Linear Algebra MAT 310 / Advanced Linear Algebra MAT 315

Oleg Viro

02/04/2021, Lecture 2

Definition of field

Definition. A **field** is a set F
which contains at least two distinct elements called 0 and 1
and is equipped with operations of **addition** and **multiplication** such that:
addition is **associative** and **commutative**:

$$a + (b + c) = (a + b) + c \quad \text{and} \quad a + b = b + a \quad \text{for } \forall\, a, b, c \in F,$$

multiplication is **associative** and **commutative**:

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \text{and} \quad a \cdot b = b \cdot a \quad \text{for } \forall a, b, c \in F,$$

multiplication is **distributive** over addition: $a(b + c) = ab + ac$ for $\forall a, b, c \in F$,
0 is an **additive identity**: $0 + a = a$ for $\forall a \in F$,
1 is a **multiplicative identity**: $1 \cdot a = a$ for $\forall a \in F$,
each element has an **additive inverse**: $\forall a \in F \ \ \exists\, b \in F \ \ a + b = 0$,
each non-zero element has a **multiplicative inverse**:
$\forall a \in F \ \ a \neq 0 \implies \exists\, b \in F \ \ a \cdot b = 1$.

These properties of addition and multiplication are called **field axioms**.

Examples. $\mathbb{Q}$, the field of rational numbers,
$\mathbb{R}$, the field of real numbers,
$\mathbb{C}$, the field of complex numbers.

We have to check if $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ satisfy all the field axioms. This an easy exercise,
because you are familiar with these properties of rational, real and complex numbers.

Uniqueness of the inverses

In any field, additive and multiplicative inverses are unique.

Indeed, if b, b' are additive inverses to a, then $b = b + (a + b') = b + a + b' = (b + a) + b' = b'$. □

Similarly, if b, b' are multiplicative inverses to a, then $b = b \cdot 1 = b(ab') = bab' = (ba)b' = 1 \cdot b' = b'$. □

Due to uniqueness, **the inverses deserve special notation.**
The additive inverse to a is denoted by $-a$;
the multiplicative inverse to a is denoted by a^{-1} or $\frac{1}{a}$.
Two extra operations are defined:
subtraction $a - b := a + (-b)$
and **division** $a/b := a \cdot (b^{-1})$ for $b \neq 0$.

Definition of field. Reformulation

Uniqueness of the additive and multiplicative inverses allows to reformulate the definition of field as a set equipped with several operations related to each other.

A set F equipped with distinguished elements $0, 1 \in F$ and operations of
addition $(a, b) \mapsto a + b$, multiplication $(a, b) \mapsto a \cdot b$,
additive inversion $a \mapsto -a$, and multiplicative inversion $a \mapsto a^{-1}$ for $a \neq 0$
is a **field** if
the addition and multiplication are associative, commutative and distributive,
for any $a \in F$ $a + 0 = a$, $a \cdot 1 = a$, $a + (-a) = 0$,
for any non-zero $a \in F$ $a \cdot a^{-1} = 1$.

Exercise. Prove that this definition is equivalent to the definition given earlier.

Let F be a field and $K \subset F$. If K is invariant under the four field operations of F, then K equipped with the restriction of these operations is a field.

Invariance of K under the field operations of F means that if
any of these operations is applied to elements of K, then the result belongs to K.
Say, if $a, b \in K$, then $a \cdot b \in K$, $a + b \in K$, $a^{-1} \in K$ and $-a \in K$.

Definition. Let $K \subset F$ be fields such that they have common 0 and 1 and the field operations of K are restrictions of the field operations of F. Then K is called a **subfield** of F and F is called an **extension** of K.

For example, $\mathbb{Q}$ is a subfield of $\mathbb{R}$ and $\mathbb{C}$, and $\mathbb{C}$ is an extension of $\mathbb{R}$.

4 / 19

Simple corollaries of field axioms

In any field, $a + c = b + c$ implies $a = b$.

