MAT 312/AMS 351 SPRING 2014
FINAL REVIEW FOR LECTURE 1 (KIRILLOV)

General

The final will be in class on **Fri, May 16, 11:15 AM to 1:45 PM, rm P131**.

Final will be cumulative. It will consist of 8-10 problems. It will be "open book": you are allowed to bring the textbook, notes on binary codes plus one sheet (letter sized, 2-sided) of personal notes. No computers or calculators may be used. Students using ebook edition or online text MUST contact the professor to arrange an alternative.

Below you will find an overview of the material covered.

Chapter 1

§1.1 Understand the statement of the division algorithm, especially how to show the uniqueness of the quotient and the remainder. Understand the definition of the *greatest common divisor* d of two positive integers a and b, and the notation $d = (a, b)$. Be able to apply the Euclidean Algorithm to two integers a and b, yielding their g.c.d. d. Be able to use that calculation to express d as an integral linear combination of a and b: $d = s \cdot a + t \cdot b$. Examples, pp. 10, 11. Understand the special case: if $(a, b) = 1$, then there exist integers j and k such that $1 = s \cdot a + t \cdot b$. Understand the proof of Theorem 1.1.6, p. 13: it uses that special case. Review assigned exercises on p. 15.

§1.2. Understand how to use induction to prove that a statement $P(n)$ holds for every integer n. Example (p. 17): $P(n)$ is the statement $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$. Problem 2 p.14. Example (see Theorem 1.2.1): The binomial coefficients $\left(\begin{array}{c} n \\ k \end{array} \right)$ are defined for $0 \leq k \leq n$ by $\left(\begin{array}{c} n \\ 0 \end{array} \right) = \left(\begin{array}{c} n \\ n \end{array} \right) = 1$ and $\left(\begin{array}{c} n+1 \\ k+1 \end{array} \right) = \left(\begin{array}{c} n \\ k \end{array} \right) + \left(\begin{array}{c} n \\ k+1 \end{array} \right)$; and $P(n)$ is the statement that $\left(\begin{array}{c} n \\ k \end{array} \right) = \frac{n!}{k!(n-k)!}$ for every $0 \leq k \leq n$.

§1.3 Be able to reproduce the definition of *prime number*. Understand the "Fundamental Theorem of Arithmetic" and be able to factorize any integer ≤ 1000 (note that it must be prime, or have a prime factor ≤ 31). Understand Lemma 1.3.2 (p. 27; it uses Theorem 1.3.1): if p is prime and divides the product $a_1 a_2 \cdots a_r$ then p must divide at least one of the factors. Know how to prove that there are infinitely many primes. Given prime factorizations for a and b, be able to immediately write down the factorization of their g.c.d, and be able to calculate their least common multiple from the rule $(\gcd(a, b))(\mathrm{lcm}(a, b)) = ab$. (Corollary 1.3.5 p. 27). Material covered

§1.4 Understand the relation of congruence mod n (p. 36); and that the congruence classes mod n form a system of numbers closed under addition and multiplication. This is modular arithmetic. Be comfortable with calculations in modular arithmetic (Theorem 1.4.1); know how to represent each congruence class modulo n by a number in the range $0, \ldots, n-1$. Be able to construct addition tables and multiplication tables modulo n. Understand what it means for a class $[a]_n$ to be *invertible*: there exists a class $[b]_n$ such that $[a]_n[b]_n = [1]_n$; equivalently, $ab \equiv_n 1$. Know how to prove that if n is prime, every *nonzero* class mod n is invertible. And more generally know how to show that $[a]_n$ is invertible if and only if $(a, n) = 1$. Know the definition of $\mathbb{Z}_n^* = G_n$, the set of invertible classes mod n. Be able to prove that for $n \geq 2$, the product of any two elements of G_n is also in G_n (Theorem 1.4.7, p. 47) Review homework.

§1.5 Understand that the congruence equation

$$ax \equiv b \bmod n$$

only has solutions if $d = (a, n)$ divides b; in case $d|b$, understand why there are d distinct solutions, and be able to calculate them in examples. (Theorem 1.5.1, p. 50). Understand how to apply the "Chinese Remainder Theorem" (1.5.2, p. 54) to solve simultaneous congruences mod relatively prime moduli m and n. Note that the solution is unique mod mn. This allows extension to a third congruence ℓ as long as $(\ell, m) = (\ell, n) = 1$ (Example, page 56, bottom).

§1.6 Understand the definition of the Euler ϕ-function: $\phi(n)$ is the number of integers between 1 and n which are relatively prime to n. (Note that 1 counts!). Understand why if p is prime, then $\phi(p) = p - 1$. Be able to use the identities $\phi(p^n) = p^n - p^{n-1}$ (p prime) and $\phi(ab) = \phi(a)\phi(b)$ (a, b relatively prime), along with factorization into primes, to calculate $\phi(n)$ for any integer n.

