should be able to answer several questions. How much of the development of §2 carries over to arbitrary real or complex polynomials (of degree 3 or higher); how much is peculiar to quadratics? What do these questions mean?

An example more challenging than the quadratic polynomial is the real or complex cubic

$$p(x) = y = ax^3 + bx^2 + cx + d, \tag{40}$$

with a, b, c and d real or complex numbers and $a \neq 0$.

If $p(x) \in \mathbb{R}[x]$, then by the intermediate value theorem, $p(x)$ must have at least one real root r. It follows that

$$\frac{p(x)}{x - r} = ax^2 + \beta x + \gamma$$

for some real constants β and γ, so that the analysis of the cubic $p(x) \in \mathbb{R}[x]$ can be reduced to a study of the quadratic $ax^2 + \beta x + \gamma$. We follow a slight variation of this observation; in prt, because it does not tell us how to find r algebraically. But first, we make a small digression to observe some facts about

5. Arbitrary real or complex polynomials

Let us return to the arbitrary n-th degree real or complex polynomial (35). A basic fact is the **Fundamental theorem of algebra**, whose easiest proof is via complex analysis (see, for example, [**1**, page 122]): such a polynomial has precisely n-complex roots[2]. Because of the division algorithm, this implies that

$$p(x) = a_n(x - r_1)(x - r_2)....(x - r_n),$$

where each of the r_i is a (complex) *root* of $p(x)$. In case the polynomial has real coefficients, we find that if $r \in \mathbb{C}$ is a root of (35), then so is its complex conjugate $\bar{r}$. The proof of this assertion is rather easy. The fact that $0 = p(r)$ tells us that

$$0 = \overline{p(r)} = \overline{\sum_{i=0}^{n} a_i r^i} = \sum_{i=0}^{n} a_i \bar{r}^i = p(\bar{r}),$$

so that $\bar{r}$ is a root of (35). We claim more: if the complex number r is a root of *multiplicity* k of (35) (that is, precisely k of the r_i equal r), then so is $\bar{r}$. The easiest proof of this assertion is by induction on the degree of the polynomial. We may and do assume that $r \notin \mathbb{R}$ since otherwise there is nothing to prove. We may also assume that $n \geq 3$ and $k \geq 2$ because otherwise there once again is nothing to prove. Our assertion holds for $n = 3$, because in this case we have at least one real root, so $k = 1$. Now assume $n > 3$ and the complex number r is a root of $p(x)$ of multiplicity k. We already know $\bar{r} \neq r$ is also a root of $p(x)$. Note that

$$(x - r)(x - \bar{r}) = x^2 - (r + \bar{r})x + r\bar{r},$$

[2]Even for real polunomials, the roots may be complex.

with both $r + \bar{r}$ and $r\bar{r}$ real numbers. Hence

$$q(x) = \frac{p(x)}{x^2 - (r + \bar{r})x + r\bar{r}}$$

is a real polynomial of degree $n - 2$ having r as a complex root of multiplicity $k - 1$. By complete induction $\bar{r}$ is also a complex root of multiplicity $k - 1$ of $q(x)$. Hence a root of multiplicity k of $p(x)$.

6. Back to the cubic polynomial

We begin a leisurely exploration of the real cubic. The study of the real cubic polynomial (40) does not require the material of the last section, except for the fact that non-real roots come in pairs (a complex number and its conjugate). We start with the useful, if trivial, general observation already encountered in §3. Let a and $b \in \mathbb{R}$ with $a \neq 0$, then r is a root of $p(x)$ if and only if $\frac{r-b}{a}$ is a root of $p(ax + b)$.

As observed earlier, $p(x)$ must have at least one real root. Therefore we have either 1, 2 or 3 distinct real roots. We consider cases:

(1) Exactly one real root.
- This root could have multiplicity three. A good example is the special case $p_1(x) = x^3$ whose graph is shown below.

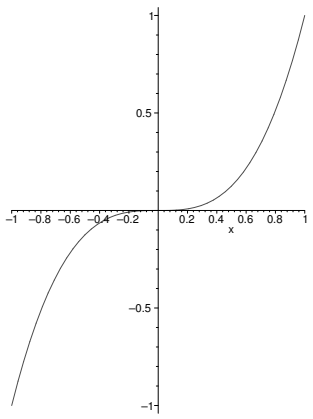


FIGURE 2. $y = x^3$

The general case $p_2(x) = a(x-b)^3$, where a and b are real numbers with $a \neq 0$, is reduced to the special case by the change of coordinates $P = \frac{p_2}{a}$ and $X = x - b$.
- This root could not have multiplicity two. If it did $p(x)$ would have to have 4 roots, counting multiplicities, of course.
- This root could have multiplicity one. In this case, the polynomial must have a pair of complex roots. A typical example here is $p_3(x) = x(x^2 + 1)$ whose graph is shown below.
  The general equation here is of the form $p_4(x) = c(x - r)(x^2 + \alpha x + \beta)$ with c, r, α, β real numbers, $c \neq 0$ and $\alpha^2 - 4\beta < 0$. If we make the change of variable $x = aX + b$ with $a \neq 0$ and b real, we transform the general equation to

$$p(aX + b) = c(aX + b - r)(a^2X^2 + (2ab + \alpha a)X + (b^2 + \alpha b + \beta)).$$

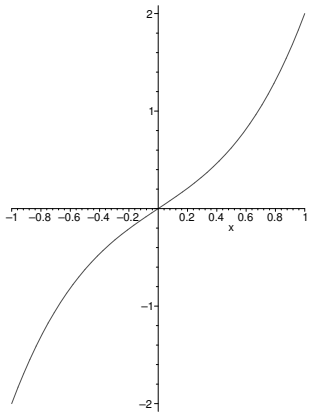


FIGURE 3. $y = x(x^2 + 1)$

We now set $b = r$ (thus placing the one real root at the origin) and consider two cases:

- If $\alpha = -2r$, we conclude that $p_4(aX + r) = caX(a^2X^2 + (\beta - r^2))$ and after further change of variables we reduce the equation to the form
$$P(X) = X(X^2 + d), \quad d > 0.$$
- If $\alpha \neq -2r$, we cannot kill the first degree term in the quadratic polynomial $a^2X^2 + (2ab + \alpha a)X + (b^2 + \alpha b + \beta)$. If $p(x)$ has complex roots at ρ and $\bar{\rho}$, then $p(aX + r)$ has complex roots at $\frac{\rho - r}{a}$ and $\frac{\bar{\rho} - r}{a}$. By properly choosing a, we can ensure that the roots of the polynomial $p(aX + r)$ are at 0 and $e \pm \imath$ for some real number e. Thus we conclude, with proper choices for a and b,
$$p(aX + b) = dX(X^2 - 2eX + (e^2 + 1))$$
for some non-zero real number d. So the standard form of our polynomial in this case is
$$P(X) = X(X^2 - 2eX + (e^2 + 1)) \text{ for some } e \in \mathbb{R}.$$

We graph another example: $p_5(x) = (x + 2)(x^2 - 2x + 3)$ which will shortly lead us to reconsider our approach.