Proof. $a + c = b + c$ implies $(a + c) + (-c) = (b + c) + (-c)$.
By associativity, this equality turns into $a + (c + (-c)) = b + (c + (-c))$.
Since $c + (-c) = 0$ by definition of $(-c)$, this equality turns into $a + 0 = b + 0$.
By definition of 0, this implies $a = b$. □

In any field, $0 \cdot a = 0$ for any a.

Proof. Since 0 is an additive identity, $0 + 0 = 0$.
Multiply both sides of this equality by a: $(0 + 0)a = 0a$.
By distributivity, this can be re-written as $0a + 0a = 0a$.
The right hand side does not change if we add 0 to it: $0a + 0a = 0 + 0a$.
Now apply the preceding statement. It gives $0a = 0$. □

In any field, $(-a)b = -(ab)$ for any a, b. *In particular, $(-1)b = -b$.*

Proof. Since $a + (-a) = 0$, we have $ab + (-a)b = (a + (-a))b = 0b = 0$.
By definition of additive inverse, $ab + (-a)b = 0$ means that $-(ab) = (-a)b$. □

In any field, $ab = 0$ implies either $a = 0$ or $b = 0$.

Proof. If $ab = 0$ and $b \neq 0$, then $a = a \cdot 1 = a(bb^{-1}) = (ab)b^{-1} = 0b^{-1} = 0.$ □

5 / 19

The smallest field

The fields $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are infinite. Can a field be finite?

Any field must contain 0 and 1, so it contains at least two elements.

There is a field which consists just of 0 and 1. It is denoted by $\mathbb{F}_2$.
The addition and multiplication in $\mathbb{F}_2$ are easy to recover.
In any field, $0+0=0$, $0+1=1+0=1$, $0\cdot 1=1\cdot 0=0\cdot 0=0$, $1\cdot 1=1$.

It is left to figure out only what $1+1$ is.

The additive inverse -1 of 1 cannot be 0, because $1+0=1$ and $1+(-1)=0$.
Therefore $-1=1$ and $1+1=1+(-1)=0$.

So far we have proved that the addition and multiplication in $\mathbb{F}_2$ are uniquely defined.

Exercise. Verify that, for these addition and multiplication, associativity and distributivity hold true.

What are the multiplicative inverses? This question makes sense only for non-zero elements. That is only for 1.
In any field, $1^{-1}=1$, because $1\cdot 1=1$.

Thus we recovered all the details of $\mathbb{F}_2$ from the number of its elements.

This means that **there exists only one field** that consists **of 2 elements**.

Characteristic

Let F be a field. Recall that F contains 1.
The n-fold sum $1+\cdots+1\in F$ is denoted by $n\cdot 1$, or just by n, the same symbol as was used for the number of summands.
Thus, in F, there is a sequence of elements: $1,2,3,\dots$.
Some of these elements may equal 0. For example, in $\mathbb{F}_2$, $2=1+1=0$.
If there exists $n\in\mathbb{N}$ such that $n\cdot 1=0$, then the **minimal** such n is called the **characteristic** of F.
If $n\cdot 1\neq 0$ for all $n\in\mathbb{N}$, then the characteristic of F is defined to be 0.
The characteristic of F is denoted by $\operatorname{char} F$.

Examples. $\operatorname{char}\mathbb{Q}=\operatorname{char}\mathbb{R}=\operatorname{char}\mathbb{C}=0$ and $\operatorname{char}\mathbb{F}_2=2$.

Theorem. The characteristic of a field can be either 0 or a prime number.

Proof. Let F be a field of finite characteristic n.
Assume that n is not prime and $n=r\cdot s$, where $r,s\in\mathbb{N}$, $r,s<n$.
Then $r\cdot 1\neq 0$ and hence there exists $(r\cdot 1)^{-1}\in F$.
On the other hand, $(r\cdot 1)\cdot(s\cdot 1)=n\cdot 1=0.$
By multiplying the equality $(r\cdot 1)\cdot(s\cdot 1)=0$ by $(r\cdot 1)^{-1}$, we get $s\cdot 1=0$,
which contradicts to the assumption that $n=\operatorname{char} F$ and $s<n$. □

Field homomorphisms

Let K and L be fields. A map $f : K \to L$ is called a **field homomorphism** if $f(a+b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$ for any $a, b \in K$.

