Fields

Recall from the last lecture

Theorem 21 If $(R, +, \times)$ is a ring with identity, then $(R^\times, \times)$ is a group.

Def A field is a commutative ring $(F, +, \times)$ satisfying the axioms:

(- $(F, +)$ is an abelian group with identity element "0")

- $(F - \{0\}, \times)$ is an abelian group with identity element "1"

because F is a commutative ring.

- $0 \neq 1$.

It might be useful to spell out the field axioms explictly as follows

A field $(F, +, \times)$

is a set with addition $+$

& multiplication $\times$

s.t.

- $(R+0) - (R+4)$

$\Rightarrow$ $(F, +)$ is an abelian group.

- $(R\times 0)\ (R\times 1)\ (R\times +)\ (R+\times)$

$\Rightarrow$ $(F, +, \times)$ is a ring

- $\forall\, a, b \in F \quad ab = ba$

$$\uparrow$$

$$a \times b$$

$\Rightarrow (F, +, \times)$ is a commutative ring

- There exists an element "1" in F s.t. $\forall\, a \in F$

$$a \cdot 1 = 1 \cdot a = a$$

$\Rightarrow (F, +, \times)$ is a commutative ring with identity

- for $^\forall a \in F - \{0\}$,

there exists an element $b \in F$

s.t. $ab = ba = 1$.

- $1 \neq 0$

Prop 19

If $1 \neq 0$, then

0 is not a unit

$$F - \{0\} = F^\times$$

$(\Rightarrow (F - \{0\}, \times)$ is an abelian group$)$

Examples

- $\mathbb{Q}$

  If $\frac{r}{s} \in \mathbb{Q} - \{0\}$,

  then $s \neq 0$, $r \neq 0$

  $\Rightarrow$ $\frac{r}{s}$ has the multiplicative inverse $\frac{s}{r}$.

- $\mathbb{R}$

  If $r \in \mathbb{R} - \{0\}$,

  $\Rightarrow$ $\frac{1}{r}$ is the multiplicative inverse of r.

- $\mathbb{Z}$ is not a field.

It is a commutative ring

but not all non-zero elements

have multiplicative inverse!

For example, 2 does NOT have

multiplicative inverse!

$\frac{1}{2}$ is NOT an integer.

Recall from earlier:

If p is a prime number,

$(\mathbb{Z}_p, +, \times)$ $\cdot$ $[a]+[b]=[a+b]$

$\cdot$ $[a][b]=[ab]$

a commutative ring,

with identity $[1]$

<u>Claim</u> $(\mathbb{Z}_p, +, \times)$ is a field.

$$\begin{array}{c} (\mathbb{Z}_p, +, \times) \\ \| \\ \mathbb{F}_p \end{array}$$

Need to check $\cdot$ $[0] \neq [1]$

$\cdot$ $(\mathbb{Z}_p - \{[0]\}, \times)$

is an abelian group.

Firstly $[0] \neq [1]$.

If they were equal, then

$[a]_p = [b]_p$

$\Leftrightarrow p \mid (a-b)$

$$[0] = [1]$$

$\Rightarrow$ p would have to divide 1.

$\Rightarrow$ This can NOT happen

since prime numbers are ≥ 2.

The hardest thing to check:

let $[a] \in \mathbb{Z}_p - \{[0]\}$.

Since $[a] \neq [0]$, p does not divide a.

$\Rightarrow \gcd(a, p) = 1.$

$\Rightarrow$ $[a]$ has multiplicatie inverse!

Theorem 12

- $\mathbb{C} :=$ the set of complex numbers.

$$= \{ \underbrace{a}_{\text{the real part}} + \underbrace{b\sqrt{-1}}_{\text{the imaginary part}} \mid a, b \in \mathbb{R} \}$$

Define "+"

$$(a+b\sqrt{-1}) + (c+d\sqrt{-1})$$

$$= (a+c) + (b+d)\sqrt{-1}.$$

§ "$\times$"

$$(a+b\sqrt{-1})(c+d\sqrt{-1})$$

$$= ac + bc\sqrt{-1} + ad\sqrt{-1} + \underbrace{bd(\sqrt{-1})^2}_{= -bd}$$

$$= (ac-bd) + (ad+bc)\sqrt{-1}.$$

Exercise / Example Sheet 1

$(\mathbb{C}, +, \times)$ is a commutative ring with identity $\underline{1} = 1 + 0\sqrt{-1}$.

Exercise Check that

$(\mathbb{C} - \{0\}, \times)$ is a group.

(G0) Given $a + b\sqrt{-1}$ $\Rightarrow (a, b) \neq (0, 0)$

$\in \mathbb{C} - \{0\}$,

$c + d\sqrt{-1}$ $\Rightarrow (c, d) \neq (0, 0)$

$$(ac - bd) + (ad + bc)\sqrt{-1} \in \mathbb{C}$$

Is this really non-zero??

Exercise: Why?

(G1)

$$(a+b\sqrt{-1})\left(\underbrace{(c+d\sqrt{-1})\cdot(e+f\sqrt{-1})}_{(ce-df)+(cf+de)\sqrt{-1}}\right)$$

$$\|$$

$$\left((a+b\sqrt{-1})(c+d\sqrt{-1})\right)(e+f\sqrt{-1})$$

$$(a(ce-df)-b(cf+de)) + (a(cf+de)+b(ce-df))\sqrt{-1}$$

(G2) $\underline{1} = 1 + 0\sqrt{-1}$

is the identity element w.r.t

$\times$.