(2) Exactly two distinct real roots.
In this case one of the roots must have multiplicity one and the other multiplicity two. A typical example is $p_6(x) = x(x - 1)^2$ whose graph is shown below

The general case is $p_7(x) = c(x - r_1)(x - r_2)^2$ with c, r_1 and r_2 real constants, $c \neq 0$ and $r_1 \neq r_2$. The change of variables $x = (r_2 - r_1)X + r_1$, $P = \frac{p}{c}$ reduces the general case to the typical example.

(3) Three distinct real roots.
A typical example is $p_8(x) = x(x+1)(x-1)$ whose graph is once again shown below

The general case is $p(x) = c(x - r_1)(x - r_2)(x - r_3)$ with $0 \neq c \in \mathbb{R}$ and r_1, r_2 and r_3 three distinct real numbers. The change of variables $x = (r_2 - r_1)X + r_1$, $P = \frac{p}{c}$ reduces the general case to the standard form
$$P(X) = X(X - 1)(X - \alpha), \text{ with } \alpha \in \mathbb{R}, \ 0 \neq \alpha \neq 1.$$

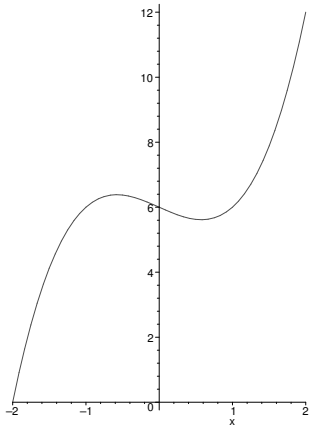


FIGURE 4. $y = (x + 2)(x^2 - 2x + 3)$

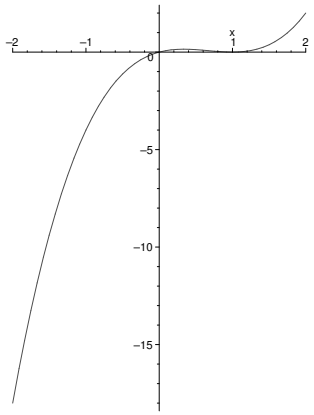


FIGURE 5. $y = x(x - 1)^2$

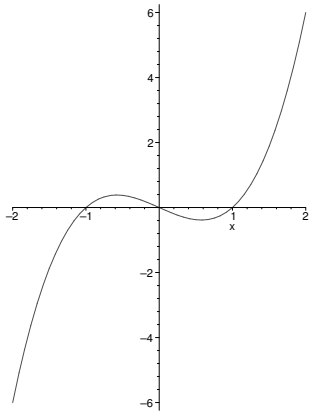


FIGURE 6. $y = x(x + 1)(x - 1) = x(x^2 - 1)$

The reader should notice a striking similarity between the graphs of p_5 (Figure 4) and p_8 (Figure 6). This is, of course, not a coincidence. As can easily be seen,

$$p_5(x) = p_8(x) + 6.$$

This suggests that we have not paid sufficient attention to the dependent variable. We now make a "bold" conjecture: If y is a cubic with 3 distinct real roots, there is a constant c such that $y + c$ has precisely one simple real root (and thus also a pair of complex roots). In verifying this claim, we may assume that $\lim_{x\to-\infty} y(x) = -\infty$, since we can replace y by $-y$ if this is not the case. Let $r_1 < r_2 < r_3$ be the three roots of the cubic. From calculus we know that the restriction of y to the closed interval $[r_2, r_3]$ has a negative minimum $-c$ at some point $x_o \in (r_2, r_3)$. So the function $y+2c$ has precisely one simple real root. Therefore, in the classification of cubic polynomials up to equivalence, we may ignore the case of three distinct real roots.

The above analysis on the structure of the roots of the real cubic can also be obtained in a very straight forward manner. As we have seen, we can think of the general cubic as the product of a linear term and a quadratic term. The quadratic term can have either no real roots, one real root of multiplicity two, or two distinct real roots, while the linear term must have exactly one simple real root. If the quadratic term has no real roots, then the cubic must have exactly one real root of multiplicity one and two complex conjugate roots. If the quadratic term has one real root of multiplicity two, then the cubic must have either two real roots (a simple one from the linear term and the one of multiplicity two from the quadratic term), or one real root of multiplicity three (if the linear and quadratic roots coincide). If the quadratic term has two distinct real roots, then the cubic has either three distinct real roots, or again, one root of multiplicity one, and one root of multiplicity two.

7. Standard forms for cubics

The above analysis does not produce a satisfactory set of standard forms for cubics. To obtain a more satisfactory set, we start with the arbitrary real cubic polynomial (40) and describe an *algorithm* consisting of a series of steps, not all intuitive, which reduces it to standard form.[3] We work only with real affine maps in this reduction process.

(1) By rescaling the dependent variable, replacing y by ay, we may assume $a = 1$.
(2) Completing the cube, replacing x by $x - \frac{b}{3}$, allows us to assume $b = 0$.
(3) If $c = 0$ we proceed to the next step. Otherwise, we resize both the dependent (replacing y by $|c|^{\frac{3}{2}}y$) and independent variables (replacing x by $x\sqrt{|c|}$), allowing us to assume $c = \pm 1$. (The case $+1$ occurs when $c > 0$ and -1 when $c < 0$.)
(4) A final translation of the dependent variable (replacing y by $y + d$) reduces the original equation to standard form

$$P(x) = x^3 + \epsilon x,\ \epsilon = -1,\ 0 \text{ or } 1. \tag{41}$$

We show next that no two of these three polynomials are equivalent. As we have seen, the family of cubics equivalent to $y = x^3$ can be written $c(ax + b)^3 + d$ with a, b, c and d real and $ac \neq 0$. But

$$c(ax + b)^3 + d = a^3cx^3 + 3a^2bcx^2 + 3ab^2cx + b^3c + d.$$

So for $x^3 + x$ or $x^3 - x$ to be in this family, we would need $a^2bc = 0$ and $ab^2c \neq 0$. Similarly, the family of cubics equivalent to $x^3 + x$ can be written $c[(ax + b)^3 + (ax + b)] + d$. If we want to reduce this to $x^3 - x$ we must have $b = 0 = d$, which gives the family $a^3cx^3 + acx$. But now we would require $a^3c = 1$ and $ac = -1$ so $a^2 = -1$ and a could not be real.