Examples. The inclusion maps $\mathbb{Q} \to \mathbb{R}$, $\mathbb{R} \to \mathbb{C}$ and $\mathbb{Q} \to \mathbb{C}$ are field homomorphisms.

Theorem. For any field homomorphism $f : K \to L$,
1. $f(0) = 0$,
2. $f(-a) = -f(a)$ for any $a \in K$,
3. $f(1) = 1$ if f is not a constant map,
4. if f is not a constant map, then $f(a^{-1}) = (f(a))^{-1}$ for any $a \in K$, $a \neq 0$.

Proof. 1. $f(1) = f(1+0) = f(1) + f(0)$. Hence, $0 = f(0)$. □

2. $f(a) + f(-a) = f(a + (-a)) = f(0) = 0$. □

3. There exists $a \in K$ such that $f(a) \neq 0$. Then $f(a) = f(1 \cdot a) = f(1)f(a)$.
By multiplying the equality $f(a) = f(1)f(a)$ by $(f(a))^{-1}$ we get
$1 = f(a)(f(a))^{-1} = f(1)f(a)(f(a))^{-1} = f(1).$ □

4. $f(a) \cdot f(a^{-1}) = f(a \cdot (a^{-1})) = f(1) = 1$. □

Field isomorphisms

Theorem. If $f : K \to L$ is a field homomorphism, then $f(K)$ is a subfield of L.

Proof. We have seen that $f(0) = 0$ and $f(1) = 1$, hence $0, 1 \in f(K)$.
If $a, b \in f(K)$, then take $x, y \in K$ such that $f(x) = a$ and $f(y) = b$. Then $a + b = f(x) + f(y) = f(x+y) \in f(K)$ and $a \cdot b = f(x) \cdot f(y) = f(x \cdot y) \in f(K)$. Hence, $f(K)$ is closed under the restrictions of addition and multiplication in L. Existence of the inverses in $f(K)$ follows from
$$-f(a) = f(-a) \text{ and } (f(a))^{-1} = f(a^{-1}).$$ □

Theorem. *Any non-constant field homomorphism is injective.*

Proof. Let $f : K \to L$ be a non-constant field homomorphism. For any $a \in K$, if $a \neq 0$ then $f(a)f(a^{-1}) = f(a \cdot a^{-1}) = f(1) = 1$. Hence $f(a) \neq 0$. Let $a, b \in K$, $a \neq b$. Then $a + (-b) \neq 0$ and $f(a) + (-f(b)) = f(a) + f(-b) = f(a + (-b)) \neq 0$.
By adding $f(b)$ to both sides of inequality $f(a) + (-f(b)) \neq 0$, we get $f(a) \neq f(b)$. □

Since any field homomorphism $f : K \to L$ is injective,
K can be identified with its image $f(K) \subset L$, which is a subfield of L.
$f : K \to L$ is considered as an extension of the field K.

Corollary. A surjective field homomorphism is invertible.

Because surjective+injective=bijective=invertible. □

An invertible field homomorphism is called a **field isomorphism.** If there exists a field isomorphism $K \to L$, then fields K and L are said to be **isomorphic**.

Prime fields

A field F is called **prime** if it contains no smaller subfield $G \subsetneq F$.

Of course, $\mathbb{F}_2$ is a prime field.

Theorem. $\mathbb{Q}$ is a prime field.

Proof. Any rational number $\frac{p}{q}$ can be obtained by arithmetic operations from 0 and 1:

$\frac{p}{q} = (p \cdot 1) \cdot (q \cdot 1)^{-1}$, therefore $\frac{p}{q}$ must belong to any subfield of $\mathbb{Q}$.

Therefore any subfield of $\mathbb{Q}$ coincides with $\mathbb{Q}$. □

Lemma. Intersection of any collection of subfields of a field F is a subfield of F.

