

## Lecture 7

### Operation by conjugation

Def: Let  $H \subset G$  subgroup.

For  $g \in G$ , conjugate subgroup

$$gHg^{-1} = \{ghg^{-1} : h \in H\}$$

This is a subgroup of  $G$ .

$$\begin{array}{ccc} \text{Conjugation} & G \times \{\text{subgroups of } G\} & \rightarrow \{\text{subgroups of } G\} \\ & (g, H) & \mapsto gHg^{-1} \end{array}$$

is an action.

The stabilizer of  $H$  for the conjugation action is called the normalizer of  $H$

$$N(H) = \{g \in G : gHg^{-1} = H\}$$

Remarks: (1) By definition  $N(H) = G \Leftrightarrow H$  is a normal subgroup of  $G$ .

(2)  $N(H)$  is a subgroup of  $G$ .

$H$  is a subgroup of  $N(H)$

$$\text{Thus, } |H| \mid |N(H)| \mid |G|$$

(3) Let  $c$  be the number of different conjugate subgroups to  $H$

$$(c = |\{gHg^{-1} : g \in G\}|)$$

By the orbit stabilizer theorem

$$|G| = |N(H)| \cdot c$$

### The Sylow theorems

This describe subgroups  $H \subset G$ ,  $G$  finite group w/

$$|H| = p^m \quad , \quad p \text{ prime}$$

We know: if  $H$  subgroup of  $G$

then  $|H|$  divides  $|G|$

The converse is not true, and it is difficult to decide for which divisors of  $|G|$  exists a subgroup.

### First Sylow theorem

For  $p$  prime number

$$|G| = p^m \cdot r \quad , \quad \text{w/ } p \nmid r$$

Then there is a subgroup of  $G$  w/  $p^m$  elements.

Such a subgroup is called a Sylow  $p$ -subgroup

In the following let  $G$  finite group,  $p$  prime number. Write  $|G| = p^m \cdot r$ ,  $m \geq 1$ ,  $p \nmid r$ .

Def: A group  $H$  is a  $p$ -group if  $|H| = p^n$  for  $n \geq 0$ .

A subgroup  $H \subset G$  is called a  $p$ -Sylow subgroup if  $|H| = p^m$ .

### Theorem (First Sylow theorem)

There is a  $p$ -Sylow subgroup of  $G$ .

### Corollary (Cauchy's Th.)

If a prime number divides  $|G|$ , then there is an element  $x \in G$  of order  $p$ .

Pf: Set  $H \subset G$   $p$ -Sylow subgroup, i.e.  $|H| = p^m$ .

Let  $y \in H$  be different from 1.

$\langle y \rangle$  has  $\text{ord}(y)$  elemnt.

$\text{ord}(y) \mid |H|$ , so  $\text{ord}(y) = p^r$  for some  $1 \leq r = m$ .

Let  $x := y^{(p^{r-1})}$ ,  $x^p = y^{(p^r)} = 1$

Thus,  $\text{ord}(x) = p$ .

Some applications:

Def: Let  $H, K$  be groups. The product  $H \times K$  of  $H$  and  $K$

$$\text{is } H \times K = \{(h, k) : h \in H, k \in K\}$$

This is a group under

$$\cdot : (H \times K) \times (H \times K) \rightarrow H \times K$$

$$(h_1, k_1)(h_2, k_2) \mapsto (h_1 h_2, k_1 k_2)$$

w/ identity  $(1, 1)$  and inverses element-wise,

Theorem: Let  $G$  group.  $H, K$  subgroups of  $G$ .

Spec.

$$(1) G = HK := \{hk : h \in H, k \in K\}$$

(2)  $H, K$  normal subgroups

$$(3) H \cap K = \{1\}$$

Then,  $G \cong H \times K$ .

Pf: we have map  $\varphi : H \times K \rightarrow G$

$$(h, k) \mapsto hk$$

v.i.z.  $\varphi$  is isomorphism.

By (2)  $\varphi$  is surjective.

To show  $\varphi$  homomorphism:

Let  $h \in H, k \in K$

$$h^{-1}k^{-1}hk = h^{-1}\underbrace{(k^{-1}h)}_{\substack{\in H \\ (H \text{ normal})}}k \in H$$

Similarly,  $h^{-1}k^{-1}hk = (h^{-1}k^{-1}h)k \in K$

So  $h^{-1}k^{-1}hk \in H \cap K$  and, by (2),  $h^{-1}k^{-1}hk = 1$

Hence  $hk = kh$

Take  $h_1, h_2 \in H, k_1, k_2 \in K$

$$\varphi(h_1, k_1) \cdot \varphi(h_2, k_2) = h_1 k_1 h_2 k_2 = h_1 h_2 k_1 k_2 = \varphi(h_1 h_2, k_1 k_2)$$

i.e.  $\varphi$  is homomorphism.

To show  $\varphi$  bijective we show  $\ker \varphi = \{1\}$

Let  $(h, k) \in \ker \varphi$ ,  $hk = 1$ . Hence,  $k = h^{-1}$  and  $k \in H$ . So,  $k \in H \cap K$  and  $k = 1$ , also  $h = 1$ .

Recall: A group  $H$  is cyclic if  $H = \langle a \rangle$  for  $a \in H$ . If  $H$  is cyclic of order  $m$  we know

$$H \cong (\mathbb{Z}/m\mathbb{Z}, +)$$

Corollary: Assume,  $m|m$   $\in \mathbb{Z}_{\geq 0}$  relatively prime.

Then,  $\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

Pf:  $[m]$  has order  $m$  in  $\mathbb{Z}/nm\mathbb{Z}$

$$[m] \cdot [n] = [mn] = [1]$$

$\mathbb{Z}/nm\mathbb{Z}$  has subgroups of order  $m$  or  $n$  and their intersection is  $\{0\}$ . Also normal b/c  $\mathbb{Z}/nm\mathbb{Z}$  is commutative.

Hence, by the previous th. the proof is done.

Corollary: Let  $p$  be a prime, and  $G$  a group of order  $p^2$ .

Then,  $G \cong \mathbb{Z}/p^2\mathbb{Z}$  or  $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

Pf: We show  $G$  is commutative.

By Cauchy's theorem  $G$  contains an element of order  $p$ .

Let  $H = \langle a \rangle$

Let  $b \in G \setminus H$ ,  $H' = \langle b \rangle$ .

Either  $H' = G$  (and  $G \cong \mathbb{Z}/p^2\mathbb{Z}$ ) or  $H' \neq G$ .

$\Rightarrow H' \neq G \Rightarrow |H'| = p$

$H \cap H'$  is a subgroup of  $H$ ,  $|H \cap H'|$  divides  $p$

$H \cap H' \neq H$ , otherwise  $H' = H$ .

So  $H \cap H' = \{1\}$ .

$H, H'$  normal subgroups,  $HH' = G$ ,  $H' \cap H = \{1\}$

So it follows  $G = H \times H' \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ .

## Lecture 8

Theorem: Let  $p \geq 3$  be a prime,  $G$  a group of order  $2p$ .

Then  $G \cong \mathbb{Z}/2p\mathbb{Z}$  or  $G \cong D_p$

( $D_p$  is a group of order  $2p$ , generated by  $a, b$   
 $a^p = 1, b^2 = 1, bab = a^{-1}$ )

Pf: By Cauchy's th.,  $G$  contains an elements  $a$  of order  $p$ ,  $b$  of order 2.

Let  $H = \langle a \rangle$ ,  $[H : G] = 2$ . Hence  $H$  normal.

Therefore

$$bab = bab^{-1} = a^i \text{ for some } i.$$

$$a = b^2ab^2 = b(bab)b = ba^ib = (bab)^i = (a^i)^2 = a^{i^2}$$

$$\Rightarrow a^{i^2-1} = 1, a \text{ has order } p$$

$$\Rightarrow p | i^2 - 1 = (i+1)(i-1) \Rightarrow p | i+1 \text{ or } p | i-1$$

$$\Rightarrow p | i-1 \Rightarrow a^{i-1} = 1 \Rightarrow a^i = a$$

$$\Rightarrow bab^{-1} = a \Rightarrow ba = ab \quad a \text{ and } b \text{ commute}$$

Since  $a$  and  $b$  generates  $G$ ,  $G$  is commutative.

Also,  $\langle b \rangle$  normal,  $\langle a \rangle \cap \langle b \rangle = \{1\}$ . By previous theorem

$$G = \langle a \rangle \times \langle b \rangle \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/2p\mathbb{Z}.$$

$$\text{If } p | i+1 \Rightarrow a^{i+1} = 1 \text{ i.e. } a^i = a^{-1}$$

$$\Rightarrow bab = a^{-1}, \quad a^p = 1, \quad b^2 = 1$$

and  $|G| = 2p$  and  $G = \langle a, b \rangle$

$$\text{So } G \cong D_p.$$

## Second Sylow theorem

Let  $K$  be a subgroup of  $G$  s.t.  $p \nmid |K|$ . Let  $H$  be a  $p$ -Sylow subgroup of  $G$ .

Then there is a conjugate subgroup  $H' = gHg^{-1}$  of  $G$  s.t.  $K \cap H'$  is a  $p$ -Sylow subgroup of  $K$ .

Corollary: (1) Let  $K \subset G$  subgroup which is a  $p$ -subgroup.

Then  $K$  is contained in a  $p$ -Sylow subgroup of  $G$ .

(2) The  $p$ -Sylow subgroups of  $G$  are all conjugate of each other.

Pf: Conjugation  $H \mapsto gHg^{-1}$  is bijection. Hence the conjugate of a  $p$ -Sylow subgroup is always a  $p$ -Sylow subgroup.

(1) If  $K$  is a  $p$ -subgroup of  $G$ ; by def,  $K$  is a  $p$ -Sylow subgroup of itself.

By our theorem, if  $H$  is a  $p$ -Sylow subgroup of  $G$ , then there is a conjugate  $gHg^{-1} = H'$  s.t.  $K \cap H' = K$ , i.e.  $K \subset H'$ .

So  $H'$  is a  $p$ -Sylow subgroup containing  $K$ .

(2) Let  $H, K$  be  $p$ -Sylow subgroups. Then there exist a conjugate  $H' = gHg^{-1}$  of  $H$  containing  $K$ , by (1).

So,  $K \subset H'$  but  $|K| = |H'| = p^n$ . Thus  $K = H'$ .

### Third Sylow theorem

Suppose  $G$  is a finite group,  $|G| = p^m r$ ,  $p \neq r$ . Let  $s$  be number of  $p$ -Sylow subgroups.  
Then,  $s$  divides  $r$  and  $s \equiv 1 \pmod{p}$ .

Theorem: Let  $G$  be a group,  $|G| = pq$ ,  $p > q$ ,  $p, q$  primes. If  $q \nmid p-1$ , then  $p$  is cyclic.

Pf: Let  $N_p = \#$  of  $p$ -Sylow subgroups of  $G$ .

We have,  $N_p \equiv 1 \pmod{p}$  and  $N_p \mid q$  as  $p > q$ , we have  $N_p = 1$ .

Let  $H$  be the unique  $p$ -Sylow subgroup.

If  $g \in G$ ,  $gHg^{-1}$  is also  $p$ -Sylow subgroup, but then  $gHg^{-1} = H$ . Proving  $H$  normal subgroup.

Let  $N_q = \#$  of  $q$ -Sylow subgroups.

$$N_q \equiv 1 \pmod{q} \text{ and } N_q \mid p$$

It follows  $N_q = 1$  or  $N_q = p$ .

If  $N_q = p$ , then  $p \equiv 1 \pmod{q}$ . Hence  $q \mid p-1$ .  $\#$

So  $N_q = 1$ .

Thus, the unique  $q$ -Sylow subgroup  $K$  is normal.

$$H \cong \mathbb{Z}/p\mathbb{Z} \quad \& \quad K \cong \mathbb{Z}/q\mathbb{Z}$$

Hence,  $H \cap K = \{1\}$

It follows by previous theorem and its proof

$$G = H \times K \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/pq\mathbb{Z}$$

### Proof of First Sylow theorem

Elementary lemma: The number of subsets of order  $p^m$  of a set w/  $n = p^m r$  elements w/  $p \nmid r$  is  $N = \binom{n}{p^m} = \frac{n(n-1)\dots(n-p^m+1)}{p^m(p^m-1)\dots(p^m-r)\dots 1}$   
Furthermore,  $p \nmid N$ .

Pf:  $N = \binom{n}{p^m}$  is well-known.

To show  $p \nmid N$ .

Notice, whenever  $p^k \mid (n-k)$  then also  $p^k \mid p^m - k$  and vice versa.

B/c this is the maximal power of  $p$  that divides  $k$ .

The maximal power of  $p$  that divides  $(n-k)$  is the maximal power of  $p$  that divides  $k$ .

And is also the maximal power of  $p$  that divides  $p^m - k$ .

Thus  $p \nmid N$ .

Proof of Sylow th. Let  $S = \{M \subset G \mid M \text{ is a subset of } G \text{ s.t. } |M| = p^m\}$

$$N = |S|.$$

$G$  acts on  $S$  via left multiplication.

$$(g, M) \mapsto gM = \{gm \mid m \in M\}$$

We can decompose  $S$  into disjoint orbits of  $G$ .

So we have

$$N = |S| = \sum_{\text{orbits}} |\text{orbit}|$$

We know  $p \nmid N$ . Hence there is an orbit  $O = G(M)$  s.t.  $p \nmid |G(M)|$ .

By proposition above,  $|G_M|$  is a power of  $p$ .

(Prop. If  $G$  acts on itself by left multip.,  $M \subset G$ . Then  $|G_M|/|M|$ .)

By the orbit stabilizer theorem,

$$p^m \cdot r = |G| = |G_M| \cdot |G(O)|$$

Since  $p \nmid |G(O)|$ , we have  $p^m = |G_M|$

Hence  $G_M$  is  $p$ -Sylow subgroup.

### Proof of Second Sylow theorem

Let  $K$  be a subgroup of  $G$ ,  $H$   $p$ -Sylow subgroup of  $G$ .

W.t.s.  $\exists g \in G \quad H' = gHg^{-1}$  s.t.  $H' \cap K$  is a  $p$ -Sylow subgroup of  $K$ .

Let  $S = C/H$  set of left cosets.

$G$  acts transitively on  $G/H$  by left multiplication.

$$g \cdot (aH) = (ga)H$$

The stabilizer of  $H = H$  is  $H$ .

Can see the the stabilizer of  $aH$  is  $aH a^{-1}$ .

Restrict this action to  $K$ .

$$K \times G/H \rightarrow G/H$$

$$k \cdot aH \mapsto kaH$$

Decompose  $S = C/H$  into  $K$ -orbits.

As  $H$  is  $p$ -Sylow subgroup,  $|G/H|$  is prime to  $p$ . Since  $|G| = p^m r$ ,  $|H| = p^n$ , hence  $|G/H| = r$ . Thus there is a  $K$ -orbit on  $G/H$ ,  $k(aH)$  s.t.  $|k(aH)|$  is not divisible by  $p$ .

Let  $H' = aH a^{-1}$ . Then  $H'$  is  $G_K$  stabilizer in  $G$ .

Thus the stabilizer  $K_{aH}$  is  $H' \cap K$ .