[3]The values of the constants a, b, c and d keep changing during the process.

It is important to realize that while the development of this section did not rely on the intermediate value theorem, it has NOT established the existence of a real root for every cubic.

Much of our discussion of cubics is accessible to bright high school students and it leads us to several natural questions; some that students can pursue. Every third degree polynomial belongs to one of three equivalence classes. How do we determine which equivalence class contains a specific polynomial. Are there common characteristics shared by all polynomials in an equivalence class? If so, what are they? Note that multiplicities of roots is not constant over an equivalence class. The polynomials $x^3 - x$ and $x(x-1)^2$ are in the same equivalence class; the first of these has three simple roots and the second only two distinct roots (precisely one of these of multiplicity 2).

We have seen that there are only three equivalence classes of cubic equation and that representatives for these classes are described by the standard forms (41). These three equations are easily solved. If $\epsilon = 0$, then 0 is a root of multiplicy 3; if $\epsilon = -1$, then 0 and ± 1 are simple roots, and if $\epsilon = 1$, then 0 and $\pm\imath$ are simple roots. Does this information help us solve the genral cubic $p(x)$ given by (40)? We know that there are four real constants α, β, γ and δ such that $\alpha\gamma \neq 0$ and

$$ax^3 + bx^2 + cx + d = \alpha\left[(\gamma x + \delta)^3 + \epsilon(\gamma x + \delta)\right] + \beta. \tag{42}$$

The unknown constants are easily determined. Equating the coefficients of the same powers of x in (42) leads to four equations:

$$a = \alpha\gamma^3,$$
$$b = 3\alpha\gamma^2\delta,$$
$$c = \alpha\gamma\left[3\delta^2 + \epsilon\right]$$

and

$$d = \alpha\delta\left[\delta^2 + \epsilon\right] + \beta,$$

and we seem to have replaced solving a single cubic equation with solving four equations in four unknowns that also involve cubics – not obviously a simpler problem. Again a change of course is useful. There exist affine maps L_1 and L_2 such that

$$L_2\left[a(L_1(x)^3) + b(L_1(x)^2) + cL_1(x) + d\right] = x^3 + \epsilon x$$

with $\epsilon = 0$ or ± 1. The algorithm described at the begining of this section tells us how to compute the two affine maps. We find that

$$L_1(x) = x - \frac{b}{3a} \text{ and } L_2(x) = \frac{1}{a}x - \left(\frac{2b^3}{27a^3} - \frac{bc}{3a^2} + \frac{d}{a}\right) = \frac{1}{a}x + \frac{9ad - bc}{9a^2}$$

when $b^2 - 3ac = 0$ (in this case $\epsilon = 0$). If $b^2 - 3ac \neq 0$, then

$$L_1(x) = \sqrt{\left|\frac{b^2 - 3ac}{3a}\right|}x - \frac{b}{3a} \text{ and } L_2(x) = \frac{1}{a\left|\frac{b^2-3ac}{3a}\right|^{\frac{3}{2}}}x - \frac{\left(\frac{2b^3}{27a^3} - \frac{bc}{3a^2} + \frac{d}{a}\right)}{\left|\frac{b^2-3ac}{3a}\right|^{\frac{3}{2}}}$$

with $\epsilon = 1$ if $b^2 - 3ac < 0$, and $\epsilon = -1$ if $b^2 - 3ac > 0$.

Inverting L_1 and L_2, we conclude that if $b^2 - 3ac = 0$ then

$$\alpha = a,\ \beta = \frac{9ad - bc}{9a},\ \gamma = 1,\ \delta = \frac{b}{3a}$$

and

$$\alpha = a\left|\frac{b^2-3ac}{3a}\right|^{\frac{3}{2}},\ \beta = \frac{2b^3}{27a^2} - \frac{bc}{3a} + d,\ \gamma = \left|\frac{b^2-3ac}{3a}\right|^{-\frac{1}{2}},\ \delta = \frac{b}{3a\left|\frac{b^2-3ac}{3a}\right|^{\frac{1}{2}}}$$

if $b^2 - 3ac \neq 0$. We are looking for the zeros (roots) of the left hand side of of (42). Using the right hand side of that equation we need to find the complex numbers r such that for $P(x) = x^3 + \epsilon x$, we have $P(\gamma r + \delta) = -\frac{\beta}{\alpha}$. So[4] the problem reduces to solving the equation

$$x^3 + \epsilon x - 2\eta = 0,\ \eta = -\frac{\beta}{2\alpha} \in \mathbb{R}. \tag{43}$$

The above discussion assumed that we were dealing with a real cubic. What changes need to be made for a general cubic? In studying the complex cubic, it is natural to consider complex affine maps in the definition of equivalence of polynomials. One can easily be convinced that in this setting the two cubics $x^3 + x$ and $x^3 - x$ are equivalent, but neither of these is equivalent to the cubic x^3 – resulting in two rather than three equivalence classes of complex cubics.

8. Solving the cubic

We continue with the notation of the previous section and aim to solve (43). Assume, however, that the two constants ϵ and $\eta \in \mathbb{C}^*$. We follow a method discovered by the sixteenth century Italian mathematician Girolama Cardano (and probably many others). Let us write

$$x = y + z.$$

This may seem like an unnecessary complication, but it actually gives us additional freedom, because we will be able to introduce a convenient side relation between y and z. Algebraic manipulations transform (43) to

$$(y^3 + z^3) + (y + z)(3yz + \epsilon) - 2\eta = 0.$$

This last formula reveals the appropriate side condition:

$$3yz + \epsilon = 0,$$

and thus leads us to consider the system

$$y^3 z^3 = -\frac{\epsilon^3}{3^3},\quad y^3 + z^3 = 2\eta.$$

But look! This reduces the problem to solving a quadratic equation (in y^3)

$$y^3 - 2\eta - \frac{\epsilon^3}{3^3 y^3}.$$

(We note that $y \neq 0$ since $\epsilon \neq 0$.) The solution is

$$y^3 = \eta \pm \sqrt{\eta^2 - \left(\frac{\epsilon}{3}\right)^3}.$$

Note that this quadratic equation in y^3 appears to give six solutions: one "positive" and one "negative" for each cube root of y^3, where "positive" and "negative" denote a choice of sign in the quadratic formula. As we know, the cubic has at most three distinct roots. We must appropriately choose three from the six possibilities. Note that the possible 6 values of

[4]The cases with $\epsilon = 0$ or $\beta = 0$ are of course trivial.

y are identical to the 6 possible values of z. We must now use the side condition $yz = -\frac{\epsilon}{3}$. Thus each of the possible values of y corresponds to a unique value of z. By symmetry, the 6 possible choices for y result in only 3 possibilities for $y + z$. In practice, it is not necessary to find all the possible solutions of the quadratic or cubic equations. Once we have a single solution to the cubic, chosen arbitrarily, we can factor this out of the original equation, leaving ourselves with a well understood quadratic term.