Proof. Let $\{K_\alpha\}, \alpha \in I$ be a family of subfields of F and $K = \bigcap_{\alpha \in I} K_\alpha$. In order to prove that K is a subfield of F, it suffices to prove that K is invariant under field operations. This means that if one applies any of four field operations to some elements of K, then the result will also belong to K. Elements of K belong to each K_α. Since K_α is a subfield, the result of operations belong to K_α. Therefore, the result of operations belong to $K = \bigcap_\alpha K_\alpha$. □

Theorem. Any field contains a unique prime subfield.

Proof. Take the intersection K of all subfields of our field F.
By Lemma, K is a subfield of F.
K is contained in any subfield of F. Therefore K is prime. □

Theorem. For any prime number p, there exists a field which consists of $0, 1, 2, \dots, p-1$. This field is unique.

Proof. This theorem has already been proved for $p = 2$. In order to prove it,
we have to recover the field operations on $n \cdot 1 = n$. It is left to you as an exercise. □

Finite fields

One can prove that the number of elements in a finite field is
p^n, where n is any natural number and p is any prime number.
A field consisting of $q = p^n$ elements is unique up to isomorphism
(i.e., up to a bijection which respects addition and multiplication.)
This field is denoted by $\mathbb{F}_q$. Other notations: $\mathbf{F}_q$ and $GF(q)$.
Here GF stands for *Galois field*.

The structure of $\mathbb{F}_q$ can be understood similarly to our study of $\mathbb{F}_2$.
We leave this outside our course.

Adjoining a square root

The field $\mathbb{C}$ of complex numbers can be obtained from the field $\mathbb{R}$ of real numbers by adjoining a square root of -1.
The same construction is applicable in other situations.
There are more general constructions for a field extension, but this one better suits our needs.

The initial data of our construction:
a field F and an element $\xi \in F$ such that the equation $x^2 = \xi$ has no root in F (i.e., there is no $x \in F$ such that $x^2 = \xi$).

The outcome of the construction:
a field $F[\sqrt{\xi}]$ that contains F and a solution of equation $x^2 = \xi$ and contains no field K such that $F \subset K \subset F[\sqrt{\xi}]$.
Let us assume for a while that F has an extension L in which the equation $x^2 = \xi$ has a solution.
Denote a solution by $\sqrt{\xi}$.
Observe that the intersection K of all subfields of L which contain F and $\sqrt{\xi}$ is the minimal subfield of L that contains F and $\sqrt{\xi}$.
Let us try to describe this field K more explicitly. K must contain all elements of L which can be obtained by field operations from elements of $F \cup \{\sqrt{\xi}\}$.
In particular, K must contain elements of the form $a + b\sqrt{\xi}$, where $a, b \in F$.
In fact, that's all: we will prove

Theorem. $K = \{a + b\sqrt{\xi} \mid a, b \in F\}$.

Adjoining a square root

Theorem. *The set* $\{a + b\sqrt{\xi} \mid a, b \in F\} \subset L$ *is a subfield of* L.

Proof. We have to verify that this set is closed under group operations.
Addition. $(a + b\sqrt{\xi}) + (a' + b'\sqrt{\xi}) = (a + a') + (b + b')\sqrt{\xi}$.
Multiplication.
$$\begin{aligned}(a + b\sqrt{\xi}) \cdot (a' + b'\sqrt{\xi}) &= aa' + ab'\sqrt{\xi} + b\sqrt{\xi} \cdot a' + b\sqrt{\xi} \cdot b'\sqrt{\xi} \\ &= aa' + bb'(\sqrt{\xi})^2 + (ab' + ba')\sqrt{\xi} \\ &= (aa' + bb'\xi) + (ab' + a'b)\sqrt{\xi}.\end{aligned}$$
Additive inverse. $-(a + b\sqrt{\xi}) = (-a) + (-b)\sqrt{\xi}$.
Multiplicative inverse.
$$\begin{aligned}\frac{1}{a + b\sqrt{\xi}} &= \frac{a - b\sqrt{\xi}}{(a + b\sqrt{\xi})(a - b\sqrt{\xi})} = \frac{a - b\sqrt{\xi}}{a^2 - b^2\xi} \\ &= \frac{a}{a^2 - b^2\xi} + \frac{-b}{a^2 - b^2\xi}\sqrt{\xi}\end{aligned}$$
□

Thus, each element of the minimal subfield $K \subset L$ which contains F and $\sqrt{\xi}$ can be presented as $a + b\sqrt{\xi}$ with $a, b \in F$.