Indeed,

$$(a+b\sqrt{-1})\cdot(1+0\sqrt{-1})$$

$$= \underline{\underline{(a\cdot 1 - b\cdot 0)}} + (a\cdot 0 + b\cdot 1)\sqrt{-1}$$

$$= a + b\sqrt{-1}.$$

Similarly

$$(1+0\sqrt{-1})(a+b\sqrt{-1}) = a+b\sqrt{-1}.$$

(G3) The inverse of $a+b\sqrt{-1}$ is

$$\frac{a}{a^2+b^2}+\frac{(-b)}{a^2+b^2}\sqrt{-1}.$$

Indeed,

$$(a+b\sqrt{-1})\left(\frac{a}{a^2+b^2}+\frac{(-b)}{a^2+b^2}\sqrt{-1}\right)$$

$$=\text{(formula)}=1$$

$$\left(\frac{a}{a^2+b^2}+\frac{(-b)}{a^2+b^2}\sqrt{-1}\right)(a+b\sqrt{-1})$$

$$=1$$

It is WRONG to compute

$$\frac{1}{a+b\sqrt{-1}} = \frac{(a-b\sqrt{-1})}{(a+b\sqrt{-1})(a-b\sqrt{-1})}$$

$$= \frac{a}{a^2+b^2} + \frac{(-b)}{a^2+b^2}\sqrt{-1}.$$

- $\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} \mid a, b \in \mathbb{Q}\}$

$$(a+b\sqrt{2}) + (c+d\sqrt{2})$$

$$= (a+c) + (b+d)\sqrt{2}$$

- $(a+b\sqrt{2})(c+d\sqrt{2})$

$$= (ac+2bd)+(ad+bc)\sqrt{2}.$$

In terms of addition & multiplication defined as above, $\mathbb{Q}(\sqrt{2})$ is a field.

- (non-examinable)

A complex number $\alpha \in \mathbb{C}$ is an algebraic number if it is a root of $f \in \mathbb{Q}[x]$

$$f = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_1 x + c_0, \quad c_n \neq 0$$

$c_i \in \mathbb{Q}$.

<u>Example</u> $\sqrt{2}$ is a root of $x^2 - 2$

$\sqrt{-1}$ — " — $x^2 + 1$

The set of <u>all</u> algebraic numbers

defines a field.

(Checking the field axioms

for those is really hard!)

§ Rings that are <u>NOT</u>

<u>fields</u>

fields $\Rightarrow$ rings $\Rightarrow$ groups.

This means that

there are rings that are

not fields!

Def A ring $(R, +, \times)$

is called a division ring

if it satisfies all the field axioms

except the commutativity w.r.t. $\times$.

Prop 24 Let $(R, +, \times)$ be

a division ring

If $ab = ac$, then $b = c$.

Pf By definition, a has inverse with respect to "$\times$"

Let a^{-1} be the inverse.

Multiplying $ab = ac$ by a^{-1} on both sides

$$a^{-1}ab = a^{-1}ac$$

$$\Rightarrow \quad 1 \cdot b = 1 \cdot c$$

$$\Rightarrow \quad b = c \qquad \square$$

Rk Recall that

if $(F, +, \times)$ is a field,

$(F^\times, \times)$ is an abelian group with $\times$.
$\parallel$
$F - \{0\}$

if $(R, +, \times)$ is a division ring
$(R^\times, \times)$ is a group
but not abelian.

Example

Let $1, p, q, r$ be symbols

satisfying the following (multiplicative) relations,

- $1 \cdot p = p \cdot 1 = p$

  $1 \cdot q = q \cdot 1 = q$

  $1 \cdot r = r \cdot 1 = r$

- $p^2 = -1$

  $q^2 = -1$

  $r^2 = -1$

- $pq = r$ $\qquad qp = -r$

$$qr = p \qquad rq = -p$$

$$rp = q \qquad pr = -q.$$

Let $\mathbb{H}$ be the set of elements of the form

$$c \cdot 1 + c(p) \cdot p + c(q) q + c(r) \cdot r$$

$$c, c(p), c(q), c(r) \in \mathbb{R}$$

with natural addition & multiplication.

$$\left(c\cdot 1 + c(p)\,p + c(q)\,q + c(r)\,r\right)$$

$$+$$

$$\left(c'\cdot 1 + c'(p)\,p + c'(q)\,q + c'(r)\,r\right)$$

$$= (c+c')\cdot 1 + \left(c(p)+c'(p)\right)p + \cdots$$

Example $\quad (2\cdot q + r)(2p + 1)$

$$= 4qp + 2q + 2rp + r$$

$-r \qquad\qquad\qquad\qquad q$

$$= (-4)\cdot r + \underbrace{2q + 2q}_{4q} + r$$

This is a division ting!

Exercise

$$a = \underline{c} + \underline{c(p)}\,p + \underline{c(q)}\,q + \underline{c(r)}\,r$$

$$b = c - c(p)\,p - c(q)\,q - c(r)\,r$$

What is ab?

The answer is

$$c^2 + c(p)^2 + c(q)^2 + c(r)^2 \in \mathbb{R}.$$

This is an analogue of

$$z = a + b\sqrt{-1}$$

complex conjugation

$$\bar{z} = a - b\sqrt{-1}$$

$$z \cdot \bar{z} = (a+b\sqrt{-1})(a-b\sqrt{-1})$$

$$= a^2 + b^2$$

Using this, the multiplicative inverse of a

is
$$\frac{b}{ab} = \frac{1}{ab}\cdot c - \frac{1}{ab}c(p)\,p - \frac{1}{ab}c(q)\,q - \frac{1}{ab}c(r)\,r.$$

This is referred to as Hamilton's quaternions!