EXAMPLE 8.1. As an example of Cardano's method we solve the cubic $x^3 - 3x + 1 = 0$. For this example, using the notation introduced above, $\epsilon = -3$ and $\eta = -\frac{1}{2}$. We are lead to solving the quadratic (in y^3) $y^6 + y^3 + 1 = 0$. The resulting 6 possible values of y are $e^{\frac{2\pi\imath}{9}}$, $e^{\frac{8\pi\imath}{9}}$, $e^{\frac{14\pi\imath}{9}}$, $e^{\frac{4\pi\imath}{9}}$, $e^{\frac{10\pi\imath}{9}}$ and $e^{\frac{16\pi\imath}{9}}$. These are also the possible 6 values of z. Since we know that $yz = 1$ (leaving us precisely 3 pairs of solutions), athe solutions $(y + z)$ to our cubic are $x = e^{\frac{2\pi\imath}{9}}\left(1 + e^{\frac{14\pi\imath}{9}}\right)$, $e^{\frac{8\pi\imath}{9}}\left(1 + e^{\frac{2\pi\imath}{9}}\right)$ and $e^{\frac{14\pi\imath}{9}}\left(1 + e^{-\frac{10\pi\imath}{9}}\right)$.

The above method solves the general cubic

$$x^3 + b_2x^2 + b_1x + b_0$$

which reduces to the form

$$x^3 + a_1x + a_0$$

after replacing x by $x - \frac{b_2}{3}$. Observe that finding the solutions involves the usual field operations (on $(\mathbb{C}, +, \cdot)$) and the extraction of square and cube roots.

9. Solving the quartic

Our aim is to solve the general quartic

$$x^4 + b_3x^3 + b_2x^2 + b_1x + b_0$$

which reduces to

$$x^4 + a_2x^2 + a_1x + a_0$$

by replacing x by $x - \frac{b_3}{4}$. We follow a method discovered by Lodovici Ferrari, who certainly was familiar with Cardano's work. To solve the reduced quartic, we factor it into a product of quadratics

$$x^4 + a_2x^2 + a_1x + a_0 = (x^2 + \alpha x + \beta)(x^2 + \gamma x + \delta). \tag{44}$$

As a consequence of the fundamental theorem of algebra, we know that such a factorization is possible. What is not obvious is that we can find an algorithm for determining the four constants α, β, γ and δ in terms of given a_2, a_1 and a_0.

Equating the coefficients of the x^3 terms in (44), we obtain $\gamma = -\alpha$, the first step in reducing the problem to more manageable size.

The next step is to equate the coefficients of the x^2 terms in the two sides of (44) to obtain

$$-\alpha^2 + \beta + \delta = a_2.$$

At this point we rely on an inspired "guess" – probably reached by Ferrari after a number of other trials:

$$\beta = \frac{1}{2}(a_2 + \alpha^2 + \eta) \text{ and } \delta = \frac{1}{2}(a_2 + \alpha^2 - \eta);$$

thus reducing the task of finding two constants β and δ to the apparently simpler task of finding one constant η. To complete the algorithm, we need to evaluate α and η.

Equating the coefficients of the x terms in the two sides of (44), we obtain

$$\frac{1}{2}\alpha(a_2+\alpha^2-\eta)-\frac{1}{2}\alpha(a_2+\alpha^2+\eta)=a_1;$$

from which we easily conclude that

$$\eta=-\frac{a_1}{\alpha};$$

provided that $\alpha\neq 0$.[5] We are left with the task of evaluating the last unknown constant α.

If we equate the constant terms in the two sides of (44), we obtain

$$a_2^2+2a_2\alpha^2+\alpha^4-\frac{a_1^2}{\alpha^2}=4a_0;$$

a cubic in α^2 that we know how to solve from the results of the previous section.

EXAMPLE 8.2. We consider the quartic $x^4+\imath x+\frac{3}{4}$. The resulting cubic in α^2 is $\alpha^6-3\alpha^2+1$. This equation was solved in the last section.

10. Concluding remarks

We proceed to some remarks about the general case of a real polynomial $p(x)$ of arbitrary degree $n\geq 3$. If n is odd, it must have at least one real root, say at $x=r$. Dividing $p(x)$ by $x-r$ we obtain a polynomial of even degree $n-1$. A polynomial of even degree may have a number of real roots and and an even number of complex roots that occur as conjugate pairs. Thus $p(x)$ has m real roots and $\frac{n-m}{2}$ pairs of non-real complex conjugate roots. Note that n and m must have the same parity. This analysis does not reveal how many families of polynomials of a given degree there are, nor what they look like. It leads to a series of questions paralleling those posed at the beginning of our discussion of the cubic.

We conclude by returning to the questions which preceded our discussion of the cubic. We have seen how the root structure of the quadratic is a special case of the root structure of arbitrary polynomials, while the standard form of a quadratic is very special. For degree 2, there is one standard form. For degree 3, there are three standard forms. What happens for polynomials of degree $n\geq 4$? For quartics an analysis similar to that used for cubics will work (how many equivalence classes will result?), not quite so for polynomials of degree five or higher. But this leads to a different fascinating chapter in the study of algebra.

11. A moduli (parameter) count

The general cubic depends on four parameters. Our equivalence relation on polynomials of degree three also depends on four parameters (two each for pre and post composition). It thus seems reasonable, as we discovered, that there are only three equivalence classes. The quartic depends on five parameters and we thus expect that there should one parameter families of equivalece classes of quartics.

EXERCISES

These exercises are more open ended than those in previous chapters – projects for the readers requiring thinking as well as readings of literature on the subject.