Lemma. *This presentation is unique.*
Indeed, let $a + b\sqrt{\xi} = a' + b'\sqrt{\xi}$, then $a - a' = (b' - b)\sqrt{\xi}$.
If $b' - b = 0$, then $b = b'$ and $a = a'$, so the presentations coincide.
If $b \neq b'$, then $\sqrt{\xi} = \dfrac{a - a'}{b' - b} \in F$,
which contradicts to the assumption that F contains no x such that $x^2 = \xi$. □

Adjoining a square root

Recall that our arguments are based on assumption that $\xi = x^2$ in some field $L \supset F$.
Relying on this, we have come up to a very explicit description
of the smallest field $K \subset L$ which contains F and in which $\xi = x^2$.
We can reformulate this description as follows: we have found a bijection $F \times F \to K : (a, b) \mapsto a + b\sqrt{\xi}$ and formulas describing the field operations in K.
The fact that these operations satisfy the field axioms
follows from the assumption about existence of L.
If we want to get rid of this assumption, we can verify the field axioms independently.
The verification is nothing but a straightforward calculation.

For example, multiplication in K is described by formula $(a+b\sqrt{\xi})\cdot(a'+b'\sqrt{\xi}) = (aa'+bb'\xi)+(ab'+a'b)\sqrt{\xi}$.
Commutativity of this multiplication follows from commutativity of addition and multiplication in F.
In order to prove associativity, we have to prove that the following equality:
$\left((a+b\sqrt{\xi})(a'+b'\sqrt{\xi})\right)(a''+b''\sqrt{\xi}) = (a+b\sqrt{\xi})\left((a'+b'\sqrt{\xi})(a''+b''\sqrt{\xi})\right)$
$\left((aa'+bb'\xi)+(ab'+a'b)\sqrt{\xi}\right)(a''+b''\sqrt{\xi})$
$= (a+b\sqrt{\xi})\left((a'a''+b'b''\xi)+(a'b''+a''b')\sqrt{\xi}\right)$ Check that both sides are equal to
$aa'a'' + (bb'a'' + ab'b'' + ba'b'')\xi + (ab'a'' + ba'a'' + aa'b'' + bb'b''\xi)\sqrt{\xi}$.
Similarly verify all the field axioms.
Field K is denoted by $F[\sqrt{\xi}]$.

Conjugation and inversion

A map $F[\sqrt{\xi}] \to F[\sqrt{\xi}] : z \mapsto \overline{z}$ defined by formula $\overline{a+b\sqrt{\xi}} = a - b\sqrt{\xi}$
which is called **conjugation**.
The conjugation is an **involution**. This means that its square is the identity map: $\overline{\overline{z}} = z$.
The conjugation is a field isomorphism: $\overline{z+w} = \overline{z}+\overline{w}$ and $\overline{z\cdot w} = \overline{z}\cdot\overline{w}$.
The former formula is obvious, let us prove the latter.
$\overline{(a+b\sqrt{\xi})(a'+b'\sqrt{\xi})} = \overline{(a\cdot a'+\xi\cdot b\cdot b')+(a\cdot b'+b\cdot a')\sqrt{\xi}}$
$= (a\cdot a'+\xi\cdot b\cdot b')-(a\cdot b'+b\cdot a')\sqrt{\xi}$.
On the other hand,
$\overline{(a+b\sqrt{\xi})}\cdot\overline{(a'+b'\sqrt{\xi})} = (a-b\sqrt{\xi})(a'-b'\sqrt{\xi})$
$= (a\cdot a'+(-b)(-b')\xi)+(a(-b')+(-b)a')\sqrt{\xi}$
$= (a\cdot a'+b\cdot b'\xi)-(a\cdot b'+b\cdot a')\sqrt{\xi}$. □