By the orbit stabilizer theorem.

$$|k(aH)| \cdot |K_{aH}| = |K|$$

But  $p \nmid |k(aH)|$ . Thus, if we write  $|K| = p^s \cdot l$

Then  $p^s \mid |K_{aH}|$ .  $H'$  is a  $p$ -group, it has  $p^n$  elements and  $H' \cap K = K_{aH}$  is a subgroup of  $K$ .

Thus,  $|K_{aH}|$  is a power of  $p$

Hence  $K_{aH} = K \cap H'$  is a  $p$ -Sylow subgroup.

### Proof of Third Sylow theorem

Let  $|G| = m = p^m \cdot r$ ,  $p \nmid r$ .

Let  $s$  be the number of  $p$ -Sylow subgroups of  $G$ .

By corollary of 2<sup>nd</sup> Sylow theorem all Sylow subgroups are conjugate to one  $p$ -Sylow subgroup  $H$ .

$G$  acts on  $p$ -Sylow subgroups by conj.

Stabilizer of  $H$  is  $N_G(H)$  normalizer.

$$s = |C(H)| = [G : N_G(H)]$$

by orbit stabilizer theorem.

$H$  subgroup of  $N_G(H)$ ,  $N_G(H)$  subgroup of  $G$ .

Hence  $s = [G : N_G(H)]$  divides  $[G : H]$ , since  $[G : H] = [G : N_G(H)][N_G(H) : H]$

Since  $[G : H] = r$  the first part is proven.

Now  $s \equiv 1 \pmod{p}$ .

$\{H_1, \dots, H_s\}$  set of  $p$ -Sylow subgroups.

$G$  acts on this set by conj. and then also  $H$ .

Decompose  $\{H_1, \dots, H_s\}$  into orbits for  $H$  action.

The orbit of  $H_i$  consists only of  $H_i \Rightarrow H \subset N_G(H_i)$

In this case both  $H$  and  $H_i$  are Sylow subgroups of  $N_G(H_i)$

$|N_G(H_i)|$  divides  $|G| = p^m \cdot r$

But  $H_i$  is a normal subgroup  $N(H_i)$ .

As all  $p$ -Sylow subgroups in  $N(H_i)$  are conj. in  $N_G(H_i)$

we have  $H = H_i$ .

Thus the orbit of  $H$  is the only one w/ one element.

For any other  $H_i$ , by the orbit stabilizer theorem  $|H(N(H_i))|$  is a divisor of the number of elements of  $|H| = p^n$  (and  $|G(N(H_i))| \neq 1$ )

Thus,  $\{H_1, \dots, H_s\}$  is a disjoint union of elements, one of them has 1 element and the rest are divisible by  $p$ .

Hence  $s \equiv 1 \pmod{p}$ .

## Lecture 9

### RING

Definition: A ring is a non-empty set  $R$  together with binary operations:

$$+ : R \times R \rightarrow R : (a, b) \mapsto a+b$$
$$\cdot : R \times R \rightarrow R : (a, b) \mapsto a \cdot b$$

and an element  $0 \in R$ , s.t.

- (1)  $(R, +)$  is a commutative group with identity  $0$ .
- (2)  $\cdot$  is associative  $\forall a, b, c \in R$   
 $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- (3)  $a \cdot (b+c) = a \cdot b + a \cdot c$   
 $(b+c) \cdot a = b \cdot a + c \cdot a$

Def: An element  $1 \in R \setminus \{0\}$  is called a unit element if  $\forall a \in R$   $1 \cdot a = a \cdot 1 = a$ .

Prop. If exist  $1$  is unique.

Pf: Suppose  $y \in R$  unit elements.

$$\text{Notice } x \cdot y = x = y \quad \blacksquare$$

Prop. Let  $R$  ring  $a, b \in R$

- (1)  $a \cdot 0 = 0 \cdot a = 0$
- (2)  $(-a) \cdot b = a(-b) = -ab$
- (3)  $(-a)(-b) = ab$
- (4) If  $R$  is a ring w.r.t.  
 $(-1)a = a(-1) = -a$

$$\text{Pf: (1)} \quad a \cdot 0 = a \cdot (0+0) = a \cdot 0 + a \cdot 0$$

$$\Rightarrow a \cdot 0 = 0$$

Similarly for  $0 \cdot a$ .

$$\text{(2)} \quad (-a) \cdot b + ab = (-a + a) \cdot b = 0 \cdot b = 0$$

$$\Rightarrow (-a) \cdot b = -(ab)$$

Similarly for  $a \cdot (-b)$ .

$$\text{(3)} \quad (-a)(-b) - ab = (-a)(-b) + (-a) \cdot b = (-a) \cdot (-b + b) = (-a) \cdot 0 = 0$$

$$\Rightarrow (-a)(-b) = -(ab) = ab,$$

uniqueness of inverses in a group.

$$\text{(4)} \quad (-1) \cdot a = - (1 \cdot a) = -a$$

$\blacksquare$

Def: Let  $R$  be a commutative ring, an element  $a \in R \setminus \{0\}$  is called a zero-divisor if there exists  $b \in R \setminus \{0\}$  s.t.  $ab = 0$ .

A commutative ring with  $1$  and no zero divisor is called an integral domain.

Prop. (cancellation property)

Let  $R$  be an integral domain. If  $a, b, c \in R$ ,  $a \neq 0$  s.t.

$$ab = ac$$

then

$$b = c$$

$$\text{Pf: } ab = ac \Rightarrow a \cdot (b-c) = 0, a \neq 0 \Rightarrow b-c = 0 \Rightarrow b = c \quad \blacksquare$$

Example:  $\mathbb{Z}_p$  with  $p$  prime is an integral domain.

Pf: Take  $m, n \in \mathbb{Z}_p \setminus \{0\}$ , i.e.  $p \nmid m$  and  $p \nmid n$ . Then  $p \nmid nm$ , hence  $nm \neq 0$  in  $\mathbb{Z}_p$ .

Def:  $R$  ring,  $a \in R$  is a unit if  $\exists b \in R$ :  $ab = ba = 1$ .  $b$  is unique.

The set of units of  $R$  is denoted  $U(R)$ .

### Polynomial Rings

Definition: Let  $R$  be a ring. A polynomial  $f$  with coeffs. in  $R$  is an formal expression

$$f = \sum_{i=0}^m a_i x^i \quad \text{for some } m \geq 0$$
$$a_i \in R$$

Two polynomials

$$f = \sum_{i=0}^m a_i x^i \quad \text{and} \quad g = \sum_{i=0}^n b_i x^i$$

are equal ( $f = g$ ) if (assuming w.l.o.g.  $m \geq n$ )

$$b_j = 0, j \geq m$$

$$\text{and } a_i = b_i, 0 \leq i \leq m.$$

We denote  $\mathbb{R}[x]$  the set of polynomials in  $x$  with coefficients in  $\mathbb{R}$ .

We have an embedding  $i: \mathbb{R} \hookrightarrow \mathbb{R}[x]$   
 $a_0 \mapsto a_0 x^0$

via this we say  $\mathbb{R} \subset \mathbb{R}[x]$

We define a ring structure on  $\mathbb{R}[x]$

For

$$f = \sum_{i=0}^m a_i x^i, \quad g = \sum_{i=0}^n b_i x^i$$

we define

$$f+g = \sum_{i=0}^{\max(m,n)} (a_i + b_i) x^i$$

and

$$f \cdot g = \sum_{r=0}^{m+n} \left( \sum_{i+j=r} a_i b_j \right) x^r$$

•  $0 \in \mathbb{R}$  is the neutral element for addition in  $\mathbb{R}[x]$ .

• If  $1 \in \mathbb{R}$  is the unit,  $1$  is also the unit in  $\mathbb{R}[x]$ .

•  $\mathbb{R}$  is a subring of  $\mathbb{R}[x]$ .

Def: Let  $f = \sum_{i=0}^m a_i x^i \in \mathbb{R}[x]$  w/  $a_m \neq 0$ . The degree of  $f$ , denoted  $\deg f$ , is  $m$ , the highest power of  $x$  w/ coeff. different to 0.

Prop. Let  $\mathbb{R}$  be an integral domain,

(1)  $f, g \in \mathbb{R} \setminus \{0\}$

$$f \cdot g \neq 0 \text{ and } \deg(f \cdot g) = \deg f + \deg g$$

(2)  $\mathbb{R}[x]$  is an integral domain

Pf: Clearly (1)  $\Rightarrow$  (2).

$$\text{Let } f = \sum_{i=0}^m a_i x^i, \quad a_m \neq 0, \quad g = \sum_{i=0}^n b_i x^i, \quad b_n \neq 0.$$

$$f \cdot g = \sum_{r=0}^{m+n} c_r x^r, \quad c_r = \sum_{i+j=r} a_i b_j;$$

$$\text{Notice } c_{m+n} = a_m \cdot b_n \neq 0$$

$$\text{Thus, } f \cdot g \neq 0, \quad \deg(f \cdot g) = \deg f + \deg g.$$

Prop. Let  $\mathbb{R}$  be an integral domain, then  $\mathcal{U}(\mathbb{R}) = \mathcal{U}(\mathbb{R}[x])$ .

Pf: If  $a \in \mathcal{U}(\mathbb{R})$ , then  $a^{-1} \in \mathbb{R}[x]$  and  $a \in \mathcal{U}(\mathbb{R}[x])$ .

Let  $f \in \mathcal{U}(\mathbb{R}[x])$ . Then, for some  $g \in \mathbb{R}[x]$

$$f \cdot g = 1$$

By the previous prop.  $0 = \deg(1) = \deg(f \cdot g) = \deg f + \deg g \Rightarrow \deg f = \deg g = 0$

Thus,  $f, g \in \mathbb{R}$  and  $f \in \mathcal{U}(\mathbb{R})$ .

## Lecture 10

Definition: A ring  $\mathbb{R}$  with 1 is a division ring if  $\mathcal{U}(\mathbb{R}) = \mathbb{R} \setminus \{0\}$ .

A commutative division ring is a field.

Prop: Every finite integral domain is a field.

Pf: Let  $a \in \mathbb{R} \setminus \{0\}$ . We have

$$a \cdot (b+c) = a \cdot b + a \cdot c, \quad \text{for all } b, c \in \mathbb{R}.$$

i.e.  $a \cdot : \mathbb{R} \rightarrow \mathbb{R}$

$$b \mapsto a \cdot b$$

is a group homomorphism  $(\mathbb{R}, +) \rightarrow (\mathbb{R}, +)$

Since  $a \cdot c = 0$  iff  $c = 0$ , b/c  $\mathbb{R}$  is an integral domain.

$\ker(a \cdot) = \{0\}$ . Thus,  $a \cdot : \mathbb{R} \rightarrow \mathbb{R}$  is injective.

As  $\mathbb{R}$  is finite and  $a \cdot$  injective,  $a \cdot$  must be bijective.

Let  $b \in \mathbb{R}$ , with  $a \cdot b = 1$ . We know  $b$  exists by the surjectivity of  $a \cdot$ .

Hence  $a^{-1} = b$  and  $a \in \mathcal{U}(\mathbb{R})$ .

Def: Let  $A, B$  be rings. A map  $\varphi: A \rightarrow B$  is said to be a ring homomorphism if for all  $a, b \in A$

$$\begin{aligned}\varphi(a+b) &= \varphi(a) + \varphi(b) \\ \varphi(a \cdot b) &= \varphi(a) \cdot \varphi(b)\end{aligned}$$

A bijective homomorphism  $\varphi: A \rightarrow B$  is called an isomorphism.

And a isomorphism  $\varphi: A \rightarrow A$  is called an automorphism.

Remarks: Since a ring homomorphism  $\varphi: A \rightarrow B$  is also a group homomorphism  $\varphi: (A, +) \rightarrow (B, +)$  we have

$$\varphi \text{ injective} \Leftrightarrow \ker \varphi = \{0\}$$

Also,  $\ker \varphi$  is a subring of  $A$ .

Def: Let  $A$  be a ring. A subset  $I \subset A$  is an ideal if

- (1)  $I$  is a subgroup for  $(A, +)$
- (2) For all  $x \in I$  and  $a \in A$ ,  $x \cdot a \in I$  and  $a \cdot x \in I$ .

In particular an ideal is an ideal.

Ex:  $\{0\}$  is an ideal,  $A$  is an ideal.

Lemma: Let  $\varphi: A \rightarrow B$  be a ring homomorph, then  $\ker \varphi$  is an ideal of  $A$ .

More generally, if  $I$  is an ideal of  $B$ , then  $\varphi^{-1}(I)$  is an ideal of  $A$ .

P.F: As  $I$  is a subgroup of  $(B, +)$  and  $\varphi$  is also a group homomorphism between  $(A, +)$  and  $(B, +)$  we have  $\varphi^{-1}(I)$  subgroup of  $(A, +)$ .

Let  $x \in \varphi^{-1}(I)$ ,  $a \in A$ .

$$\varphi(ax) = \varphi(a) \cdot \varphi(x)$$

(Clearly  $\varphi(x) \in I$ . Hence  $\varphi(a) \cdot \varphi(x) \in I$ .

$$\text{So, } \varphi(ax) \in \varphi^{-1}(I).$$

Lemma: Let  $\varphi: A \rightarrow B$  be a surjective ring homomorphism.

The map  $I \mapsto \varphi^{-1}(I)$  is a bijection from the set of ideals of  $B$  to the set of ideals of  $A$  which contains  $\ker \varphi$ .

P.F: We define the inverse map

$$\begin{array}{ccc} \left. \begin{array}{c} \text{ideals of } A \\ \text{which contain } \ker \varphi \end{array} \right\} & \xrightarrow{\quad} & \left. \begin{array}{c} \text{ideals of } B \\ I \end{array} \right\} \\ J & \longmapsto & \varphi(J) \end{array}$$

Let  $J \subset A$  ideal s.t.  $\ker \varphi \subset J$ . We know  $\varphi(J)$  is a subgroup of  $(B, +)$ .

Let  $b \in B$ ,  $y \in \varphi(J)$ , can write  $b = \varphi(a)$ ,  $a \in A$ ,  $y \in \varphi(x)$ ,  $x \in J$ .

$$by = \varphi(a) \cdot \varphi(x) = \varphi(a \cdot x) \in \varphi(J)$$

namely  $by \in \varphi(J)$ . Thus,  $\varphi(J)$  is an ideal of  $B$ .

Let  $I$  be an ideal in  $B$ .  $\varphi(\varphi^{-1}(I)) = I$ .

Let  $J$  be an ideal in  $A$  s.t.  $\ker \varphi \subset J$ .

We have  $\varphi^{-1}(\varphi(J)) \supseteq J$

Let  $z \in \varphi^{-1}(\varphi(J))$ , then  $\varphi(z) \in \varphi(J)$  i.e.  $\exists x \in J$  s.t.  $\varphi(z) = \varphi(x)$ .

Notice  $0 = \varphi(z) - \varphi(x) = \varphi(z-x)$ , thus  $z-x \in \ker \varphi \subset J$

Since  $z-x \in J$ ,  $x \in J$  we have  $z \in J$ .

Hence  $\varphi^{-1}(\varphi(J)) = J$ .

And  $\ell$  is bijective.