[5]The condition $\alpha=0$ implies that the reduced quartic is of the form $x^4+a_2x^2+a_0$ – a quadratic in x^2 and hence easily solved. Thus we may assume that $\alpha\neq 0$.

(1) Let n be a positive integer. On how many parameters does the space of equivalence classes of n-th degree polynomials depend? Does it make any difference if one considers polynomials with coefficients in the rings $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$ and the affine maps with coeffiecents in the corresponding rings.
(2) Complete the work needed to compute the 4 roots of Example 8.2.
(3) Find the roots of each of the following polynomials.
   (a) $1 + 2x + 2x^2 + x^3$
   (b) $1 + 2x + 3x^2 + 4x^3$
   (c) $1 + 2x + 2x^2 + 2x^3 + x^4$
   (d) $1 + 2x + 3x^2 + 4x^3 + 5x^4$
(4) Complete the details for the classification of complex cubics into two equivalence classes.
(5) Determine the set of standard forms for quartics over the reals and complex numbers. On how many parameters does each of the equivalence classes depend?

CHAPTER 9

Nonsolvability by radicals

The main aim of this chapter is to prove that polynomials of degree greater than 4 cannot be solved by simple formulae. We follow a path described in Chapter VI of [**8**]. To avoid some technical complications, we assume that all fields under discussion are contained in $\mathbb{C}$; they automatically contain $\mathbb{Q}$. THE MATERIAL IN THIS CHAPTER IN PRELIMINARY FORM – MANY REVISIONS ARE REQUIRED.

1. Algebraic extensions of fields

We begin with a general

DEFINITION 9.1. Let $F \subseteq \mathbb{C}$ be a field. A number $\alpha \in \mathbb{C}$ is *algebraic* over F if there exists a polynomial $P(x) \in F[x]$ of positive degree with $P(\alpha) = 0$. Thus α is a *root* of $P(x)$ and $P(x)$ *vanishes* at α. A number $\alpha \in \mathbb{C}$ is *algebraically independent* or *transcendental* over F if it is not algebraic. The definitions make perfectly good sense for integral domains $F \subset \mathbb{C}$.

REMARK 9.2. If the polynomial $P(x)$ of the last definition has degree 1, then $\alpha \in F$ if the latter is a field.. Hence, for fields, the interesting cases involve polynomials of degree at least 2. The complex numbers $\pm\sqrt{2}$, $\pm i$ are algebraic over $\mathbb{Q}$ satisfying the polynomial equations $x^2 - 2 = 0$ and $x^2 + 1 = 0$, respectively. The reason for allowing polynomials of degree one to appear in the last definition is to guarantee that all the elements of the field F are algebraic over F.

DEFINITION 9.3. Let F be a subfield of E. We view E as a F-vector space and call it an *extension* of the field F and a *finite* extension if the dimension of E as an F-vector space is finite. We say that E is *algebraic* over F if every $e \in E$ is algebraic over F.

THEOREM 9.4. *If E is a finite extension of the field F, then every element $\alpha \in E$ is algebraic over F.*

PROOF. If $\alpha \in E$ there is nothing to prove. So assume that $\alpha \notin E$. If n is bigger than or equal to the dimension of E as an F-vector space, then the $n+1$ elements $1, \alpha, ..., \alpha^n$ in E cannot be linearly independent over F. So there exists elements $a_i \in F$, not all zero, such that

$$a_0 + a_1\alpha + ... + a_n\alpha^n = 0. \tag{45}$$

The degree of the last polynomial must be at least two since otherwise α would belong to E. □

PROPOSITION 9.5. *Let $\alpha \in \mathbb{C}$ be algebraic over the field F. Let J be the ideal of polynomials in $F[x]$ which vanish at α. Let $p(x)$ be the monic polynomial that generates J. Then $p(x)$ is irreducible.*

PROOF. Suppose that $p(x) = g(x)h(x)$ is a factorization of the polynomial $p(x)$ and the degrees of $g(x)$ and $h(x)$ are strictly less than the degree of $p(x)$. Since $p(\alpha) = 0$, either $g(\alpha) = 0$ or $h(\alpha) = 0$. Since $p(x)$ is a polynomial of minimal degree in J, we have reached a contradiction. □

DEFINITION 9.6. With the notation of the last theorem, we may assume that $p(x)$ is monic. It is then uniquely determined by α and F, and we call it the *irreducible polynomial of α over F*. Its degree is the *degree of α over F*.

REMARK 9.7. Note that $\alpha \in F$ if and only if $p(x) = x - \alpha$ if and only if the degree of α over F is one.

THEOREM 9.8. (a) *Let $\alpha \in \mathbb{C}$ be algebraic over the field F. Let n be the degree of its irreducible monic polynomial $p(x)$ over F. Then the F-vector space*[1]*, $F(\alpha)$, generated by $1,\ \alpha,\ ...,\ \alpha^{n-1}$ is a field, and the dimension of $F(\alpha)$ as a F-vector space is n (also denoted by $[F(\alpha) : F]$).*
(b) *Let $\alpha \in \mathbb{C}$ be algebraicaly independendent over the field F. Then the F-vector space, E, generated by $1,\ \alpha,\ ...,\ \alpha^n,\ ...$ is infinite dimensional, an integral domain, and the map θ that is the identity on F and sends α to x extends to a ring isomorphism $\theta : E \to F[x]$.*
(c) *Under the same assumptions and notation as in the previous part, let $F(\alpha)$ be the smallest subfield of $\mathbb{C}$ containing F and α. Then $F(\alpha)$ is the field of fractions of the integral domain E and isomorphic to the field of rational functions $F(x)$.*

PROOF. (a) Let $f(x) \in F[x]$. By the division algorithm, we can find polynomials $q(x)$ and $r(x) \in F[x]$ with

$$f(x) = q(x)p(x) + r(x) \text{ and } \deg r(x) < \deg p(x).$$

Thus

$$f(\alpha) = r(\alpha).$$

Denote by E the F-vector space generated by $1, \alpha, ...\alpha^{n-1}$. (We need to show that E is a field; hence $F(\alpha)$.) Let a and $b \in E$. Then there exist polynomials $f_1(x)$ and $f_2(x) \in F[x]$ each of degree less than n with $f_1(\alpha) = a$ and $f_2(\alpha) = b$. Thus (using $f(x) = f_1(x)f_2(x)$)