Understand the concept of the *multiplicative order* of a mod n.

Know how to prove Fermat's Theorem (1.6.3): if p is prime, and a is not divisible by p, then $a^{p-1} \equiv 1 \bmod p$ and Euler's Theorem:

$$\text{if } (a, n) = 1 \text{ then } a^{\phi(n)} \equiv 1 \bmod n.$$

Use this and 1.6.2 to deduce Corollary 1.6.4: with p and a as above, the multiplicative order of a mod p must divide $p - 1$. Be able to find remainders of large powers of a number mod n (e.g., $5^{2014} \bmod 7$).

Chapter 4

§4.1 Remember that in the product permutation $\pi\sigma$ the σ permutation is performed first. Know simple examples, say with $n = 3$, where $\pi\sigma \neq \sigma\pi$. Be able to read off the inverse of a permutation from its "two-row" representation, p.152 (Exercise 2 p.158). Know the definition of a cycle (p.152) and be able to represent any permutation (given, for example, in "two-row" notation) as a product of disjoint cycles. Be comfortable multiplying cycles (p.156). Exercise 4 p.158.

§4.2 Understand that powers of a single permutation multiply following the law of exponents (Theorem 4.2.1), and that $(\pi\sigma)^r = \pi^r\sigma^r$ if $\pi\sigma = \sigma\pi$ and not, in general, otherwise. Understand why every permutation π of the n objects $1, 2, \ldots, n$, i.e. $\pi \in S(n)$, has some power equal to the identity (Theorem 4.2.2), and the definition of the *order* of a permutation, p.161. Understand that if π is a cycle of length k, then the order $o(\pi)$ of π is exactly k (Theorem 4.2.4). Understand why, if π is

the product of *disjoint* cycles $\pi = \tau_1 \cdot \cdots \cdot \tau_p$, then $o(\pi) = \text{l.c.m.}(o(\tau_1), \ldots, o(\tau_p))$. Exercises 6, 7, 10 p.168.

Understand that the *sign* $\text{sgn}\pi$ of a permutation $\pi \in S(n)$ can be defined as $+1$ or -1 so that if $\sigma, \pi \in S(n)$ then $\text{sgn}(\sigma\pi) = \text{sgn}\sigma \cdot \text{sgn}\pi$ and the sign of any transposition is -1. Understand how every cycle of length k can be written as a product of $k-1$ transpositions (Theorem 4.2.10), and consequently has sign $(-1)^{k-1}$. Understand how this calculation can be extended to any permutation (Theorem 4.2.11).

§4.3 Understand that the set $S(n)$ with the operation $(\sigma, \pi) \to \sigma\pi$ satisfies conditions (G1), ..., (G4) (p.170) and is therefore a *group*. [(G1) is often incorporated into the definition of the operation as a function from $G \times G$ to G.] Be comfortable with the notation e or 1 for the unit element when the group is described multiplicatively, and 0 when the group is described additively (only done if the group is commutative). Know how to prove Theorem 4.3.1 (uniqueness of identity and of inverses). Be familiar with Examples 2 ($\mathbf{Z}_n$, addition) and 3 (G_n, the invertible elements of $\mathbf{Z}_n$, multiplication). Understand the concept of *subgroup* and that for example the set of permutations in $S(n)$ which have even order is a subgroup (the "alternating group" $A(n)$) of $S(n)$. Understand that the set of 2×2 matrices with non-zero determinant form a group under matrix multiplication. [Here you need to check (G1); it is satisfied because the determinant $\det(AB)$ of the product of two matrices is the product $\det A \det B$ of their determinants]. Examples 2 and 3 give subgroups. Exercises 2, 3, 8.

Chapter 5

§5.1 Understand that the "arithmetic" of elements in a group is completely similar to what we are used to from multiplication of non-zero real [or rational] numbers *except* that elements don't commute, in general. This is how to understand Theorem 5.1.1 and Examples 1, 2, 3, p.203. Furthermore the definition and calculus of powers and order are exactly what we did for permutations. Subgroups are defined explicitly on p.206 (we already have some examples from permutations and from matrices; see Examples 3, 4, 5 p.208). Note part (iii) of Theorem 5.1.5 gives a 1-line characterization of a subgroup. Understand the definition of *proper* subgroup. Be able to prove Theorem 5.1.6 (intersection of 2 subgroups is a subgroup) and Theorem 5.1.7 (set of (positive and negative) powers of an element g is a subgroup; called the "cyclic" subgroup generated by g, and denoted $\langle g \rangle$. Understand Examples 1, 2, 3, 4 pp.209-210. Review homework exercises.