Def: Let  $R$  be a commutative ring,  $a_1, \dots, a_n \in R$ . The ideal generated by  $a_1, \dots, a_n$  is

$$\langle a_1, \dots, a_n \rangle = \{ a_1r_1 + \dots + a_nr_n \mid r_1, \dots, r_n \in R \}$$

For  $a \in R$ ,  $\langle a \rangle = aR = \{ ar \mid r \in R \}$  is called the principal ideal generated by  $a$ . An ideal that it is generated by just one element is called a principal ideal.

Lemma: Let  $R$  be an integral domain. Let  $a, b \in R$ .

Then  $\langle a \rangle = \langle b \rangle$  iff  $a = ub$  for some  $u \in U(R)$ .

P.F: " $\Rightarrow$ " Sps.  $\langle a \rangle = \langle b \rangle$ , then  $b = ua$  for some  $u \in R$ .

also  $a = wb$  for some  $w \in R$ .

Hence  $b = uwb$ , so  $uw = 1$  and  $u, w \in U(R)$ .

" $\Leftarrow$ " Sps.  $a = ub$ ,  $u \in U(R)$ , then  $b \in \langle a \rangle$  and  $\langle b \rangle \subset \langle a \rangle$ .

Also  $b = u^2a$ . Then  $a \in \langle b \rangle$  and  $\langle a \rangle \subset \langle b \rangle$ .

Namely  $\langle a \rangle = \langle b \rangle$ .

- Remark:
- (1) Let  $I$  be an ideal in a ring  $R$ . If  $I$  contains a unit, then  $I = R$ .
  - (2) The only ideals in a field  $F$  are  $F$  and  $\{0\}$ .
  - (3) Let  $\kappa$  be a field,  $\varphi: \kappa \rightarrow R$  be a ring homomorphism to a ring  $R$ . Then,  $\varphi \equiv 0$  or  $\varphi$  is injective.

- Pf:
- (1) Let  $a \in I \cap \text{U}(R)$ ,  $a^{-1} \in R$ , hence  $1 = a^{-1}a \in I$ . Then, if  $x \in R$ ,  $x = x \cdot 1 \in I$ , so  $R = I$ .
  - (2) Use  $\text{U}(\kappa) = \{\kappa \setminus \{0\}\}$ . Hence either only  $0 \in I$  or  $I = R$ .
  - (3)  $\ker \varphi$  is an ideal of  $\kappa$ . By (2)  $\ker \varphi = \{0\}$  and  $\varphi$  is injective or  $\ker \varphi = \kappa$  and  $\varphi \equiv 0$ .

Def: Let  $R$  be a ring,  $I \subset R$  ideal.

$(R, +)$  is commutative, hence  $I$  is a normal subgroup.

The quotient group  $R/I = \{x+I : x \in R\}$

w/  $x+I = \{x+a : a \in I\} = [x]$  equivalence class.

for equivalence relation

$$x \sim y \Leftrightarrow x-y \in I$$

The group operation is  $(x+I) + (y+I) = (x+y)+I$

Prop:  $R/I$  is a ring with operation

$$[x]+[y] := [x+y]$$

$$[x] \cdot [y] := [xy]$$

The natural projection  $\pi: R \rightarrow R/I$  is a surjective ring homomorphism.  
 $x \mapsto [x]$

Pf: By normality of  $I$  as a subgroup, the well-definedness of addition  $\circ$  given.

Since  $[x]+[y] = [x+y]$ ,  $\pi$  is clearly a group homomorphism with kernel  $I$ .

To show the product is well-defined.

Let  $x, y, y' \in R$  s.t.  $[x] = [x']$ ,  $[y] = [y']$ .

Then  $x-x' \in I$ ,  $y-y' \in I$ .

$$xy - x'y' = (\underbrace{x-x'}_I)y - x'(\underbrace{y-y'}_I) \in I$$

Hence,  $[x] \cdot [y] = [x \cdot y] = [x' \cdot y'] = [x'] \cdot [y']$

and the product is well-defined.

Associativity and distributivity are induced from  $R$ .

$$([x] \cdot [y]) \cdot [z] = [x \cdot y] \cdot z = [x \cdot (y \cdot z)] = [x] \cdot ([y] \cdot [z]).$$

$$[x] \cdot ([y] + [z]) = [x \cdot (y+z)] = [x \cdot y + x \cdot z] = [x] \cdot [y] + [x] \cdot [z].$$

For  $x, y \in R$ :

$$\pi(x+y) = [x+y] = [x] + [y] = \pi(x) + \pi(y)$$

Hence  $\pi$  is a ring homomorphism.

Corollary: There is a bijection from the ideals of  $R/I$  to the ideals of  $R$  containing  $I$ .

Theorem (Universal property):

Let  $\varphi: A \rightarrow B$  be a ring homomorphism. Let  $I \subset A$  ideal s.t.  $\ker \varphi \subset I$ .

Then, there is a unique homomorphism  $\bar{\varphi}: A/I \rightarrow B$  s.t. the diagram

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ \downarrow \pi & \nearrow \bar{\varphi} & \\ A/I & & \end{array}$$

commutes. Furthermore,  $\ker \bar{\varphi} = (\ker \varphi)/I$ ,  $\bar{\varphi}(A/I) = \varphi(A)$ .

Pf:  $\bar{\varphi} = \bar{\varphi} \circ \pi$  means  $\bar{\varphi}([x]) = \varphi(x)$

Hence, if  $\bar{\varphi}$  exists it is unique. To prove  $\bar{\varphi}$  exists we show  $\bar{\varphi}([x]) = \varphi(x)$  is well-defined.

If  $[x] = [y]$ , then  $x-y \in I \subset \ker \varphi$ . Hence  $0 = \varphi(x-y) = \varphi(x) - \varphi(y)$ . So,  $\varphi(x) = \varphi(y)$ .

And  $\bar{\varphi}([x]) = \bar{\varphi}([y])$ .

It is immediate that  $\bar{\varphi}$  is a ring homomorphism.

Also, by definition  $\bar{\varphi}(R) = \bar{\varphi}(R/I)$ .

And  $[x] \in \ker \bar{\varphi} \Leftrightarrow \bar{\varphi}([x]) = 0 \Leftrightarrow \varphi(x) = 0 \Leftrightarrow x \in \ker \varphi \Leftrightarrow [x] \in (\ker \varphi)/I$ .

### Theorem (Homomorphism theorem)

If  $\varphi: A \rightarrow B$  is surjective a ring homomorphism w/  $\ker \varphi = I$ .  
Then the map  $\bar{\varphi}: A/I \rightarrow B$  is an isomorphism.

Pf: By the universal property  $\bar{\varphi}$  is a surjective ring homomorphism with kernel  $\ker \bar{\varphi} = (\ker \varphi)/I = I/I = \{0\}$ .  
Hence,  $\bar{\varphi}$  is an isomorphism. ■

### Lecture 10

#### Prime ideals and maximal ideals

In the following a ring is always taken to be commutative and with 1.

Def: An ideal  $P \subset R$  is called a prime ideal if whenever  $ab \in P$ , for  $a, b \in R$ , we have  $a \in P$  or  $b \in P$ .

Def: An ideal  $M$  in a ring  $R$  is called a maximal ideal if there is no other ideal  $I$  in  $R$  s.t.  $M \subsetneq I \subset R$ .

Prop: (1) Let  $R$  be a ring. An ideal  $P \subset R$  is prime iff  $R/P$  is an integral domain.

(2) An ideal  $M \subset R$  is maximal iff  $R/M$  is a field.

Pf:  $R$  is commutative with 1. Thus  $R/P$  is also commutative with 1.

For given  $a, b \in R$ .  $[a] \in R/P$

$$[a] = 0 \Leftrightarrow a \in P$$

$$\text{Hence, } [a][b] = [a \cdot b] = 0 \Leftrightarrow ab \in P$$

Thus,  $[a]$  is a zero divisor iff  $a \notin P$  and  $\exists b \in R \setminus P$  s.t.  $ab \in P$

i.e.  $R/P$  has zero divisors iff  $P$  is not prime.

Spc.  $M \subset R$  ideal s.t.  $R/M$  is a field.

Thus, the only ideals of  $R/M$  are  $\{0\}$  and  $R/M$ .

By prop. this statement is equivalent to saying that the only ideals of  $R$  containing  $M$  are  $M$  and  $R$ .

Which is equivalent to  $M$  being maximal!

" $\Leftarrow$ " is, thus, proven.

For " $\Rightarrow$ " we spc. that the only ideals of  $R/M$  are  $\{0\}$  and  $R/M$ , again this is equivalent to  $M$  being maximal!

Let  $a \in R \setminus M$ , we wish to show  $\exists b \in R/M$  s.t.  $ab = 1$

$\langle a \rangle$  is an ideal, and  $\langle a \rangle = M$ .

Thus,  $\langle a \rangle = R/M$ , in particular  $1 \in \langle a \rangle$ . From  $R/M$  is a field. ■

Corollary: Every maximal ideal is prime.

Pf: Let  $M \subset R$  be a maximal ideal. We know  $R/M$  is a field. Hence  $R/M$  is a integral domain, proving  $M$  prime.

#### Polynomial rings over a field

Let  $K$  be a field,  $K[x]$  polynomial ring.

Def: Let  $R$  be an integral domain,  $a, b \in R$ . We say  $a$  divides  $b$ , denoted  $a|b$  if  $\exists c \in R : a \cdot c = b$ . Otherwise, we say  $a$  does not divide  $b$  and denote it by  $a \nmid b$ .

We have,

$$a|b \Leftrightarrow b \in \langle a \rangle$$

$$a|b, b|c \Rightarrow a|c$$

$$a|b, a|c \Rightarrow a|(b+c)$$

#### Theorem:

Let  $f, g \in K[x]$ ,  $g \neq 0$ . Then, exist unique  $q, r \in K[x]$ ,  $\deg r < \deg g$  s.t.

$$P = fg + r$$

Pf: If  $\deg f < \deg g$  we're done,  $q=0$ ,  $r=f$ .

If  $\deg f \geq \deg g$  proceed by induction on  $m := \deg f$ .

Let  $a, b$  the leading coefficient of  $f, g$  resp.

Let  $\bar{f} = f - \frac{a}{b}x^{\deg g} \cdot g$ , since  $m > \deg g$  we have  $\frac{a}{b}x^{\deg g} \cdot g \in K[x]$  and has degree at most  $\deg g$ .

Also,  $\deg \bar{f} = m$  implying  $\deg \bar{f} \leq m$ .

The coeff. of  $x^m$  in  $\bar{f}$  is  $a - \frac{a}{b} \cdot b = 0$ . Thus,  $\deg \bar{f} < m$ .

By induction  $\bar{f} = q'g + r'$  with  $\partial r' < \partial g$ .

$$\text{Put } r := r' \\ q := q' + \frac{a}{b} x^{\partial g}$$

$$\text{Notice } qg + r = q'g + r + \frac{a}{b} x^{\partial g} \cdot g \\ = \bar{f} + \frac{a}{b} x^{\partial g} \cdot g = f$$

And  $\partial r < \partial g$ . So existence is proven.

To prove uniqueness, s.p.s. we have  $q, r, q', r'$  s.t.  $\partial r < \partial g, \partial r' < \partial g$ .

$$f = qg + r = q'g + r'$$

Then

$$0 = (q - q')g + r - r' \\ \Rightarrow (q - q')g = r' - r$$

If  $q \neq q'$ , then  $\partial(q - q') \geq 0$ . It follows  $\partial(r - r') \geq \partial g$  \*

Hence  $q = q'$  and  $r = r'$ .

This proof gives an explicit algorithm:

$$\begin{array}{r} (x^3 + 4x^2 + x + 1) \mid x+2 \\ x^3 + 2x^2 \\ \hline 2x^2 + x + 1 \\ 2x^2 + 4x \\ \hline -3x + 1 \\ -3x - 6 \\ \hline 7 \end{array}$$

$$\Rightarrow x^3 + 4x^2 + x + 1 = (x+2)(x^2 + 2x - 3) + 7$$

Def: Let  $R$  be an integral domain. Let  $a_1, \dots, a_n \in R$ .

An element  $r \in R$  is called a common divisor of  $a_1, \dots, a_n$  if  $r | a_i$  for all  $i = 1, \dots, n$ .

$r \in R$  is the greatest common divisor of  $a_1, \dots, a_n$  if it is a common divisor and for every common divisor  $s$  divides  $r | s$ .

Remark: The greater common divisor is unique up to multiplication by units.

FF: Let  $r, s \in R$  be gcd of  $a_1, \dots, a_n \in R$ . Then  $r | s$  and  $s | r$ , hence  $r = us$ , for  $u \in U(R)$ .

In  $k[x]$  use division with remainder to compute the gcd.

Let  $f, g \in k[x] \setminus \{0\}$ .

$$r_0 := f, \quad r_1 := g$$

Write via division with rest

$$r_0 = q_1 r_1 + r_2, \quad \partial r_2 < \partial r_1$$

$$r_1 = q_2 r_2 + r_3, \quad \partial r_3 < \partial r_2$$

Inductively

$$r_{i-1} = q_i r_i + r_{i+1}, \quad \partial r_{i+1} < \partial r_i$$

This procedure stops when

$$r_m = q_m r_{m+1}$$

Claim:  $r_m$  is the gcd( $f, g$ ) in  $k[x]$ .

FF: We have  $r_m | r_{m+1}$ . Also

$$r_{m+2} = q_{m+1} r_{m+1} + r_m$$

thus  $r_m | r_{m+2}$

Inductively,  $r_m | r_{i+1}$  and  $r_m | r_i$  which implies  $r_m | r_{i+1}$  for all  $i = 1, \dots, m$ .

In particular  $r_m | r_0 = f, r_m | r_1 = g$ . So  $r_m$  is a common divisor.

Now let  $s$  be a common divisor of  $f, g$ .

$$s | f = r_0, \quad s | g = r_1$$

Since  $r_0 = q_1 r_1 + r_2$

It follows,  $s | r_2$ .

$$\text{Inductively } r_{i-1} = q_i r_i + r_{i+1}$$

and  $s | r_{i+1}, s | r_i$ , hence  $s | r_{i+2}$ .

Thus,  $s | r_m$ .

Remark: Let  $K$  be a field, let  $k$  be a subfield. Then  $k[x]$  is a subring of  $K[x]$ .

Corollary: Let  $f, g \in k[x]$ , let  $h = \gcd(f, g)$  in  $K[x]$ . If the leading coeff. of  $h$  is in  $k$ , then  $h \in k[x]$ .

Pf: Let  $\ell$  be the gcd of  $f, g$  as computed by the Euclidean algo. in  $K[x]$ .

As  $\ell$  is computed by repeated division with rest it follows  $\ell \in k[x]$ .

Let  $h$  be a gcd of  $f, g$ .

Then  $h = a \cdot \ell$ ,  $a \in K \setminus \{0\}$ .

Let  $h_n, \ell_m$  be the leading coeffs. of  $h, \ell$  resp.

Notice  $h_n = a \cdot \ell_m$ . If  $h_n \in k$ , we have  $a \in k$ . Thus  $h = a \cdot \ell \in k[x]$ .

Def: Let  $f = \sum_{i=0}^n a_i x^i \in K[x]$ . Let  $R$  be a ring that contains  $K$  subring.

For  $s \in R$  let

$$f(s) = \sum_{i=0}^n a_i s^i \in R.$$

Obs:  $(f+g)(s) = f(s) + g(s)$

$$(f \cdot g)(s) = f(s) \cdot g(s)$$

Hence this evaluation at  $s$

$$\text{eval}_s: K[x] \rightarrow R \\ f \mapsto f(s)$$

is a ring homomorphism.