$z\cdot\overline{z} \in F$ for $\forall z \in F[\sqrt{\xi}]$. **Proof.** $(a+b\sqrt{\xi})(a-b\sqrt{\xi}) = a^2 - b^2\xi$ □

Now we can explain the origin of a formula for multiplicative inverse $\dfrac{1}{a+b\sqrt{\xi}} = \dfrac{a}{a^2-b^2\xi} + \dfrac{-b}{a^2-b^2\xi}\sqrt{\xi}$ in $F[\sqrt{\xi}]$.
For $z = a+b\sqrt{\xi}$, we have $z\cdot\overline{z} = (a+b\sqrt{\xi})(a-b\sqrt{\xi}) = a^2-b^2\xi \in F$
The formula for multiplicative inversion comes from a more conceptional formula:
$z^{-1} = \overline{z}\cdot(z\cdot\overline{z})^{-1}$

Examples

The main our motivation for adjoining square root construction was to speak on complex numbers.
The field $\mathbb{C}$ is obtained by adjoining $\sqrt{-1}$ to $\mathbb{R}$. We will elaborate on $\mathbb{C}$ later.
However this construction gives many other interesting and useful fields.
For example, if we apply it to $F=\mathbb{Q}$ and $\xi=2$,
then it gives $\mathbb{Q}[\sqrt{2}]$, the smallest field of characteristic 0 which contains $\sqrt{2}$.
A few other examples:

$\mathbb{F}_3[\sqrt{-1}]=\mathbb{F}_9$.

More generally, $\mathbb{F}_p[\sqrt{-1}]=\mathbb{F}_{p^2}$ for any prime number $p\equiv -1 \mod 4$.

$\mathbb{Q}[\sqrt{6}]=\mathbb{Q}[\sqrt{\frac{3}{2}}]$, because $F[\sqrt{\xi}]=F[\sqrt{\eta}]$ if $\frac{\xi}{\eta}=x^2$ for some $x\in F$.

Similarly, $\mathbb{F}_7[\sqrt{-1}]=\mathbb{F}_7[\sqrt{3}]$

One cannot adjoin $\sqrt{-1}$ to $\mathbb{F}_5$, since $2^2=4=-1$ in $\mathbb{F}_5$.
2 is not a square in $\mathbb{F}_5$ and $\mathbb{F}_5[\sqrt{2}]=\mathbb{F}_{25}$.

16 / 19

Complex numbers

The field $\mathbb{C}$ is obtained by adjoining $\sqrt{-1}$ to $\mathbb{R}$.
The $\sqrt{-1}$ is denoted by i (after Leonard Euler, 1777).
$\mathbb{C}=\{a+bi \mid a,b\in\mathbb{R}\}=\mathbb{R}[i]$, $i^2=-1$.
Addition. $(a+bi)+(a'+b'i)=(a+a')+(b+b')i$.
Multiplication. $(a+bi)(a'+b'i)=(aa'-bb')+(ab'+a'b)i$.

Conjugation. A map $\mathbb{C}\to\mathbb{C}: a+bi\mapsto \overline{a+bi}=a-bi$ is a field isomorphism.

A complex number z is real $\iff$ $\overline{z}=z$.

Let $z=a+bi$, where $a,b\in\mathbb{R}$.
The **real part** of z, denoted $\operatorname{Re} z$, is defined by $\operatorname{Re} z=a$.
The **imaginary part** of z, denoted $\operatorname{Im} z$, is defined by $\operatorname{Im} z=b$.

Warning. The **imaginary** part of a complex number is **real**.

Relations: $z=\operatorname{Re} z+(\operatorname{Im} z)i$, $\overline{z}=\operatorname{Re} z-(\operatorname{Im} z)i$,

$$\operatorname{Re} z=\frac{1}{2}(z+\overline{z}), \qquad \operatorname{Im} z=\frac{1}{2i}(z-\overline{z})$$

17 / 19

Absolute value

$z \cdot \overline{z} = (a+bi)(a-bi) = a^2 + b^2 \geq 0$ for any complex number $z = a + bi$.