$$ab = f_1(\alpha)f_2(\alpha) = r(\alpha) \in E.$$

Now suppose $f(x) = f_1(x)f_2(x)$ has degree less than n and $f(\alpha) \neq 0$. Then $p(x)$ does not divide $f(x)$. Since $p(x)$ is irreducible, we conclude that the polynomials $p(x)$ and $f(x)$ must be relatively prime and hence there exist polynomials $g(x)$ and $h(x) \in F[x]$ such that $g(x)f(x) + h(x)p(x) = 1$. Hence $g(\alpha)f(\alpha) = 1$. Showing that every non-zero element of E is invertible. This suffices to establish that the ring E is a field.
(b) It is clear that E is a ring. It is an infinite dimensional F-vector space since for every positive integer n, the vectors $1,\ \alpha,\ ...,\ \alpha^n$ are lineraly independent over F since a relation of the form (45) would imply that α is algebraic over F. The ring E is an integral domain since in is contained in $\mathbb{C}$. The F-linear map θ is extended to the vector space E by defining $\theta(\alpha^n) = x^n$. It is clearly a ring isomorphism.
(c) It is clear that the field of fractions of E is equal to $F(\alpha)$. The map $\theta : F(\alpha) \to F(x)$ is defined as the identity on F and by sending α to the indeterminate x. It is rather obvious how to extend it to all of $F(\alpha)$ to obtain a ring homomorphism to the space of rational

[1]The notation implies that we vector space we obtain is a field, as we establish below.

functions $F(x)$ over F. To show that θ is an isomorphism between fields, all we need to show that it is surjective. So let $p(x)$ and $q(x) \in F[x]$ with $q(x) \neq 0$. Hence $\frac{p(x)}{q(x)}$ is an arbitrary element of $F(x)$. Certainly both $p(\alpha)$ and $q(\alpha) \in F(\alpha)$. We claim that $q(\alpha) \neq 0$ since otherwise α would (once again) be algebraic over F. It is clear $\theta\left(\frac{p(\alpha)}{q(\alpha)}\right) = \frac{p(x)}{q(x)}$. □

DEFINITION 9.9. In general, if E is a finite dimensional extension of F, we denote by $[E : F]$ the dimension of E as an F-vector space.

THEOREM 9.10. *If E_1 is a finite extension of the field F and E_2 is a finite extension of E_1, then E_2 is a finite extension of F and*

$$[E_2 : F] = [E_2 : E_1][E_1 : F].$$

DEFINITION 9.11. Let α_1 and $\alpha_2 \in \mathbb{C}$ be algebraic over a field F, then α_2 is obviously algebraic over $F(\alpha_1)$ and we can form the field $F(\alpha_1)(\alpha_2)$. Since any field that contains F, α_1 and α_2 will contain $F(\alpha_1)(\alpha_2) = F(\alpha_2)(\alpha_1)$, this is the smallest field that contains F, α_1 and α_2; we will denote it by $F(\alpha_1, \alpha_2)$. This field is algebraic over F. In particular, sums and products of algebraic numbers are algebraic. For if α_1 and α_2 are algebraic over the field F, then both $\alpha_1 + \alpha_2$ and $\alpha_1\alpha_2 \in F(\alpha_1, \alpha_2)$. By induction, if $\alpha_1,\ \alpha_2,\ ...,\ \alpha_r$ are algebraic over F, we obtain the field

$$F(\alpha_1,\ \alpha_2,\ ...,\ \alpha_r),$$

by *adjoining* $\alpha_1,\ \alpha_2,\ ...,\ \alpha_r$ to F.

REMARK 9.12. In the notation of the last definition, we have the equality

$$[F(\alpha_1,\ \alpha_2,\ ...,\ \alpha_r) : F] = [F(\alpha_1,\ \alpha_2,\ ...,\ \alpha_r) : F(\alpha_1,\ \alpha_2,\ ...,\ \alpha_{r-1}]\ [F(\alpha_1,\ \alpha_2,\ ...,\ \alpha_{r-1}) : F(\alpha_1,\ \alpha_2,\ ...,\ \alpha_{r-2}]$$

Hence Theorem 9.21 will tell us that $F(\alpha_1,\ \alpha_2,\ ...,\ \alpha_r) = F(\gamma)$ for some $\gamma \in \mathbb{C}$ that is algebraic over F.

Let F be a field. The discussion of transcendental numbers over F is similar, but not completely parallel to the discussion of algebraic numbers over F.

DEFINITION 9.13. Let F be a subfield of $\mathbb{C}$ and $\alpha_1,\ \alpha_2,\ ...,\ \alpha_r \in \mathbb{C}$. Let $F_0 = F$ and define inductively $F_i = F_{i-1}(\alpha_i)$ for $i = 1,\ 2,\ ...,\ r$. We will say that the r complex numbers $\alpha_1,\ \alpha_2,\ ...,\ \alpha_r$ are *algebraically independent* over F if for $i = 1,\ 2,\ ...,\ r$, α_i is algebraically independent over F_{i-1}.

PROPOSITION 9.14. *Under the notation of the last definition, F_r is independent of the ordering of the $\alpha_1,\ \alpha_2,\ ...,\ \alpha_r$ and is hence denoted by $F(\alpha_1,\ \alpha_2,\ ...,\ \alpha_r)$.*

2. Field embeddings

DEFINITION 9.15. Let F and E be fields. A ring homomorphism $\sigma : F \to E$ is automatically injective and we will hence refer to it also as an *embedding* of F in E. Since $\sigma(F)$ is a subfield of E, the map $\sigma : F \to \sigma(F)$ is an isomorphism and hence invertible. If

$$p(x) = a_n x^n + ... + a_0 \in F[x],$$

then we define the polynomial

$$\sigma p(x) = \sigma(a_n)x^n + ... + \sigma(a_0) \in E[x].$$

PROPOSITION 9.16. *Let F and E be fields and $\sigma : F \to E$ an embedding. The induced map $\sigma : F[x] \to \sigma(F)[x]$ is an $\mathbb{Q}$-algebra isomorphim. Further, if $p(x) \in F[x]$ is irreducible over F, then $\sigma p(x) \in \sigma(F)[x]$ is irreducible over $\sigma(F)$.*

Let F and L be fields and $f(x) \in F[x]$. Let $\alpha \in \mathbb{C}$, be algebraic over F. If $\sigma : F(\alpha) \to L$ is an embedding, then

$$(\sigma f)(\sigma(\alpha)) = \sigma(f(\alpha)).$$

In particular, the embedding σ of $F(\alpha)$ into L is determined by the restriction of σ to $F \cup \{\alpha\}$.

DEFINITION 9.17. Let $\sigma : F \to L$ and $\tau : E \to L$ be field embeddings and let E be an extension of F. We say that τ is an *extension* of σ to E or that σ is a *restriction* of τ to F if $\tau(f) = \sigma(f)$ for all $f \in F$.