An element  $s \in R$  is called a zero of the polynomial  $f$  if  $f(s) = 0$ .

Prop: Let  $f \in K[x]$ ,  $a \in K$ . Then  $a$  is zero of  $f$  iff  $(x-a) \mid f$ .

Pf: " $\Leftarrow$ "

Sps.  $(x-a) \mid f$ , then  $f = (x-a)g$ ,  $g \in K[x]$

$$\text{So, } f(a) = (a-a) \cdot g = 0.$$

" $\Rightarrow$ " Sps.  $f(a) = 0$ .

Compute  $f$  divide by  $(x-a)$ .

$$f = (x-a) \cdot q + r, \quad q, r \in K[x], \quad \deg r < \deg(x-a) = 1$$

$$\text{Since } 0 = f(a) = (a-a) \cdot q + r = r. \text{ Hence } r = 0.$$

$$\text{And } (x-a) \mid f.$$

Corollary: Let  $f \in K[x] \setminus \{0\}$ . Then  $f$  has at most  $\deg f$  zeros in  $K$ .

Pf: If  $\deg f = 0$ , then  $f$  is constant and has no zeros.

By induction sps. the theorem proven for polynomials of degree  $n$ .

Let  $f \in K[x]$  s.t.  $\deg f = n+1$ .

If  $f$  has no zeros we're done.

Sps.  $a \in K$  is a zero of  $f$ .

$$\text{Then } f = (x-a) \cdot g, \quad g \in K[x], \quad \deg g = \deg f - 1 = n$$

Notice  $g$  has at most  $n$  zeros.

If  $b$  is a zero of  $f$

$$0 = f(b) = (b-a) \cdot g(b)$$

So, either  $b = a$  or  $b$  is a zero of  $g$ . Proving  $f$  has at most  $n+1$  zeros.

### Euclidean Domains

Intuitively, euclidean domains (ED) are rings where we can divide with rest.

Def:

A ring  $R$  is an ED if there is a function

$$\| \cdot \| : R \setminus \{0\} \rightarrow \mathbb{Z}_{\geq 0} \text{ s.t.}$$

$$(1) \forall a, b \in R : \exists q, r \in R : a = qb + r \wedge (\|r\| < \|b\| \vee r=0)$$

$$(2) \forall b \in R \setminus \{0\} \cup \{0\}, a \in R \setminus \{0\} \text{ we have } \|ab\| \leq \|a\|$$

Cex:

$$(1) (\mathbb{Z}, \|m\| = |m|)$$

$$(2) (R[i], \|x\| = 2^{\deg(x)})$$

$$(3) \mathbb{Z}[i] = \{n+mi \in \mathbb{C} \mid n, m \in \mathbb{Z}\}$$

$$\text{is an ED with } \|n+mi\| = \sqrt{n^2+m^2}$$

$$\text{Notice, for } z, w \in \mathbb{C}, \|z-w\| = \|z\| \|w\|$$

$$\text{Let } z, w \in \mathbb{Z}[i], w \neq 0.$$

$$\text{Let } z/w = a+bi \text{ quotient in } \mathbb{C}$$

$$\text{Choose } n, m \in \mathbb{Z}, |a-n| \leq \frac{1}{2}$$

$$|b-m| \leq \frac{1}{2}$$

$$\text{Put } q = n+im \in \mathbb{Z}[i]$$

$$\|(z-w)-(n+im)\| = (a-n)^2 + (b-m)^2 \leq \frac{1}{2}$$

$$\text{Let } r := z - (n+im)w. \text{ Notice}$$

$$z = (n+im)w + r.$$

$$\text{And, } \|r\| = \|(z-w)-(n+im)\| \|w\| \leq \frac{1}{2} \|w\| < \|w\|.$$

$$\text{Hence, } (\mathbb{Z}[i], \|\cdot\|) \text{ is an ED.}$$

Def: An ID  $R$  is called an principal ideal domain (PID) if every ideal of  $R$  is principal.  
i.e.  $\forall I \subseteq R \text{ ideal: } \exists a \in R \text{ s.t. } I = \{x \in R \mid x = ra \text{ for some } r \in R\}$ .

Theorem: Every ED is an PID.

PF: If  $I = \{0\}$ , then  $I = \{0\}$ .

Now sps.  $I$  not trivial.

Let  $a \in I \setminus \{0\}$  s.t.

$$\|a\| \leq \|x\| \quad \forall x \in I.$$

This minimum exists, since the codomain of  $\|\cdot\|$  is the  $\mathbb{N} \cup \{0\}$  which is well-ordered.

Let  $b \in I$ . We do division with rest:

$$b = qa + r, \text{ for } q, r \in R, \|r\| < \|a\|$$

$$\text{If } r = 0, \text{ then } b = qa \text{ and } b \in \langle a \rangle.$$

If  $r \neq 0$ , then  $\|r\| < \|a\|$ ,  $r \in I \setminus \{0\}$  contradicting the minimality of  $a$ .  $\blacksquare$

Hence  $I = \langle a \rangle$ .  $\blacksquare$

In particular,  $\mathbb{Z}, \mathbb{Z}[i], K[x]$  are PIDs.

Prop: Let  $R$  be a PID. Let  $a_1, \dots, a_n \in R$ .

A gcd  $d$  of  $a_1, \dots, a_n$  exists and  $d = a_1x_1 + a_2x_2 + \dots + a_nx_n$  for  $x_1, \dots, x_n \in R$ .

PF: Let  $I = \langle a_1, \dots, a_n \rangle$  the ideal generated by  $a_1, \dots, a_n$ .

Since  $R$  is a PID, there is a  $d \in I$  s.t.  $I = \langle d \rangle$ .

First we have  $d \in I$ , hence  $d = a_1x_1 + \dots + a_nx_n$ , for  $x_1, \dots, x_n \in R$ .

Also, for all  $i = 1, \dots, n$   $a_i \in I = \langle d \rangle$ , hence  $d \mid a_i$ .

Let  $e$  be a common divisor of  $a_1, \dots, a_n$ .

Then,  $e \mid a_1x_1 + \dots + a_nx_n = d$ . Hence,  $d$  is the gcd.  $\blacksquare$

## Irreducibility of Polynomials

Def: Let  $R$  be an ID.

An element  $g \in R \setminus \{0\}$  is called irreducible if  $g \notin U(R)$  and if

$$g = ab, \quad a, b \in R$$

then  $a \in U(R)$  or  $b \in U(R)$ .

Otherwise (if  $\exists a, b \in R \setminus U(R)$  s.t.  $g = ab$ )  $g$  is said to be reducible.

e.g.:

(1)  $q \in \mathbb{Z}$  irreducible iff  $q = \pm p$ ,  $p$  prime

(2) If  $K$  is a field it has no irreducible elements.

(3) In  $K[x]$ ,  $ax+b$  with  $a \in K^*, b \in K$   
is irreducible.

Indeed, if  $ax+b = f \cdot g$ ,  $f, g \in K[x]$ ,  $0 = \deg(ax+b) = \deg(f) + \deg(g)$ , so  $\deg(f) = 0$  or  $\deg(g) = 0$ .

Thus,  $f \in U(K[x])$  or  $g \in U(K[x])$ .

Prop: Let  $R$  be a PID,  $p \in R$  irreducible element.

$\langle p \rangle$  is maximal ideal in  $R$  and  $R/\langle p \rangle$  is a field.

Pf: Let  $I \subset R$  be an ideal s.t.  $p \in I$ .

Since  $R$  PDI,  $I = \langle a \rangle$ ,  $a \in R$ .

Hence  $p = x \cdot a$ , for some  $x \in R$ .

Either,  $x$  is a unit, then  $\langle p \rangle = \langle a \rangle$ .

or  $a$  is a unit, and  $\langle a \rangle = R$ .

Hence,  $\langle p \rangle$  is maximal. ■

Corollary: Let  $K$  be a field and  $p \in K[x]$  irreducible, then  $K[x]/\langle p \rangle$  is a field. which contains  $K$  as a subfield.  
(The restriction of  $\pi: K[x] \xrightarrow{\cong} K[x]/\langle p \rangle$  to  $K$  is isomorphism onto the image).

Def: A polynomial

$$f = \sum_{i=0}^n a_i x^i \in \mathbb{Z}[x]$$

is called primitive if  $a_0, \dots, a_n$  are coprime.

Lemma (Gauss):

Let  $f, g \in \mathbb{Z}[x]$  be primitive. Then  $f \cdot g$  is primitive.

Pf: By contradiction.  $f \cdot g$  not primitive. Write

$$f = \sum_{i=0}^n a_i x^i, \quad g = \sum_{j=0}^m b_j x^j$$

Then there is a prime  $p \in \mathbb{Z}$  s.t.  $p$  divides all coeffs of  $f \cdot g$  but does not divide all  $b_j, a_i$ .

Let  $i$  be minimal s.t.  $p$  does not divide  $a_i$ :

$j \leq i$  s.t.  $p$  does not divide  $b_j$ .

Let  $c_{i,j}$  be the coeffs of  $x^{i+j}$  in  $f \cdot g$ .

Then

$$c_{i,j} = a_i b_j + \sum_{k \geq i} a_k b_{j+k-i} + \sum_{k < j} a_k b_{i+j-k}$$

Since  $i+j-k < j$  ( $k < i$ ),  $p \nmid b_{i+j-k}$

and  $p \nmid a_k$  ( $k < i$ )

Hence,

$$p \nmid c_{i,j} - a_i b_j$$

But  $p \mid a_i b_j$ ,

And  $p \nmid c_{i,j}$ . ■

Theorem (Gauss Lemma):

Let  $f \in \mathbb{Z}[x]$  non-constant primitive polynomial

Then  $f$  is irreducible in  $\mathbb{Z}[x]$  iff  $f$  is irreducible in  $\mathbb{Q}[x]$ .

PF: " $\Leftarrow$ " If  $f$  is reducible in  $\mathbb{Z}[x]$  then  $f = gh$ ,  $g, h \in \mathbb{Z}[x]$  not units in  $\mathbb{Z}[x]$ .

If  $\partial g = 0$ ,  $g$  is a non-unit of  $\mathbb{Z}$

$g$  is a common factor of all coeffs. of  $f > gh$ , hence  $f$  is not primitive.

Thus  $\partial g > 0$ , similarly  $\partial h > 0$ .

So  $f$  is reducible in  $\mathbb{Q}[x]$ . By contrapositive, " $\Rightarrow$ " is proven.

" $\Rightarrow$ " Sup.  $f = gh$ ,  $g, h \in \mathbb{Q}[x]$  s.t.  $\partial g, \partial h > 0$  i.e.  $f$  reducible in  $\mathbb{Q}[x]$ .

Clear denominators of coeffs. of  $f$  and  $g$  and divide by the gcd of non coeffs.

So

$$f = \frac{a}{b} g' h' \text{ with } a, b \in \mathbb{Z} \text{ and } g', h' \text{ primitive in } \mathbb{Z}[x] \\ \text{and } a, b \text{ coprime.}$$

$$\text{Write } g' = \alpha g, h' = \beta h \quad \alpha, \beta \in \mathbb{Q}$$

Also

$$b f = \alpha g' h'$$

Both,  $f$ ,  $g' h'$  are primitive

gcd of coeffs. of  $b f$  is  $b$ , and the gcd of  $\alpha g' h'$  is  $a$ .

Hence  $a = b$  or  $a = -b$ .

$$\text{So, } f = g' h' \text{ or } f = -g' h'.$$

Hence  $f$  is not irreducible in  $\mathbb{Z}[x]$ .

Theorem: (Eisenstein's criterion)

Let  $f = \sum_{i=0}^n a_i x^i \in \mathbb{Z}[x]$  be primitive  $n > 0$ .

If there is a prime number  $p$  s.t.

$$p \mid a_0, p \mid a_1, \dots, p \mid a_{n-1}, p \nmid a_n$$

but  $p^2 \nmid a_0$ .

Then  $f$  is irreducible in  $\mathbb{Z}[x]$  and, therefore, in  $\mathbb{Q}[x]$ .

PF: Sup.  $f = g \cdot h$  with  $g, h \in \mathbb{Z}[x]$ .

Let

$$f = \sum_{i=0}^n b_i x^i, \quad g = \sum_{i=0}^r c_i x^i, \quad h = \sum_{i=0}^l d_i x^i, \quad r, l \neq 0,$$

As  $p \mid a_0$  but  $p^2 \nmid a_0$  and  $a_0 = b_0 c_0$

We have  $p$  divides precisely one of  $b_0, c_0$  (otherwise  $p^2 \mid a_0$ )

W.l.o.g. sup.  $p \mid b_0$  and  $p \nmid c_0$ .

Notice  $n = r + l$ ,  $a_n = b_r \cdot c_l$

Since  $p \nmid a_n$ ,  $p \nmid b_r c_l$ .

So there exists a maximal  $j \in \{1, \dots, k\}$  s.t.

$p \mid b_i$  for all  $i < j$ ,  $p \nmid b_j$

$$a_j = b_j c_0 + b_{j-1} c_1 + \dots + b_0 c_j$$

By our choice of  $j$

$p \nmid b_j$  and  $p \mid b_{j-1}, p \mid b_{j-2}, \dots, p \mid b_0$ .

Thus,  $p \mid a_j$ . Hence  $j = n$ , and  $k$  must equal  $n$ .

Proving  $\partial h = 0$ .

Remark: If  $f \in k[x]$  is a polynomial of degree 2 or 3. Then  $f$  is reducible iff  $f$  has a zero.

Indeed, if  $f = gh$ ,  $g, h \in \mathbb{Z}[x]$  of degree  $> 0$ .

Then  $\deg g = 1$  or  $\deg h = 1$ , i.e.  $h = ax + b$ . Thus  $-\frac{b}{a}$  is a zero of  $f$ .

If  $f \in \mathbb{Z}[x]$  is monic i.e.  $f = x^n + \sum_{i=0}^{n-1} a_i x^i$

If  $a \in \mathbb{Z}$  is a zero of  $f$ . Then  $a \in \mathbb{Z}$ , also in  $\mathbb{Z}$ .

Thus, if  $f \in \mathbb{Z}[x]$  is monic,  $\deg f \leq 3$ ,  $f$  irreducible iff none of the divisors of  $a_0$  is a zero of  $f$ .

Remark: Let  $f = \sum_{i=0}^n a_i x^i \in k[x]$ , let  $a \in k$ .

$f$  is irreducible in  $k[x] \Leftrightarrow f(x+a)$  is irreducible over  $k$

Indeed:  $\sigma_a : k[x] \rightarrow k[x]$   
 $g \mapsto g(x+a)$

is clearly an isomorphism (with inverse  $\sigma_{-a}$ )

Hence  $f$  irreducible iff  $\sigma_a(f)$  irreducible.

E.g. Let  $p \in \mathbb{Z}$  be a prime.

$f = x^{p-1} + \dots + x + 1$  is irreducible in  $\mathbb{Q}[x]$ .

Notice

$$(x-1)f = x^p - 1$$

$$x \cdot \sigma_{-1}(f) = (x+1)^p - 1$$

$$\text{So, } \sigma_{-1}(f) = \sum_{i=1}^p \binom{p}{i} x^{i-1}$$

Since  $p \mid \binom{p}{i}$  for  $1 \leq i \leq p-1$

So, by the Eisenstein's criteria,  $\sigma_{-1}(f)$  is irreducible. Hence  $f$  is irreducible.