The **absolute value** or **modulus** of a complex number z,
denoted $|z|$, is defined by $|z| = \sqrt{z\overline{z}} = \sqrt{(\operatorname{Re} z)^2 + (\operatorname{Im} z)^2}$.

Obvious properties. $|\overline{z}| = |z|$, $|\operatorname{Re} z| \leq |z|$, $|\operatorname{Im} z| \leq |z|$ for any $z \in \mathbb{C}$. □

Multiplicativity of modulus. $|zw| = |z||w|$ for any $z, w \in \mathbb{C}$.

Proof. $|zw| = \sqrt{(zw)\overline{(zw)}} = \sqrt{z \cdot w \cdot \overline{z} \cdot \overline{w}} = \sqrt{z \cdot \overline{z} \cdot w \cdot \overline{w}} = \sqrt{z\overline{z}}\sqrt{w\overline{w}} = |z||w|$. □

Triangle inequality. $|z+w| \leq |z| + |w|$ for any $z, w \in \mathbb{C}$.

Proof. $|z+w|^2 = (z+w)(\overline{z}+\overline{w}) = z\overline{z} + z\overline{w} + w\overline{z} + w\overline{w} = |z|^2 + z\overline{w} + w\overline{z} + |w|^2$

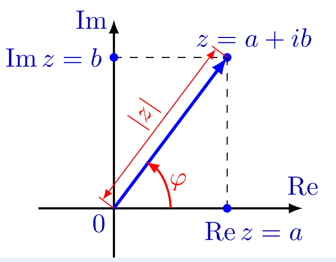
$$= |z|^2 + |w|^2 + z\overline{w} + \overline{z\overline{w}} = |z|^2 + |w|^2 + 2\operatorname{Re} z\overline{w}$$

$$\leq |z|^2 + |w|^2 + 2|z||\overline{w}| = |z|^2 + |w|^2 + 2|z||w| = (|z| + |w|)^2.$$

Thus $|z+w|^2 \leq (|z|+|w|)^2$, which implies the required $|z+w| \leq |z| + |w|$. □

Geometry of a complex number

A complex number $z = a + bi$ is characterized by an ordered pair (a, b) of real numbers, that is a point on the coordnate plane $\mathbb{R}^2$.



The same point is characterized by its **polar coordinates** $|z|$ and $\varphi = \arg z$.
The second coordinate φ is called the **argument** of z and denoted by $\arg z$.
Clearly,
$\operatorname{Re} z = |z| \cos\varphi$ and $\operatorname{Im} z = |z| \sin\varphi$.
Therefore,
$z = \operatorname{Re} z + i \operatorname{Im} z = |z|(\cos\varphi + i\sin\varphi)$.

Theorem. $\arg(z \cdot w) = \arg z + \arg w$ *for any non-zero* $z, w \in \mathbb{C}$.

Proof. Let $\arg z = \alpha$, $\arg w = \beta$ and $\arg(z \cdot w) = \gamma$. Then $z = |z| \cdot (\cos\alpha + i\sin\alpha)$, $w = |w| \cdot (\cos\beta + i\sin\beta)$ and $z \cdot w = |z \cdot w| \cdot (\cos\gamma + i\sin\gamma)$. On the other hand,

$$z \cdot w = |z| \cdot |w| \cdot (\cos\alpha + i\sin\alpha)(\cos\beta + i\sin\beta)$$
$$= |z| \cdot |w| \cdot ((\cos\alpha\cos\beta - \sin\alpha\sin\beta) + i(\cos\alpha\sin\beta + \sin\alpha\cos\beta)).$$
$$= |z| \cdot |w| \cdot (\cos(\alpha+\beta) + i\sin(\alpha+\beta)).$$

Comparing the two expressions for $z \cdot w$ and taking into account that $|z \cdot w| = |z| \cdot |w|$, we get $\cos\gamma = \cos(\alpha+\beta)$ and $\sin\gamma = \sin(\alpha+\beta)$, which implies $\gamma \equiv \alpha + \beta \mod 2\pi$. □