THEOREM 9.18. *Let $\sigma : F \to L$ be a field embedding. Let $p(x) \in F[x]$ be irreducile. Let $\alpha \in \mathbb{C} - F$ be a root of $p(x)$ and let β be a root of $(\sigma p)(x)$ in L. Then there exists an embedding $\tau : F(\alpha) \to L$ which is an extension of σ and satisfies $\tau(\alpha) = \beta$. Conversely, for every extension τ of σ to $F(\alpha)$, $\tau(\alpha)$ is a root of $(\sigma p)(x)$.*

COROLLARY 9.19. *Let $p(x)$ be an irreducible polynomial over the field F and $\alpha \in \mathbb{C}$ a root of $p(x)$. Let $\sigma : F \to \mathbb{C}$ be an embedding. Then the number of possible embeddings of $F(\alpha)$ into $\mathbb{C}$ that extend σ equals the degree of the polynomial $p(x)$ (which is the same as the degree of the complex number α over the field F).*

COROLLARY 9.20. *Let E be a finite extension of the field F of degree n. Let $\sigma : F \to \mathbb{C}$ be an embedding. Then the number of extensions of σ to an embedding of $E \to \mathbb{C}$ equals n.*

THEOREM 9.21. *If E is a finite field extension of F, then there exists an element $\gamma \in E$ such that $E = F(\gamma)$.*

3. Splitting fields

DEFINITION 9.22. Let E be a finite extension of the field F. Let σ be an embedding of F (into some field) and τ an extension of σ to an embedding of E. If σ is the identity map, then it is convenient to say that τ is an embedding of E *over* F and that τ leaves F *fixed*.

PROPOSITION 9.23. *Let σ be an embedding over F of a finite extension K of a field F. If $\sigma(K) \subseteq K$, then $\sigma(K) = K$ and is an automorphism of the field K.*

PROPOSITION 9.24. (a) *The set G of all automorphisms of a field K is a group under composition.*
(b) *If G is a group of automorphisms of a field K, then*

$$K^G = \{a \in K; \sigma(a) = a \text{ for all } g \in G\}$$

is a subfield of K.

DEFINITION 9.25. A finite extension K of a field F is *Galois* if every embedding of K over F is an automorphism of K; it is a *splitting field* of the polynomial $p(x) \in F[x]$ if $K = F(\alpha_1, \ ..., \ \alpha_n)$, where $\alpha_1, \ ..., \ \alpha_n$ are (all) the roots of $p(x)$.

THEOREM 9.26. *A finite extension of a field F is Galois if and only if it is the splitting field of a polynomial $p(x) \in F[x]$.*

THEOREM 9.27. *Let K be a Galois extension of a field F. If $p(x) \in F[x]$ is irreducible (over F) and has one root in K, then all its roots are in K.*

4. Galois extensions

THEOREM 9.28. *Let K be a Galois extension of a field F. If G is the group of automorphisms of K over F, then F is the fixed field of G.*

THEOREM 9.29. *Let K be a Galois extension of a field F. To each intermediate field E (between F snd K) associate the subgroup $G_{K/E}$ of the automorphism group of K consisting of those automorphisms that leave E fixed. Then K is Galois over E and the map*

$$E \mapsto G_{K/E}$$

is a bijection between the set of intermeddiate fields onto the set of subgroups of G. Further E is the fixed field of $G_{K/E}$.

DEFINITION 9.30. If K is a Galois extension of the field F, we call the group of automorphisms $G_{K/F}$ the *Galois group* of K over F. If K is the splitting field of the polynomial $P(x) \in F[x]$, then we also say that $G_{K/F}$ the *Galois group* of $P(x)$.

PROPOSITION 9.31. *Let F be a field, $\alpha_1,\ \alpha_2,\ ...,\ \alpha_n \in \mathbb{C}$ and*

$$p(x) = (x-\alpha_1)(x-\alpha_2)...(x-\alpha_n).$$

Let $K = F(\alpha_1,\ \alpha_2,\ ...,\ \alpha_n)$ and $\sigma \in G_{K/F}$. Then $\{\sigma(\alpha_1),\ \sigma(\alpha_2),\ ...,\ \sigma(\alpha_n)\}$ is a permutation $\pi_\sigma \in S(n)$ of $\{\alpha_1,\ \alpha_2,\ ...,\ \alpha_n\}$. The map that sends $\sigma \in G_{K/F}$ to $\pi_\sigma \in S(n)$ is an injective group homomorphism.

5. Quadratic, cubic and quartic extensions

5.1. Linear extensions. The only irreducible monic polynomial of degree 1 over a field F is of the form $x + b$ with $b \in F$. Hence the only extension E of F with $[E : F] = 1$ is $E = F$.

5.2. Quadratic extensions. Let F be a field. An irreducible polynomial $p(x) = x^2 + bx + c,\ b$ and $c \in F$ over F has a splitting field $F(\alpha)$, where

$$\alpha = \frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$

We conclude that $F(\alpha)$ is Galois over F and $G_{F(\alpha)/F}$ is cyclic of order 2. If we let $d = b^2 - 4c$ (this is the *discriminant* of the quadratic polynomial $p(x)$), then we see that $F(\alpha) = F(\sqrt{d})$. Conversely, the polynomial $x^2 - d$ is irreducible over F if and only d is not a square in F[2].

5.3. Cubic extensions. We start with a field F and a cubic plynomial $p(x) \in F[x]$. We have already seen several times that after completing a square, a monic cubic can be reduced to the form

$$p(x) = x^3 + bx + c = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3),$$

where b and $c \in F$, but the complex roots α_i may or may not be elements of the field F. If $p(x)$ has no root in F, then it is irreducible over F, (which we assume for the rest of this subsection) and simple calculations show that

$$-(\alpha_1+\alpha_2+\alpha_3) = 0,\ \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = b,\ -\alpha_1\alpha_2\alpha_3 = c.$$

[2]Whenever d is a square in F, $F(\sqrt{d}) = F$, of course.

It is convenient to define

$$\delta = (\alpha_2 - \alpha_1)(\alpha_3 - \alpha_1)(\alpha_3 - \alpha_2) \text{ and } D = \delta^2,$$

and call D the *discriminant* of the polynomial $p(x)$.