## Field extension

Def: A subring  $k$  of a field  $L$  is called a subfield of  $L$  if  $k$  is a field. Then  $L$  is called an extension of  $k$ , denoted  $L/k$ .

If  $L/k$  and  $K/k$  are extensions of  $k$ .

A homomorphism  $\varphi: K \rightarrow L$  is called a  $k$ -homomorphism if  $\varphi|_k$  is the identity.

Remark: Let  $L/k$  be a extension. Then  $(L, +)$  is an abelian group

and the restriction of the multiplication on  $L$  to  $k \times L$  gives  $\circ: k \times L \rightarrow L$ .

Then, for all  $a, b \in k$ ,  $x, y \in L$

$$\begin{aligned} \text{dist. laws: } (a+b) \cdot x &= a \cdot x + b \cdot x \\ a \cdot (x+y) &= a \cdot x + a \cdot y \end{aligned}$$

$$\text{assoc. laws: } (a \cdot b) \cdot x = a \cdot (b \cdot x)$$

$$\text{idnt. } x = 1 \cdot x$$

Hence  $L$  is a  $k$ -vector space.

Def: Let  $L/k$  be a field extension the degree  $[L:k]$  of  $L/k$  is the dimension of  $L$  as a  $k$ -vector space.

Remark: If  $[L:k] = 1$ . Then  $L = k$ . Since for all  $a \in L$ ,  $a = r \cdot 1 = r$ ,  $r \in k$  (choosing 1 as basis vector).

Def: Let  $K/k$  be a field extension, and let  $L/k$  be a field extension of  $K/k$ . Then  $L$  is an intermediate field of  $K/k$ .

Theorem (Degree th.):

Let  $L$  be an intermediate field of  $K/k$ . Then,  $[K:k] = [K:L][L:k]$  (using comb.  $\# = \# \cdot \# = n \cdot m = \# \cdot n$ , for  $n \in \mathbb{Z}_{\geq 0}$ )

Pf: If  $[K:L]$  is not infinite or  $[L:k]$  is not finite it's clear  $[K:k]$  is not infinite.

So suppose both finite.

Let  $[K:L] = m$ ,  $[L:k] = n$ .

Let  $x_1, \dots, x_m$  basis of  $L/k$ ,  $y_1, \dots, y_n$  basis of  $K/L$ .

We claim  $\{x_i y_j | i=1, \dots, m, j=1, \dots, n\}$  is a basis for  $K/k$ .

Take  $g \in K$ ,  $g = \sum_{j=1}^n b_j y_j$ ,  $b_j \in L$ .

Also  $b_j = \sum_{i=1}^m a_{ij} x_i$ ,  $a_{ij} \in k$ .

$$\text{Hence } g = \sum_{j=1}^m \sum_{i=1}^n a_{ij} x_i y_j$$

So our set generates  $K$ .

Given  $a_{ij} \in k$  s.t.

$$\sum_{j=1}^m \sum_{i=1}^n a_{ij} x_i y_j = 0$$

As  $y_j$  are linearly independent over  $L$  we get

$$\sum_{i=1}^n a_{ij} x_i = 0 \text{ for all } j$$

Again,  $x_i$  linearly independent over  $k$  so

$$a_{ij} = 0 \text{ for all } i, j$$

Hence our set is linearly independent.

Corollary: If  $K/k$  is a field extension and  $L$  an intermediate field,  $[L:k] \mid [K:k]$ .

### Algebraic extensions:

Fix a field extension  $K/k$

Def: A element  $\alpha \in K$  is called algebraic over  $k$ , if there is some non-null polynomial

$$f = \sum_{i=0}^n b_i x^i \in k[x]$$

$$\text{with } f(\alpha) = 0, \text{ i.e. } 0 = \sum_{i=0}^n b_i \alpha^i \in k.$$

Otherwise,  $\alpha$  is called transcendental.

$K/k$  is called an algebraic extension if all elements  $\alpha \in K$  are algebraic over  $k$ .

e.g.:  $\sqrt{3}$  algebraic over  $\mathbb{Q}$ , since it is a zero of  $x^2 - 3$

$$(x - \sqrt{3})(x + \sqrt{3}) = x^2 - 3$$

$\pi$  transcendental over  $\mathbb{Q}$

Def: Let  $a_1, \dots, a_n \in K$ . The extension of  $k$  generated by  $a_1, \dots, a_n$  is the smallest intermediate extension  $L \subset K$  that contains  $a_1, \dots, a_n$ . It is denoted  $k(a_1, \dots, a_n)$

Def: Let  $\alpha \in K$  be algebraic over  $k$ , then  $k(\alpha)$  is called a simple algebraic extension.

Def: A polynomial  $f \in k[x]$  is monic if its leading coeff. is 1.

For  $f \in k[x] \setminus \{0\}$  there is a unique monic polynomial  $g \in k[x]$  s.t.  $\langle g \rangle = \langle f \rangle$ .

Let  $\alpha \in K$  algebraic over  $k$ .

Let  $\text{eva}: k[x] \rightarrow K$

$$f \mapsto f(\alpha)$$

As  $\alpha$  is algebraic, the kernel of  $\text{eva}$  is not  $\{0\}$ .

As  $k[x]$  is P.I.D,  $\text{ker}(\text{eva})$  is principal, so there is a unique monic polynomial  $f_\alpha$  s.t.

$$\text{ker}(\text{eva}) = \langle f_\alpha \rangle$$

This polynomial is called the minimal polynomial of  $\alpha$  over  $k$ .

Prop: Let  $\alpha \in K$ , algebraic over  $k$ . The minimal poly. of  $\alpha$  over  $k$  is the unique monic irreducible poly.  $f \in k[x]$  s.t.  $f(\alpha) = 0$ .

B: Let  $f_\alpha$  be the min. poly. of  $\alpha$  over  $k$ .

Sp.  $f_\alpha = gh$ ,  $g, h \in k[x]$ .

$$f_\alpha(\alpha) = 0, \text{ hence}$$

$$g(\alpha)h(\alpha) = 0$$

Wlog.  $g(\alpha) = 0$ . Hence  $g \in \text{ker}(\text{eva})$ , and so  $g = l \cdot f_\alpha$  for  $l \in k[x]$ .

$$f_\alpha = l \cdot f_\alpha \cdot h \Rightarrow l \cdot h = 1$$

$$\Rightarrow h \in U(k[x]) = U(k) \subset k$$

Hence  $f_\alpha$  irreducible.

Conversely, sp.  $g \in k[x]$  is a monic irreducible polynomial with  $g(\alpha) = 0$

$g \in \text{ker}(\text{eva}) = \langle f_\alpha \rangle$ . Hence  $g = l \cdot f_\alpha$ ,  $l \in k[x]$ . By the irreducibility of  $g$ ,  $l \in U(k)$ . Since  $g$  monic,  $l = 1$ .

Thus  $g = f_\alpha$ .

C.S. Let  $p$  be a prime number,  $m \in \mathbb{Z}_{\geq 0}$

$x^m - p$  is the min. poly. of  $\sqrt[p]{p}$  over  $\mathbb{Q}$  (by prop. and the Eisenstein's criterion).

Theorem (description of the simple algebraic extensions)

Let  $a \in \mathbb{K}$ , algebraic over  $\mathbb{K}$ . Let  $f_a$  be the min. poly. of  $a$  over  $\mathbb{K}$ . Let  $m := \deg f_a$ .

Then,  $(1) \quad \mathbb{K}(a) \cong \mathbb{K}[x]/(f_a)$

(2)  $[\mathbb{K}(a) : \mathbb{K}] = m$ . Moreover,  $\{1, a, a^2, \dots, a^{m-1}\}$  is a basis for  $\mathbb{K}(a)$ .

P.F.:

$$(1) \quad ev_a: \mathbb{K}[x] \rightarrow \mathbb{K}(a)$$

$$g \mapsto g(a)$$

is a ring homomorphism, whose kernel is  $\langle f_a \rangle$ .

Let  $L := ev_a(\mathbb{K}[x])$ , a subring of  $\mathbb{K}(a)$ .

By isomorphism th.

$$L \cong \mathbb{K}[x]/(f_a).$$

As  $f_a$  is irreducible,  $\langle f_a \rangle$  is maximal, thus  $L$  is a field which contains  $\mathbb{K}$ .

Clearly,  $a = ev_a(x) \in L$ . Hence  $\mathbb{K}(a) \subset L$ . Proving  $L = \mathbb{K}(a)$ .

(2) We have proven,  $ev_a: \mathbb{K}[x] \rightarrow \mathbb{K}(a)$  surjective.

Thus,  $\mathbb{K}(a) = \{g(a) \mid g \in \mathbb{K}[x]\}$

Let  $b \in \mathbb{K}(a)$ ,  $b = g(a)$  for some  $g \in \mathbb{K}[x]$ .

If  $2g \geq m$ , we have

$$g = q \cdot f_a + r, \quad q, r \in \mathbb{K}[x], \text{ or } r = 0.$$

By  $f_a(a) = 0$ , we have  $g(a) = r(a)$ . So  $b = r(a)$ . Write  $b = \sum_{i=0}^{m-1} b_i a^i$ . Then  $b \in \langle 1, a, \dots, a^{m-1} \rangle$ .

So our proposed basis generates  $\mathbb{K}(a)$ .

Sps. there is  $b_0, \dots, b_{m-1} \in \mathbb{K}$  s.t.

$$\sum_{i=0}^{m-1} b_i a^i = 0$$

$$\text{Sos } g = \sum_{i=0}^{m-1} b_i x^i \in \ker(ev_a) = \langle f_a \rangle.$$

But  $2g < 2f_a$ . Hence  $g = 0$ , so  $b_i = 0$  for  $i = 0, \dots, m-1$ . Proving  $1, \dots, a^{m-1}$  linearly independent.

Remark: Let  $\mathbb{K}(a)/\mathbb{K}$  be a simple algebraic extension of degree  $m$  and min. pol.  $f_a$  of  $a$ .

Then

$$\mathbb{K}(a) = \left\{ \sum_{i=0}^{m-1} b_i a^i \mid b_i \in \mathbb{K} \right\}$$

e.g.:  $\mathbb{C} = \mathbb{R}(i)$ , min. pol. of  $i$  is  $x^2 + 1$ . Thus

$$\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}\}$$

Theorem: Let  $L/\mathbb{K}$  be a field extension

$L/\mathbb{K}$  finite  $\Leftrightarrow L/\mathbb{K}$  is algebraic and exists finitely many

$a_1, \dots, a_n \in L$  s.t.  $L = \mathbb{K}(a_1, \dots, a_n)$

P.F.: " $\Rightarrow$ " Let  $m := [L : \mathbb{K}]$ .

Then, for  $a \in L$ ,  $1, a, \dots, a^m$  are linearly dependent in  $L$ .

So, there are  $b_0, \dots, b_m \in \mathbb{K}$  s.t.

$$\sum_{i=0}^m b_i a^i = 0$$

Hence,

$$g = \sum_{i=0}^m b_i x^i \in \mathbb{K}[x] \setminus \{0\}$$

s.t.  $g(a) = 0$ . So  $a$  is algebraic.

Also, let  $a_1, \dots, a_n$  be a basis for  $L$  over  $\mathbb{K}$ . Then,

$$\mathbb{K}(a_1, \dots, a_n) = L.$$

" $\Leftarrow$ " By induction over  $m$ .  $m=0$  is trivial.

Sps.  $L = \mathbb{K}(a_1, \dots, a_n)$

let  $L' = \mathbb{K}(a_1, \dots, a_n)$ . Notice  $[L : \mathbb{K}] = m \in \mathbb{N}$  by induction.

We know  $a_1, \dots, a_n$  alg. over  $\mathbb{K}$  and, thus, over  $L'$ .

Then,  $[L : \mathbb{K}] = [L' : \mathbb{K}] \cdot [L : L'] = \deg(g) \cdot m$ , w/  $g$  is the min. pol. of  $a_{n+1}$  over  $L'$ , notice also  $L = L'(a_{n+1})$

## Extensions of field homomorphism.

Fix  $\mathbb{F}/\mathbb{K}$  field extension.

**Def:** Let  $\varphi: \mathbb{K} \rightarrow \mathbb{K}'$  be a field isomorphism.

Let  $L/\mathbb{K}, L'/\mathbb{K}'$  be field extensions.

Then an isomorphism  $\tilde{\varphi}: L \rightarrow L'$  is called an extension of  $\varphi$  if

$$\tilde{\varphi}|_{\mathbb{K}} = \varphi.$$

**Remark:** If  $\varphi: \mathbb{K} \rightarrow \mathbb{K}'$  is an isomorphism, then

$$\varphi_*: \mathbb{K}[\mathbb{K}] \rightarrow \mathbb{K}'[\mathbb{K}]: \sum_{i=0}^n a_i x^i \mapsto \sum_{i=0}^n \varphi(a_i) x^i$$

is a ring isomorphism.

**Theorem:** Let  $\varphi: \mathbb{K} \rightarrow \mathbb{K}'$  be a ring isomorphism.  $L/\mathbb{K}, L'/\mathbb{K}'$  field extensions.

Let  $a \in L$  algebraic with min. pol.  $f_a$ .

Take  $a' \in L'$  s.t.  $\varphi_*(f_a)(a') = 0$ .

Then, there exists a unique extension

$$\tilde{\varphi}: \mathbb{K}(a) \rightarrow \mathbb{K}'(a')$$

with  $\tilde{\varphi}(a) = a'$ ,  $\tilde{\varphi}|_{\mathbb{K}} = \varphi$ .

**Pf:** (Uniqueness)

Let  $\phi: \mathbb{K}(a) \rightarrow \mathbb{K}'(a')$  be such an extension.

Note  $\mathbb{K}(a) = \{g(a) \mid g \in \mathbb{K}[x]\}$

$\mathbb{K}'(a') = \{h(a') \mid h \in \mathbb{K}'[x]\}$ .

Thus,  $b \in \mathbb{K}(a)$ ,  $b = g(a)$ ,  $g \in \mathbb{K}[x]$ .

$$g = \sum_{i=0}^n b_i x^i, \quad b_i \in \mathbb{K}$$

$$\begin{aligned} \phi(b) &= \phi(g(a)) = \phi\left(\sum_{i=0}^n b_i a^i\right) = \sum_{i=0}^n \phi(b_i) \phi(a)^i = \\ &= \sum_{i=0}^n \varphi(b_i) a'^i \\ &= \varphi(g)(a') \end{aligned}$$

(Existence)

Define  $\phi: \mathbb{K}(a) \rightarrow \mathbb{K}'(a')$

$$g(a) \mapsto (\varphi_* \circ g)(a)$$

Clearly,  $\phi$  is a ring homomorphism and surjective, since  $\varphi_*: \mathbb{K}[x] \rightarrow \mathbb{K}'[x]$  isomorphism.

Thus,  $\phi$  is an isomorphism, since  $\ker \phi$  is an ideal of a field, and, by the surjectivity, is not trivial.

For  $b \in \mathbb{K}$ ,  $\phi(b) = \varphi_*(b) = \varphi(b)$ .