§5.2 Understand the definition of *left coset* aH and *right coset* Ha corresponding to a subgroup H of a group G and an element $a \in G$. Understand the Notes on pp.212-213, and the 4 Examples given pp.213-214. Be able to repeat the analysis of Example 3 for different G and H, e.g. $G = S(4), H = \langle (1234) \rangle$, etc. Be able to prove Theorem 5.2.1 (different cosets do not overlap). Understand why left multiplication by ba^{-1} defines a one-one correspondence $aH \to bH$ (and right multiplication by $a^{-1}b$ defines a one-one correspondence $Ha \to Hb$), and so in particular (Theorem 5.2.2): If the order of G is finite, any two cosets of a subgroup H have the same number of elements. And how this in turn implies Theorem 5.2.3 (Lagrange's Theorem): the order of H must divide the order of G. (The quotient is called the

index of H and written $[G : H]$). Understand this special case: the order of the element $g \in G$ is the order of the subgroup $\langle g \rangle$ and therefore must divide the order of G. Exercises 1, 2, 5 pp.218-219.

§5.3 Besides the definitions in the book, understand that for groups $G_1, *$ and $G_2, \circ$ a function $\theta : G_1 \to G_2$ is a *homomorphism* if it respects the group operations: $\theta(g * g') = \theta(g) \circ \theta(g')$. A homomorphism which is a bijection (one-one and onto) is an *isomorphism*. Example 3 p.221 is a homomorphism but not an isomorphism. Be able to prove Theorem 5.3.1 for homomorphisms as well as for isomorphisms. Be able to explain why G_5 and G_8 are not isomorphic, even though they are both abelian (commutative) with four elements. Understand the definition of the *direct product* $G \times H$ of groups G and H. Be able to construct an isomorphism $G_8 \to C_2 \times C_2$ (we use C_n for the cyclic group of order n, written multiplicatively). Be able to prove that if $(m, n) = 1$ then $C_m \times C_n$ is cyclic; or, in additive notation, $\mathbf{Z}_m \times \mathbf{Z}_n$ is cyclic. Be able to prove that every group of prime order is cyclic. Understand the argument p.226 that if G is a group of of order 6 with no element of order 6 then it must have an element of order 3.

§5.4, notes on binary codes. Understand how error detection with simple check digits such as ISBN or UPC code works. Understand the notion of distance between words in a binary code and relation between minimal distance and the number of errors detected and corrected (Theorems 5.4.1, 5.4.2).

Understand how a linear code is defined by a generator matrix G or by parity-check matrix H (note: you are not required to know how one constructs matrices G and H, or how one matrix is computed from the other). Finding the minimal distance between codewords in a linear code, defined in either way.

Chapter 6

§6.1, 6.2 Understand the similarity between the divisibility of polynomials $s(x), t(x), \ldots$ with coefficients in a field (the real numbers, $\mathbf{Z}_2$, etc.) and the divisibility of integers. Be able to carry out the division algorithm ("long division") for polynomials, giving a quotient and a remainder. Be able to carry out the Euclidean Algorithm to calculate a greatest common divisor $d(x)$ of $s(x), t(x)$ and to write $d(x)$ as a polynomial linear combination of $s(x)$ and $t(x)$. Know Corollary 6.2.3: a polynomial $p(x)$ has a linear factor $(x - \alpha)$ if and only if $p(\alpha) = 0$. This is very useful in finite fields, since there are only finitely many possible α.

Not in the book: know how to find rational roots of polynomials with integer coefficients.

§6.3 Understand the definition of *irreducible* polynomial (p.273); the distinction between irreducible and *prime* is not important in this context. Understand the proof of Theorem 6.3.4 (every polynomial can be written as a product of irreducibles) and the difference from Theorem 1.3.3 (unique factorization for integers): an irreducible factor is only determined *up to a nonzero multiplicative constant.* Understand Examples 1 and 2 on p.277 completely. Know Fundamental Theorem of Algebra: Every non-constant polynomial with complex coefficients has a root, and Corollaries 6.3.5, 6.3.6.

§6.4 Understand that polynomial congruence classes are defined, and have many properties like, congruence classes of integers *mod* m. Understand multiplication and addition in the set $\mathbf{R}[x]/f$ of congruence classes modulo f.

Know the definition of a field and know that the set of polynomial congruence classes mod f is a field if and only if f is irreducible (one direction is Proposition 6.4.3 in the book; the other is not in the textbook). Be familiar with the examples worked out in class:

- $\mathbf{R}[X]/x^2+1 \simeq \mathbf{C}$
- $\mathbf{Z_2}[X]/x^2+x+1$

Be able to calculate products and inverses of equivalence classes in these and similar cases.