Let $K = F(\alpha_1, \alpha_2, \alpha_3)$ be the splitting field of $p(x)$ and G its Galois group over F. The group G is isomorphic to a subgroup of the symmetric group $S(3)$. Since K contains a root (say α_1) of $p(x)$, it follows that the order of $G = [K : E]$ is either 3 or 6 – it cannot be 2. In the first case G is cyclic of order 3 and $K = F(\alpha_1)$. In the second case G is isomorphic to $S(3)$.

THEOREM 9.32. *We have two mutually exclusive possibilities:*
(a) *If D is a square in F, then K has degree 3 over F, or*
(b) *If D is not a square in F, then the group G is isomorphic to $S(3)$.*

THEOREM 9.33. $K = F(\sqrt{D}, \alpha_1)$.

EXAMPLE 9.34. Consider the polynomial $p(x) = x^3 - 3x + 1$. It has no roots over $\mathbb{Z}_2$; hence no roots in $\mathbb{Z}$. Thus irreducible over $\mathbb{Q}$. Its discriminant is 3^4, a square in $\mathbb{Q}$. The Galois group of $p(x)$ is thus cyclic of order 3 and its splitting field is $\mathbb{Q}(\alpha)$, where α is a root of $p(x)$; for example, $e^{\frac{2\pi\imath}{9}}\left(1 + e^{\frac{14\pi\imath}{9}}\right)$ (see Example 8.1).

5.4. Quartic extensions.

6. Nonsolvability

DEFINITION 9.35. A Galois field extension whose Galois group is abelian is called an *abelian* extension.

Let $K = F(\alpha)$ is a Galois extension of the field F where $\alpha \in \mathbb{C} - F$. If σ and τ are automorphisms of K over F, then $\sigma\tau = \tau\sigma$ if and only if $(\sigma\tau)(\alpha) = (\tau\sigma)(\alpha)$.

We begin the build-up to our main (nonsolvability) theorem.

THEOREM 9.36. *Let n be a positive integer and ω be an n-th root of unity. Let F be a field that does not contain ω. Then $K = F(\omega)$ is an abelian extension of F.*

THEOREM 9.37. *Let n be a positive integer and F a field that contains the n-th roots of unity. Let $\alpha \in \mathbb{C} - F$ with $\alpha^n \in F$. Then $K = F(\alpha)$ is an abelian extension of F.*

DEFINITION 9.38. Let F be a field and $f(x) \in F[x]$ be a polynomial of degree ≥ 1. We say that F or $f(x)$ is *solvable by radicals* if the splitting field of F is contained in a Galois extension K which has a sequence of subfields $\{F_i\}$ such that

$$F = F_0 \subset F_1 \ \subset ... \ F_r = K$$

with
(a) $F_1 = F(\omega)$ for some primitive n-th root of unity ω, and
(b) For $0 < i < r$, $F_{i+1} = F_i(\alpha_i)$ with $\alpha_i \notin F_i$, $\alpha^d \in F_i$ and $d|n$.

REMARK 9.39.
- Because the field inclusions in the above definition are proper, we have to consider the possibility that F already contains an appropriate n-th root of unity. In this case condition (a) in the above definition is dropped and the indeces i in condition (b) run from 0 (to $r - 1$).

- Degree 1 polynomials are, of course, solvable. For such polynomials ($f(x) = ax + b, a \in F^*, b \in F$), $r = 0$.

We use the notation and cocepts of our last definition. Since $d|n$, $\omega^{\frac{n}{d}}$ is a primitive d-th root of unity. Hence F_{i+1} is an abelian extension of F_i. Thus the Galois group G of K over F decomposes into a sequence of abelian extensions and if we let H_i be the Galois group of K over F_i, we get a sequence of groups that satisfy 16 and that G is a solvable group. We have thus established

THEOREM 9.40. *If $f(x)$ is solvable by radicals, then its Galois group is solvable.*

We can now state the main theorem of this chapter:

THEOREM 9.41. *Let $\alpha_1, \alpha_2, \ ..., \alpha_n$ be algebraically independent over a field F_0, and let*

$$f(x) = \prod_{i=1}^{n}(x - \alpha_i) = x^n + a_{n-1}x^{n-1} + ... \ a_0 \in \mathbb{C}[x].$$

Let $F = F_0(a_{n-1}, ..., \ a_0)$ and $K = F(\alpha_n, ..., \ \alpha_1)$. Then K is a Galois extension of F with Galois group $S(n)$.

We need to know we can find a set of complex numbers $\alpha_1, \alpha_2, \ ..., \alpha_n$ that are algebraically independent over a field $F_0 \subset \mathbb{C}$; for example, over $\mathbb{Q}$. This will follow from the fact that $\mathbb{Q}$ is countable, while $\mathbb{C}$ is not.

DEFINITION 9.42. Let F be a field. We define the *algebraic closure* $\bar{F}$ of F to be the set of complex numbers that are algebraic over F.

PROPOSITION 9.43. *If F is a countable field, so are $\bar{F}$ and $F(x)$.*

COROLLARY 9.44. *For every positive integer n, there exists n algebraically independent complex numbers over $\mathbb{Q}$.*

EXERCISES

(1) In our discussion of quadratic extensions, we assumed that the polynomial $p(x) = x^2 + bx + c$ was irreducible over the field F. What happens when the polynomial is reducible?
(2) Formulate and solve problems similar to the last question for cubic and quartic extensions.

Bibliography

[1] L.V. Ahlfors, *Complex Analysis (third edition)*, McGraw-Hill, 1979.

[2] H. Anton and Ch. Rorres, *Elementary Linear Algebra (Applications Version), 8th edition*, John Wiley and Sons, 2000.

[3] R. Corless, *Essential Maple 7*, Springer, 2002.

[4] H. Derksen, *The fundamental theorem of algebra and linear algebra*, Amer. Math. Monthly **110** (2003), 620–623.

[5] A. F. Coxford et al, *Contemporary Mathematics in Context, A unified approach; Course 2, Part A*, Everyday Learning, 1997.

[6] J. P. Gilman, I. Kra, and R. Rodriguez, *Complex Analysis, In the Spirit of Lipman Bers*, Graduate Texts in Mathematics, vol. 245, Springer-Verlag, 2007.

[7] J.F. Humphreys and M.Y. Prest, *Numbers, Groups and Codes*, Cambridge University Press, 1989.

[8] S. Lang, *Algebraic Structures*, Addison-Wesley, 1967.

[9] M. Spivack, *Calculus*, Publish or Persish, Inc.

[10] R.S. Wolf, *Proof, Logic, and Conjecture: The Mathematician's Toolbox*, W.H. Freeman and Company, 1998.

Index