So  $\phi|_{\mathbb{K}} = \varphi$ , also  $\phi(a) = \varphi_*(\mathbb{K}(a)) = \mathbb{K}(a) = a'$ . ■

**Corollary:** Let  $L/\mathbb{K}$  be a field extension. Take  $a, a' \in L$  with the same min. pol. Then there is a unique  $\mathbb{K}$ -isomorphism

$$\phi: \mathbb{K}(a) \rightarrow \mathbb{K}(a')$$

$$\text{s.t. } \phi(a) = a'$$

## ALGEBRAIC CLOSURE

Def: Let  $L$  be a field,  $L$  is algebraically closed if the following equivalent statements hold:

- 1) Every  $f \in L[x]$  has a zero in  $L$ .
  - 2) Every  $f \in L[x]$  splits over  $L$  into linear factors i.e.
- $$\exists b, a_1, \dots, a_n \in L \text{ s.t. } f = b(x - a_1) \dots (x - a_n)$$

Pf of eqn.

$$(2) \Rightarrow (1) \text{ is clear}$$

$$(1) \Rightarrow (2)$$

Let  $a \in L$  be a zero of  $f \in L[x]$ , we can write

$$f = (x - a)g, \quad g \in L[x]$$

$$\deg g = \deg f - 1$$

(2) follows by induction on the degree of  $f$ .

Eg.:  $\mathbb{Q}$  is not alg. cl.,  $x^2 - 3$  has no roots over  $\mathbb{Q}$

$\mathbb{R}$  " " " " " " " "  $\mathbb{R}$

$\mathbb{Q}[i]$  is alg. closed.

Def: A field  $L/\mathbb{K}$  is called an algebraic closure, if the field extension is algebraic and  $L$  is algebraically closed.

Theorem: (1) Every field has an algebraic closure

(2) If  $K, L$  are algebraic closures of  $\mathbb{K}$ , then there exists a  $\mathbb{K}$ -isomorphism

$$\varphi: K \rightarrow L$$

Example:  $\mathbb{Q}[i]$  is an algebraic closure of  $\mathbb{Q}$

$\mathbb{Q}[i]$  is algebraic closure of  $\mathbb{R}$

## Splitting field:

Theorem: Let  $f \in \mathbb{K}[x]$ , irreducible. Then there is a simple algebraic extension  $L/\mathbb{K}$  s.t.  $f$  has a zero in  $L$ .

$$[\mathbb{L} : \mathbb{K}] = \deg f.$$

Pf:  $f$  is irreducible. Hence  $\langle f \rangle$  is a max. ideal in PID  $\mathbb{K}[x]$ .

Thus  $L = \mathbb{K}[x]/\langle f \rangle$  is a field extension of  $\mathbb{K}$ .

Notice  $O = [f]$  in  $L$ . Write

$$f = \sum_{i=0}^n a_i x^i \Rightarrow O = [f] = \sum_{i=0}^n [\alpha_i] [x]^i = \sum_{i=0}^n a_i [\mathbb{x}]^i = f([\mathbb{x}])$$

Hence,  $f$  has a zero in  $L$ , namely,  $[\mathbb{x}]$ .

$L = \mathbb{K}([\mathbb{x}])$ , b/c for  $g \in \mathbb{K}[x]$ , we have  $[g] = g([\mathbb{x}])$ .

$f$  is irreducible over  $\mathbb{K}[x]$ , by dividing by the leading coeff., can sps.  $f$  monic.

Then  $f$  is the minimal pol. of  $[\mathbb{x}]$ . ■

When creating a field extension in this way, we say we formally adjoin a root to  $\mathbb{K}$ .

Corollary: Let  $f \in \mathbb{K}[x]$ ,  $\deg f = n > 0$ , then there exists a field extension of at most degree  $n$ , s.t.  $f$  has a root.

Def. Let  $f \in \mathbb{K}[x]$  pol. of degree  $n$ . A finite extension  $L/\mathbb{K}$  is called the splitting field of  $f$  over  $\mathbb{K}$  if

- (1)  $f$  splits over  $L$  into linear factors.
- (2)  $f$  does not split over any intermediate field into linear factors.

$$\mathbb{K} \subset F \subset L$$

Corollary: Let  $f \in \mathbb{K}[x]$  monic.

- (1) If  $L/\mathbb{K}$  is a field extension s.t.  $f$  splits in  $L$  into linear factors

$$f = (x - a_1) \dots (x - a_n)$$

Then,  $\mathbb{K}(a_1, \dots, a_n)$  is splitting field of  $f$  over  $\mathbb{K}$ .

- (2) There exists a splitting field  $L/\mathbb{K}$  of  $f$  of degree  $[\mathbb{L} : \mathbb{K}] \leq \deg f$

- (3) Let  $L/\mathbb{K}$  be a splitting field of  $f$  over  $\mathbb{K}$ . Let  $F/\mathbb{K}$  be an intermediate field

Then  $L$  is also a splitting field of  $f$  over  $F$ .

PF: (1) Let  $L/k$  s.t.

$$f = (x - a_1) \dots (x - a_m) \text{ over } L.$$

Clearly,  $f$  splits over  $K/k = k(a_1, \dots, a_m)$

Sps.  $M/k$  intermediate field  $M \subset K$  s.t.  $f$  splits over  $M$ .

$$f = (x - c_1) \dots (x - c_n), \quad c_i \in M$$

$$\forall i: 0 = f(a_i) = (a_i - c_1) \dots (a_i - c_n)$$

$$\Rightarrow a_i = c_j \text{ for some } j = 1, \dots, n$$

$$\Rightarrow \forall i: a_i \in M$$

$$\text{Hence } k(a_1, \dots, a_m) \subset M.$$

(2) By prev corollary there exist an extension of  $K_1/k$  of degree at most  $\deg f$  s.t.  $f$  has a zero in  $K_1$ .

$$\text{Let } g = f/(x - a_1) \in K_1[x] \text{ of deg. } n-1.$$

By induction  $f$  splits over  $F$  which is an extension of  $K_1$  of degree at most  $(n-1)!$

$$[F : k] = [F : K_1][K_1 : k] \leq n!$$

If  $a_1, \dots, a_n$  are zeros of  $f$  in  $F$ , then  $k(a_1, \dots, a_n)$  is a splitting field of  $f$  over  $k$  (by (1))  
and  $[k(a_1, \dots, a_n) : k] = [F : k] \leq n!$

(3)  $f \in k[x]$ , so also  $f \in F[x]$  and splits over  $L$ .

Since  $F$  does not split over any intermediate field,  $f$  does not split over  $F$ .

Example: (1) If  $f \in k[x]$  irreducible of degree 2,  $b$  is a zero in an extension of  $k$ .

Then  $k(b)$  is the splitting field of  $f$  over  $k$ .

(2) Splitting field of  $f = x^4 + 1$  over  $\mathbb{Q}$ .

Let  $\alpha \in \mathbb{C}$  be any zero of  $f$ .

Claim:  $\mathbb{Q}(\alpha)$  is a splitting field of  $f$  over  $\mathbb{Q}$ .

RE: We see  $-\alpha, \frac{1}{\alpha}, -\frac{1}{\alpha}$  are zeros of  $f$ , all different (otherwise  $\alpha = -\alpha$ ,  $\alpha = 0 \neq \alpha$ ;  $\alpha = -\frac{1}{\alpha}$ ,  $\alpha^2 = -1$ ,  $\alpha^4 = 1 \neq -1 \neq 0$ )

$$\text{Thus, } x^4 + 1 = (x - \alpha)(x + \alpha)(x - \frac{1}{\alpha})(x + \frac{1}{\alpha})$$

So,  $f$  splits over  $\mathbb{Q}(\alpha)$  into linear factors and, therefore,  $\mathbb{Q}(\alpha)$  is the splitting field.

(3) Splitting field  $x^3 - 2$  over  $\mathbb{Q}$ . Can write

$$x^3 - 2 = (x - \sqrt[3]{2})(x - e^{\frac{2\pi i}{3}}\sqrt[3]{2})(x - e^{\frac{4\pi i}{3}}\sqrt[3]{2})$$

Therefore,  $\mathbb{Q}(\sqrt[3]{2}, e^{\frac{2\pi i}{3}})$  is splitting field of  $x^3 - 2$  over  $\mathbb{Q}$ .

$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$  and  $e^{\frac{2\pi i}{3}} \notin \mathbb{Q}(\sqrt[3]{2})$  b/c. not in  $\mathbb{R}$ .

Thus,  $[\mathbb{Q}(\sqrt[3]{2}, e^{\frac{2\pi i}{3}}) : \mathbb{Q}(\sqrt[3]{2})] = 2$ .

Hence  $[\mathbb{Q}(\sqrt[3]{2}, e^{\frac{2\pi i}{3}}), \mathbb{Q}] = 6 = 3!$ .

### Extension of field isomorphisms to splitting fields

Theorem: Let  $\varphi: k \rightarrow k'$  be a field isomorphism.

Let  $f \in k[x] \setminus \{0\}$  polynomial.

Let  $f' = \varphi_*(f)$ .

Let  $L, L'$  be splitting field of  $f, f'$  over  $k, k'$  resp.

Then there is an isomorphism

$$\phi: L \rightarrow L', \quad \phi|_k = \varphi.$$

PF: By induction over  $[L : k]$ . If  $[L : k] = 1$ , then

$L = k$ . Then,  $f$  splits over  $k$ . Since  $\varphi$  isomorphism  $f'$  also splits over  $k'$ .

$k'$  is an extension of itself.

If  $[L : k] > 1$ , then  $f$  has an irreducible factor  $g \in k[x]$  of degree  $> 1$ .

Let  $g' = \varphi_*(g) \in k'[x]$ ,  $g'$  also irreducible

Let  $a \in L$  be a zero of  $g$ .

Let  $a' \in L'$  be a zero of  $g'$ .

Thus  $k(a)/k, k'(a')/k'$  are simple alg. extn.

By prev. thm. there exists an isomorphism

$$\tilde{\varphi}: k(a) \rightarrow k'(a') \text{ with } \tilde{\varphi}|_k = \varphi, \tilde{\varphi}(a) = a'.$$

$$[L : k(a)] [k(a) : k] = [L : k]$$
  
$$\geq 2$$

$\Rightarrow [L : k(a)] \leq [L : k]$ ,  $L$  splitting field of  $f$  over  $k(a)$

By induction there is a field isomorphism

$$\phi: L \rightarrow L', \text{ with } \phi|_{k(a)} = \tilde{\varphi}, \text{ so } \phi|_k = \varphi.$$

Remark: We don't know how many such extension exists.

Corollary: If  $L, L'/k$  are splitting field of  $f \in k[x]$  over  $k$ , there is a  $k$ -isomorphism  $\phi: L \rightarrow L'$ .

### Normal extension

Def: An extension  $L/k$  is called normal, if every polynomial  $f \in k[x]$  with a zero in  $L$ , splits over  $L$  into linear factors

Example:  $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$  is not normal

$\sqrt[3]{2}$  is root of  $x^3 - 2$  over  $\mathbb{Q}(\sqrt[3]{2})$   
but  $x^3 - 2$  doesn't split over  $\mathbb{Q}(\sqrt[3]{2})$

Theorem: A finite field extension  $L/k$  is normal iff  $L$  is the splitting field of a polynomial  $f \in k[x]$ .

Pf: " $\Leftarrow$ " Let  $L$  be the splitting field of  $f \in k[x]$

Let  $g \in k[x]$  be irreducible with a zero  $\alpha \in L$ .

Let  $\beta$  be another zero of  $g$  over an extension of  $L$ .

Since  $g$  is irreducible,  $k(\alpha)/k$ ,  $k(\beta)/k$  are simple alg. extensions.

With same minimal polynomial (i.e.  $g$ )

thus there is a  $k$ -isomorphism

$$\gamma: k(\alpha) \rightarrow k(\beta), \gamma(\alpha) = \beta$$

$L$  is splitting field of  $f$  over  $k$ . Hence  $L$  splitting field of  $f$  over  $k(\alpha)$ ?  
 $L(\beta)$  is splitting field of  $f$  over  $k(\beta)$ .

By extension of field isomorphism to the splitting fields.

There is an isomorphism  $\phi: L \rightarrow L'$  s.t.  $\phi|_{k(\alpha)} = \gamma$

In particular,  $\phi|_k = \text{id}_k$

Thus,  $\phi: L \rightarrow L(\beta)$  is an isomorphism between  $k$ -vector spaces.

$$[L(\beta) : L] = [L(\beta) : E]/[L : k] = 1$$

Hence  $L(\beta) = L$  i.e.  $\beta \in L$ .

Putting all roots of  $g$  over any extension are already in  $L$ .

" $\Rightarrow$ "

Let  $L/k$  finite normal extension.

Can write  $L = k(a_1, \dots, a_n)$ ,  $a_i \in L$  algebraic over  $k$ .

Let  $f_i$  minimal poly. of  $a_i$  over  $k$ .

Then  $f_i$  has a zero in  $L$ . Hence  $f_i$  splits over  $L$  into linear factors.

Let  $f = f_1 \cdots f_n$ ,  $f$  clearly splits over  $L$ .

And  $L$  is the splitting field of  $f$  over  $k$ .

### Characteristic of a field:

Df. Let  $k$  be a field. The characteristic of  $k$  is the smallest  $n \in \mathbb{Z}_{\geq 0}$  with  $n \cdot 1 = \underbrace{1 + \dots + 1}_{n \text{ times}} = 0$  if it exists such  $n$ , otherwise  $k$  is defined to be zero. We denote it by  $\text{char}(k)$

e.g.  $\text{char}(\mathbb{Q}) = \text{char}(\mathbb{R}) = 0$

$$\text{char}(\mathbb{Z}/p\mathbb{Z}) = p$$

Remarks: (1)  $\text{char}(k) = 0$  or  $\text{char}(k)$  prime for all fields  $k$ .

(2) If  $L/k$  is an extension,  $\text{char}(L) = \text{char}(k)$ .

Pf: "Let  $I = \{n \in \mathbb{Z} : n \cdot 1 = 0 \text{ in } k\}$ .  $I$  is an ideal"

Note, by dist. law

$$(m \cdot 1)(n \cdot 1) = mn \cdot 1 \quad \text{for all } m, n \in \mathbb{Z}.$$

Thus, if  $(nm) \cdot 1 = 0$  in  $k$ ,  $(n \cdot 1) = 0$  or  $(m \cdot 1) = 0$ .

Hence  $I$  prime ideal.

Since  $I \subset \mathbb{Z}$ ,  $I = \langle 0 \rangle = \{0\}$  or  $I = \langle p \rangle$  for  $p$  prime.

(2)  $1 \in L$  is the same element as  $1 \in k$ .

Thus  $n \cdot 1$  is the same element in  $L$  and  $k$ .

## Separable extensions

Def: An algebraic field extension  $L/k$  is separable, if every irreducible polynomial in  $k[x]$  with a zero in  $L$  does not have multiple roots in its splitting field.

Given  $k$ , if all algebraic field extension is separable,  $k$  is called perfect.

Def: Let  $f = \sum_{i=0}^n a_i x^i \in k[x]$  the derivative of  $f$  is

$$f' := \sum_{i=1}^n a_i i x^{i-1} \in k[x]$$

Lemma: Let  $f \in k[x]$  and  $L/k$  splitting field of  $f$ . Then

$a \in L$  is a multiple root of  $f$  iff  $f(a) = f'(a) = 0$

Pf: Let  $r$  be the order of the root  $a$ . Then

$$f = (x-a)^r \cdot g, \quad g(a) \neq 0.$$

$$\text{So } f' = r(x-a)^{r-1}g + (x-a)^r g'$$

thus

$$f' = (x-a)^{r-1} \cdot h \text{ with } h(a) \neq 0$$

Proving  $r > 1$  iff  $f'(a) = 0$ .

Theorem: Let  $f \in k[x]$  irreducible, then

$f$  has no multiple roots in its splitting field iff  $f' \neq 0$ .

Pf: Let  $L/k$  be the splitting of  $f$ .

If  $f' = 0$ , by prev lemma, every root is multiple in  $L/k$ .

Now sps.  $a \in L$  multiple root of  $f$  in  $L$ .

$$\text{Then } f(a) = f'(a) = 0$$

As  $f$  is irreducible, up to multiplying by elements of  $k$ ,  $f$  is the minimal poly. of  $a$  over  $k$ .

Thus  $f' \in \langle f \rangle$ , i.e.  $f \mid f'$ . Hence,  $f' = 0$ , iff  $f' \geq f$ . But  $\partial f' < \partial f$ , proving  $f' = 0$ .

Corollary: Every field of characteristic 0 is perfect.

Pf: If  $\text{char}(k) = 0$ . Then if  $f \in k[x] \setminus k$ , then

$$f' = \sum_{i=1}^n a_i i x^{i-1} \text{ and } n \cdot a_n \neq 0$$

Hence,  $f' \neq 0$ .

Theorem (primitive element):

Let  $L/k$  be finite separable extension. Then there exists an element  $a \in L$  s.t.  $L = k(a)$

Pf: For simplicity, sps.  $k$  infinite (e.g.  $\text{char } k = 0$ )

As  $[L : k]$  finite we know

$$L = k(a_1, \dots, a_m) \text{ for some } a_1, \dots, a_m \in L.$$

Proceed by induction. Clearly th. holds trivially if  $m=1$ .

Sps. by induction  $k(a_1, \dots, a_{m-1}) = k(a)$  for some  $a \in L$ .

Thus, we part from the assump.

$$L = k(a, b) \quad a, b \in L.$$

We can choose  $c = a + z b$ , for suitable  $z \in k$ .

Let  $f$  be the minimal polynomial of  $a$  over  $k$ .

$$g = " " " " " b \text{ over } k.$$

Let  $F/L$  be a field extension s.t. both  $f$  and  $g$  splits over linear factors on  $F$ .

Let  $x_1, \dots, x_n$  be the roots of  $f$  over  $F$  with multiplicity,

$$y_1, \dots, y_m = " " " " g \text{ over } F = " " .$$

As  $L/k$  is separable extension we have that all roots  $x_i$  are pairwise distinct. Same for  $y_j$ .

Thus for  $i = 1, \dots, n$ ,  $j = 1, \dots, m$

$$z_{ij} = \frac{x_i - a}{b - y_j} \text{ is the unique elem. of } F$$

$$\text{s.t. } a + z_{ij} b = x_i + z_{ij} y_j \left( \Leftrightarrow z_{ij} b - z_{ij} y_j = x_i - a \Leftrightarrow z_{ij} = \frac{x_i - a}{b - y_j} \right)$$

Let  $a \in k$  be different from  $z_{ij}$  ( $i=1, \dots, n$ ;  $j=1, \dots, m$ )

Thus  $a+zb \neq z_i + z_j$ , for all  $i=1, \dots, n$ ;  $j=1, \dots, m$ .

Claim:  $\text{tcc}(c) = \text{tcc}(a, b) = L$

Clearly,  $\text{tcc}(c) \subset \text{tcc}(a, b)$ , since  $c = a+zb$ .

To show  $b \in \text{tcc}(c)$ , let  $h \in \text{tcc}(c)[x]$  be defined by

$$h(x) = f(c - zx)$$

$$\text{so } h(b) = f(c - zb) = f(a) = 0$$

Thus,  $b$  is a zero of  $h$ , so  $(x-b) \mid h$ .

$$\text{Also, } (x-b) \mid g$$

Since  $g$  splits into linear factors in  $F$ , a divisor of  $g$  (up to  $k$ ) is a product of some linear factors of  $g$ .

But  $(x-g_1)$  is a zero of  $h$  iff  $h(g_1) = 0$

$$\text{and } h(g_1) = f(c - zg_1) = f(a+zb - zg_1), \text{ by def. of } z, \quad a+zb - zg_1 \neq x_i \text{ for all zeros of } f.$$

Thus,  $(x-b)$  is the gcd of  $h$  and  $g$ .

As  $h$  and  $g$  both in  $\text{tcc}(c)[x]$  then its gcd also in  $\text{tcc}(c)[x]$ .

Proving  $b \in \text{tcc}(c)$ .

$$\text{So, } a+zb - c \in \text{tcc}(c). \text{ Proving } \text{tcc}(c) = \text{tcc}(a, b) = L.$$

### Finite fields:

If  $p$  is a prime number then  $F_p = \mathbb{Z}_p$  is a field with  $p$  elements.

We'll show that for all prime power  $q = p^n$ , there is a field with  $q$  elements.

And, up to isomorphism these are all the possible finite fields.

Lemma: Let  $F$  be a field of characteristic  $p$ , then (for  $q = p^n$ )

$x^q - x$  has precisely  $q$  simple roots in its splitting group over  $F$ .

Pf: If  $a \in F$  is a root  $x^q - x$

$$(x^q - x)(a) = 0$$

$$(x^q - x)'(a) = (p p^{n-1} - 1)(a) = -1 \neq 0,$$

Lemma: There exist a field of  $q = p^n$  elements.

Pf: Let  $\mathbb{F}$  be the splitting field of  $x^q - x$  over  $F_p$

Let  $\mathbb{F} := \{a \in k \mid a^q - a = 0\}$ , by prev. lemma  $|\mathbb{F}| = q$ .

For  $a, b \in \mathbb{F}$ :

$$\bullet (a^q - a)(b^q - b) = 0 \Rightarrow ab \in \mathbb{F}$$

$$\bullet (a^{-1})^q = (a^q)^{-1} = a^{-q} \Rightarrow a^{-q} \in \mathbb{F}$$

$$\bullet (a \pm b)^q = \sum_{i=0}^q \binom{q}{i} a^i b^{q-i}, \text{ since } \binom{q}{i} = 0 \text{ if } i \neq 0 \text{ and } i \neq q \text{ and } 1 \text{ otherwise}$$

$$= a^q \pm b^q = (a \pm b)$$

$$\Rightarrow a \pm b \in \mathbb{F}$$

$$\bullet \mathbb{F} \neq \emptyset$$

Hence,  $\mathbb{F}$  is a field of  $q$  elements.

Remark: If  $F$  is a finite field of characteristic  $p$ .

Then  $F$  contains  $F_p = \{a^p \mid a \in F\}$  and it is a subset

and  $F_p \cong F_p$ . Hence  $F/F_p$  is a finite extension

In particular  $F$  is a finite dimensional  $F_p$ -vector space.

Thus  $|F| = p^n$ ,  $n = [F, F_p]$

Prop: Let  $F$  be a finite field with  $p^n$  elements, then  $F$  is the splitting field of  $x^q - x$  over  $F_p$ .

Pf: Take  $a \in F$ . We can see  $a^q - a = 0$ .

If  $a = 0$ , this is true.

$(F \setminus \{0\}, \cdot)$  is a group of  $q-1$  elements.

Hence for all  $a \in F \setminus \{0\}$ ,  $a^{q-1} = 1$ , hence  $a^q = a$ .

Proving  $a^q - a = 0$  for all  $a \in F$ .

But  $x^q - x$  has at most  $q$  roots over  $F$ . Thus  $x^q - x$  splits over  $F$ .

Since  $F$  consists exactly of all roots of  $x^q - x$ , hence is the splitting field of  $x^q - x$ .

Theorem: Finite fields with  $q$  elements exists only if  $q$  is a prime power. And every finite field of  $p^n$  elements there is, up to isomorphism, a unique field, namely the splitting field of  $x^{p^n} - x$  over  $\mathbb{F}_p$ .

### Galois theory

Def: Let  $L/\mathbb{K}$  be a field extension. Then the Galois group of  $L$  over  $\mathbb{K}$ , denoted  $\text{Gal}(L/\mathbb{K})$ , is the group of  $\mathbb{K}$ -automorphisms of  $L$ .

Theorem: Let  $\mathbb{K}(a)/\mathbb{K}$  a simple algebraic extension of degree  $m$ . Let  $f \in \mathbb{K}[x]$  be the minimal polynomial.

Let  $R = \{b \in \mathbb{K}(a) \mid f(b) = 0\}$ . Then  $\text{Gal}(\mathbb{K}(a)/\mathbb{K})$  acts simply transitively on  $R$ . In particular,  $\text{Gal}(\mathbb{K}(a)/\mathbb{K})$  is isomorphic to a subgroup of  $S(R)$  and  $|\text{Gal}(\mathbb{K}(a)/\mathbb{K})| = |R| \leq m$

Pf: Let  $\varphi \in \text{Gal}(\mathbb{K}(a)/\mathbb{K})$

If  $f = \sum_{i=0}^n a_i x^i \in \mathbb{K}[x]$  and  $b \in R$

$$0 = f(b) = \varphi \left( \sum_{i=0}^n a_i b^i \right) = \sum_{i=0}^n a_i (\varphi(b))^i = f(\varphi(b)).$$

Thus  $\varphi(b) \in R$ .

And we have,  $\varphi|_R$  maps to  $R$  itself injectively. Since  $R$  finite,  $\varphi|_R$  bijective. Proving  $\varphi|_R \in S(R)$ .

This allows us to define a group homomorphism

$$\text{res}_R : \text{Gal}(\mathbb{K}(a)/\mathbb{K}) \rightarrow S(R)$$

$$(\varphi \circ \varphi|_R = \varphi|_R \circ \varphi|_R)$$

By the existence and uniqueness theorem of field isomorphism extension:

For all  $b, b_1, b_2 \in R$ ,  $\exists! \varphi \in \text{Gal}(\mathbb{K}(a)/\mathbb{K}) : \varphi(b_1) = \varphi(b_2)$ ,

thus  $\text{Gal}(\mathbb{K}(a)/\mathbb{K})$  acts simply transitively on  $R$ .

Which implies  $\text{res}_R : \text{Gal}(\mathbb{K}(a)/\mathbb{K}) \rightarrow S(R)$  is injective.

As  $\text{Gal}(\mathbb{K}(a)/\mathbb{K})$  acts simply transitively,

$$|\text{Gal}(\mathbb{K}(a)/\mathbb{K})| = |R| \leq m.$$

Example: (1)  $\text{Gal}(\mathbb{Q}(\sqrt{2}), \mathbb{Q})$ ,  $f = x^2 - 2$  is min. poly.

$$\begin{cases} \text{id}, & a+b\sqrt{2} \mapsto a+b\sqrt{2} \\ \text{id}, & a+b\sqrt{2} \mapsto a-b\sqrt{2} \end{cases}$$

$$(2) \text{Gal}(\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}) = \{ \text{id} \}$$

The min. poly. is  $f = x^3 - 2$

In  $\mathbb{Q}(\sqrt[3]{2})$ ,  $f$  has no other roots.

Def: A field extension is called a Galois extension if it is separable and normal.

Corollary: Let  $L/\mathbb{K}$  be a Galois extension of degree  $m$ . Then,  $\text{Gal}(L/\mathbb{K})$  is isomorphic to a subgroup of  $S_m$  which acts simply transitively on the numbers  $1, \dots, m$ . In particular,  $|\text{Gal}(L/\mathbb{K})| = [L : \mathbb{K}]$ .

Pf: By the primitive element theorem, there is an element  $a \in L$  s.t.  $L = \mathbb{K}(a)$ . Let  $f$  be the minimal polynomial of  $a$  over  $\mathbb{K}$ . As  $L/\mathbb{K}$  is normal,  $f$  splits over  $L$  in linear factors. Hence, by sep. of  $L$ , all roots of  $f$  in  $L$  are distinct. Hence,  $R$ , the set of roots of  $f$  in  $L$ , has  $m$  elements.

Prop: Let  $L/\mathbb{K}$  be a Galois extension. Let  $a, b \in L$ . Then there is a  $\varphi \in \text{Gal}(L/\mathbb{K})$  with  $\varphi(a) = b \iff a$  and  $b$  have the same minimal polynomial over  $\mathbb{K}$ .

Pf " $\Leftarrow$ " Spc.  $a, b$  have same minimal poly.

By unique extnsn of field isom. of simple alg. extensions there is a  $\mathbb{K}$ -isomorphism  $\varphi : \mathbb{K}(a) \rightarrow \mathbb{K}(b)$  with  $\varphi(a) = \varphi(b)$ .

As  $L/\mathbb{K}$  is normal,  $L$  is the splitting field of some polynomial in  $f \in \mathbb{K}[x]$  over  $\mathbb{K}$ , thus  $L$  is also the splitting field of  $f$  over  $\mathbb{K}(a)$  and  $\mathbb{K}(b)$ .

By extnsn of isom. to splitting fields there exist an isomorphism  $\Phi : L \rightarrow L$  with  $\Phi|_{\mathbb{K}(a)} = \varphi$ .

As  $\Phi|_{\mathbb{K}(x)} = \varphi$ ,  $\varphi|_x = \text{id}_x$ ,  $\Phi \in \text{Gal}(L/\mathbb{K})$  sending  $a$  to  $b$ .  
 "  $\Rightarrow$  "

Sps.  $\varphi \in \text{Gal}(L/\mathbb{K})$  s.t.  $\varphi(a) = b$ .

Let  $f \in \mathbb{K}[x]$  be the min. poly. of  $a$ .

$g \in \mathbb{K}[x]$  be the min. poly. of  $b$ .

$$0 = \varphi(f(a)) = f(\varphi(a)) = f(b)$$

Thus,  $b$  is a root of  $f$ . Hence  $g | f$ .

Conversely,

$$0 = \varphi^{-1}(g(b)) = g(\varphi^{-1}(b)) = g(a)$$

Hence,  $f | g$ . Proving  $f = g$ .

Def: Let  $L/\mathbb{K}$  be a Galois extension. Let  $G$  be a subgroup of  $\text{Gal}(L/\mathbb{K})$ .

$$\text{let } \text{Fix}(G) := \{a \in L \mid \varphi(a) = a \ \forall \varphi \in G\}$$

Theorem: Let  $L/\mathbb{K}$  Galois extension. Then  $\text{Fix}(\text{Gal}(L/\mathbb{K})) = \mathbb{K}$ .

Pf: "  $\supset$ " All elements of  $\mathbb{K}$  are fixed, since elements of the Galois group are  $\mathbb{K}$ -automorphisms.

"  $\subset$ " Let  $\varphi(a) = a$ ,  $\forall \varphi \in \text{Gal}(L/\mathbb{K})$ .

Let  $f$  the min. poly. of  $a$  over  $\mathbb{K}$ .

As  $L/\mathbb{K}$  normal,  $f$  splits in  $L$ .

Let  $b$  be a root of  $f$  in  $L$ .

Then, by above,  $\exists \varphi \in \text{Gal}(L/\mathbb{K}) : \varphi(a) = b$ .

Hence,  $a = b$ .

Since  $L/\mathbb{K}$  separable,  $f$  has no multiple roots.

Hence,  $\partial f = 1$ , proving  $a \in \mathbb{K}$ .

Def: Let  $f \in \mathbb{K}[x] \setminus \mathbb{K}$ . Let  $L$  be the splitting field of  $f$  over  $\mathbb{K}$ .

The Galois group  $\text{Gal}(f) := \text{Gal}(L/\mathbb{K})$ .

Prop: let  $f \in \mathbb{K}[x] \setminus \mathbb{K}$  of degree  $n$ . Let  $R$  be the set of roots of  $f$  over its splitting field  $L$ .

(1)  $\text{Gal}(f)$  is isomorphic to a subgroup of  $S(R)$  and  $|\text{Gal}(f)|$  divides  $n!$ .

(2) If all roots of  $f$  are simple then  $f$  is irreducible iff  $\text{Gal}(f)$  acts transitively on  $R$ .

Pf:  $\text{Gal}(f) = \text{Gal}(L/\mathbb{K})$ ,  $\varphi \in \text{Gal}(f)$

(1) If  $a \in R$ ,  $f(\varphi(a)) = \varphi(f(a)) = \varphi(0) = 0$ , i.e.  $\varphi(a) \in R$ .

Thus restriction to  $R$ :

$$(\varphi: L \rightarrow L) \mapsto (\varphi|_R: R \rightarrow R)$$

gives a group homomorphism  $\text{res}: \text{Gal}(f) \rightarrow S(R)$ .

If  $\varphi \in \text{ker}(\text{res})$ , i.e.  $\varphi|_R = \text{id}$ , then  $\varphi = \text{id}_L$ ,  $b/c \in \mathbb{K}$ .

Hence  $\text{res}$  is injective. Proving  $\text{Gal}(f) \cong \text{Im}(\text{res}) \leq S(R)$ .

thus,  $|\text{Gal}(f)|$  divides  $|S(R)| = |R|! = n!$  divides  $n!$

(2) " $\Leftarrow$ " Sps.  $\text{Gal}(f)$  acts transitively on  $R$  and  $f$  reducible.

Then there exists  $g_1, g_2$  irreducible in  $\mathbb{K}[x]$  s.t.  $g_1, g_2 | f$ .

Since  $\text{Gal}(f)$  acts transitively on  $R \subset L$ .

Let  $a_1$  be a root of  $g_1$  in  $L$  and  $a_2$  be a root of  $g_2$  in  $L$ .

Then  $a_1, a_2 \in R$ . By transitivity of the action

$$\exists \varphi \in \text{Gal}(L/\mathbb{K}) : \varphi(a_1) = a_2$$

$$\text{Then } 0 = \varphi(g_1(a_1)) = g_1(\varphi(a_1)) = g_1(a_2)$$

$$\text{Similarly } g_2(a_1) = 0.$$

Hence, up to multiplication by a constant,  $g_2$  is the minimal polynomial of  $a_2$  over  $\mathbb{K}$ . Thus  $g_2 | g_1$ .

And also  $g_1 | g_2$ . Hence  $g_1 = g_2$ .

So  $g_1^2 | f$ . But then  $f$  has multiple zeroes.

Thus, by contrapositive, this direction is proven.

" $\Rightarrow$ " Suppose  $f$  is irreducible (and  $f$  only has simple roots).  
Take  $a, b \in R$ .

Then,  $f$  is the minimal polynomial of  $a, b$  over  $R$ .

Thus, there exists a  $K$ -automorphism  $\tau: K(a) \rightarrow K(b)$  s.t.  $\tau(a) = b$ .

Notice  $L$  is also the splitting field of  $f$  over  $K(a)$  and over  $K(b)$ .

By the extension of isom. to splitting fields there exists an isom.  $\phi: L \rightarrow L$  s.t.  $\phi|_{K(a)} = \tau$ .

Hence,  $\phi|_K = id$ .

So,  $\phi \in Gal(F)$  and  $\phi(a) = b$ .

Remark: If  $L/K$  is a Galois extension, then  $L$  is the splitting field of some  $f \in K[x]$ .

Then  $Gal(F)$  is in two different ways a subgroup of a symmetry group.

(1) If  $R$  is the set of roots of  $f$  in  $L$ .

Then  $Gal(F)$  is a subgroup of  $S(R)$ .

This is the way to study it for a concrete  $f$ .

(2)  $L/K$  is a simple algebraic extension. By the primitive element theorem

$L = K(\alpha)$ , for some  $\alpha \in L$ .

Let  $g$  be the minimal polynomial of  $\alpha$  over  $K$ .

Let  $\Sigma$  be the set of roots of  $g$  in  $L$ .

Let  $N := |\Sigma|$ , then  $|\Sigma| = N$  (b/c  $L/K$  is normal, meaning  $g$  splits, and separable, namely  $g$  has only simple roots).

Then  $Gal(L/K)$  is isomorphic to a subgroup of  $S_N$  which acts simply transitively on  $\Sigma$ .

Example:  $f = x^4 + 1 \in \mathbb{Q}[x]$

If  $\alpha$  is a root of  $f$ , also  $-\alpha, \frac{1}{2} + \frac{\sqrt{3}}{2}i$  are roots.

So  $\mathbb{Q}(\alpha)$  is the splitting field of  $f$  over  $K$ .

Claim:  $Gal(F) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

Pf: As  $\mathbb{Q}(\alpha)$  is a simple algebraic extension,  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \partial(x^4 - 1) = 4$ .

$$|Gal(F)| = [\mathbb{Q}(\alpha) : \mathbb{Q}] = 4.$$

The map  $\alpha \mapsto -\alpha$  is a field automorphism.

$$\text{If } g = \sum_{i=0}^N a_i \alpha^i \text{ is sent to } g(-\alpha) = \sum_{i=0}^N a_i (-\alpha)^i$$

this is compatible with the operation, thus  $(\alpha \mapsto -\alpha) \in Gal(F)$

$$\text{Also } (\alpha \mapsto 1) \in Gal(F)$$

These two are involutions.

So they generate a subgroup of  $Gal(F)$  that is isomorphic to  $\mathbb{Z}_2 \times \mathbb{Z}_2$ .

Since  $Gal(F)$  has only 4 elements, we have  $Gal(F) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ .

## Fundamental theorem of Galois theory

Def: Let  $L/K$  be a Galois extension. For a subgroup  $H \subset Gal(L/K)$ , the fixed field is

$$Fix(H) = \{ \alpha \in L \mid \forall \varphi \in H \quad \varphi(\alpha) = \alpha \}$$

It can be proven that  $Fix(H)$  is an intermediate field of  $L/K$ .

Recall:  $Fix(Gal(L/K)) = K$ .

Remark: If  $F$  is an intermediate field of  $L/K$

$$Gal(L/F) = \{ \varphi \in Gal(L/K) \mid \varphi|_F = id_F \}$$

So,  $Gal(L/F) \cong Gal(L/K)$

Theorem: Let  $L/k$  be a Galois extension with Galois group  $G$

(1) Let  $\mathcal{H} = \{H \subseteq G\}$  the set of subgroups of  $G$

$\mathcal{I}$  be the set of intermediate fields of  $L/k$ .

We define maps

$$\begin{aligned}\mathcal{H} &\rightarrow \mathcal{I} & \mathcal{I} &\rightarrow \mathcal{H} \\ H &\mapsto \text{Fix}(H) & F &\mapsto \text{Gal}(L/F)\end{aligned}$$

are bijections (and the inverse of each other)

that is,  $\text{Fix}(\text{Gal}(L/F)) = F$  for all  $F \in \mathcal{I}$

$\text{Gal}(L/\text{Fix}(H)) = H$  for all  $H \in \mathcal{H}$

$$(2) [L : \text{Fix}(H)] = |H|, [\text{Fix}(H) : k] = [G : H]$$

$$(3) [L : F] = |\text{Gal}(L/F)|, [F : k] = [G : \text{Gal}(L/F)]$$

Pf: (1) Let  $L/F$  be an intermediate field of  $L/k$ . Then  $L/F$  is a Galois extension.

Since  $L$  is the splitting field of  $f \in k[x]$ , so  $L$  is also the splitting field of  $f \in F[x]$ .

This implies  $L/F$  is normal.

Let  $g$  be the minimal polynomial over  $k$  of some element  $a \in L$  and let  $h$  be the min poly. of  $a$  over  $F$ .

As  $L/k$  is separable,  $g$  has no multiple roots in its splitting field.

$h$  divides  $g$ . Thus  $h$  has no multiple roots.

This proves that  $L/F$  is separable. So  $L/F$  is indeed a Galois extension.

By previous theorem:

$$\text{Fix}(\text{Gal}(L/F)) = F$$

This proves half of (1).

Now let  $G = \text{Gal}(L/k)$  and take a subgroup  $H \subseteq G$ .

Write  $F := \text{Fix}(H)$

By the theorem of the primitive element

$$L = k(a) \text{ for some } a \in L.$$

$$\text{Let } f := \prod_{h \in H} (x - h(a)), f \in L[x] \text{ and } \deg f = |H|$$

All roots of  $f$  in  $L$  are distinct.

Notice, if  $\varphi(a) = \psi(a)$  for  $\varphi, \psi \in H$ ,  $\varphi \circ \psi^{-1}(a) = a$

$$\text{thus } \varphi \circ \psi^{-1} = \text{id}, \varphi = \psi.$$

$$\text{We can write } f = \sum_{i=0}^{|H|} a_i x^i, a_i \in L.$$

$$\text{Take } \varphi \in H, \varphi_* f = \sum_{i=0}^{|H|} \varphi(a_i) x^i = \prod_{h \in H} (x - \varphi(h(a))) = f$$

Thus,  $f \in F[x]$ . We have  $f(a) = 0$ .

Hence the minimal polynomial of  $a$  over  $F$   $g$  divides  $f$ , so  $\deg g \leq \deg f = |H|$   
 $L = k(a) = F(a)$

$$\text{thus } |\text{Gal}(L/F)| = [L : F] = \deg f \leq |H|$$

Clearly,  $\text{Gal}(L/F) = H$

Hence,  $\text{Gal}(L/F) = H$ .

(2) Let  $F = \text{Fix}(H)$ . Then  $L/F$  is a Galois extension

$$\text{So } [L : F] = |\text{Gal}(L/\text{Fix}(H))| = |H|$$

$$[L : F][F : k] = [L : k] = |\text{Gal}(L/k)| = |G|$$

(3)  $L/F$  Galois  $\Rightarrow [L : F] = |\text{Gal}(L/F)|$

$$[L : F][F : k] = [L : k] = |G|.$$

■

Notation: Let  $E$  intermediate field of  $L/K$ .  
 Let  $\alpha \in \text{Gal}(L/K)$   
 Then  $\alpha(E) = \{\alpha(a) \mid a \in E\}$   
 (Every  $\alpha(E)$  is an intermediate field of  $L/K$ )

Lemma: Let  $E$  be an intermediate field of Galois extension  $L/K$ , let  $\alpha \in \text{Gal}(L/K)$ .  
 Then  $\text{Gal}(L/\alpha(E)) = \langle \text{Gal}(L/E) \alpha^{\circ} \rangle$

PF: Let  $\varphi \in \text{Gal}(L/K)$   
 Then  $\varphi \in \text{Gal}(L/\alpha(E)) \iff \varphi(\alpha(a)) = \alpha(a) \text{ for all } a \in E$   
 $\iff \alpha^{-1}\varphi \in \text{Gal}(L/E)$   
 $\iff \varphi \in \alpha(\text{Gal}(L/E)) \alpha^{\circ}$  ■

Theorem: Let  $L/K$  be a Galois extension,  $F$  an intermediate field.

The following are equivalent:

- (1)  $L/F$  is normal
- (2)  $\alpha(F) = F$  for all  $\alpha \in \text{Gal}(L/K)$
- (3)  $\text{Gal}(L/K)$  is a normal subgroup of  $\text{Gal}(L/F)$

PS: "(1)  $\Rightarrow$  (2)"

Let  $L/F$  normal,  $a \in F$ . Let  $\alpha \in \text{Gal}(L/K)$ .

Take  $f$ , the minimal polynomial of  $a$  over  $K$ .

As  $F$  is normal, all roots of  $f$  in  $L$  are in  $F$ .

$$f(\alpha(a)) = \alpha(f(a)) = 0, \quad \alpha(a) \text{ is a root of } f.$$

So  $\alpha(a) \in F$ , proving  $\alpha(F) \subset F$ .

Using the same argument for  $\alpha^{-1}$  we get  $\alpha^{-1}(F) \subset F$ . So  $F = \alpha(F)$ .

Proving  $F = \alpha(F)$ .

"(2)  $\Rightarrow$  (3)"

Say  $\alpha \in \text{Gal}(L/K)$ ,  $\langle \text{Gal}(L/F) \alpha^{\circ} \rangle = \text{Gal}(L/\alpha(F)) = \text{Gal}(L/F)$  by assumption.

Hence,  $\text{Gal}(L/F) \trianglelefteq \text{Gal}(L/K)$ .

"(3)  $\Rightarrow$  (1)"

Say  $\alpha \in \text{Gal}(L/K)$ .

Thus, for all  $\alpha \in \text{Gal}(L/K)$ ,  $\text{Gal}(L/F) = \alpha \text{Gal}(L/F) \alpha^{\circ} = \text{Gal}(L/\alpha(F))$ ,

By the fundamental theorem of Galois theory  $F = \alpha(F)$ .

Let  $f \in K[x]$  be irreducible with a zero in  $F$ ,  $a \in F$ .

As  $L/K$  normal,  $f$  splits over  $L$  into linear factors.

Let  $b \in L$ ,  $f(b) = 0$ .

Then  $f$  is the minimal polynomial of  $a$  and  $b$  over  $K$ .

We know there is a  $\varphi \in \text{Gal}(L/K)$  s.t.  $\varphi(a) = b$ .

Thus,  $b \in \alpha(F) = F$ .

Hence all roots of  $f$  in  $L$  are also in  $F$ , proving  $F$  normal. ■

Corollary: Let  $L/K$  Galois extension,  $F$  intermediate field s.t.  $F/K$  normal.

Then  $\text{Gal}(F/K) \cong \text{Gal}(L/K)/\text{Gal}(L/F)$

PF: Take  $\alpha \in \text{Gal}(F/K)$ , then  $\alpha(F) = F$ .

Thus,  $\alpha|_F : F \rightarrow F \in \text{Gal}(F/K)$

so the restriction map

$$\tau : \text{Gal}(L/K) \rightarrow \text{Gal}(F/K)$$

$$\alpha \mapsto \alpha|_F$$

is a group homomorphism with  $\ker \tau = \text{Gal}(L/F)$

thus  $\text{Im } \tau \cong \text{Gal}(F/K)/\text{Gal}(L/F)$ .

$$\text{But } |\text{Gal}(L/K)/\text{Gal}(L/F)| = \frac{[L:K]}{[L:F]} = [F:K] = |\text{Gal}(F/K)|$$

Hence,  $\tau$  is a bijection. ■

Example: Let  $f = x^4 + 7 \in \mathbb{Q}[x]$

If  $\alpha$  is a root of  $f$  over  $\mathbb{Q}[x]$

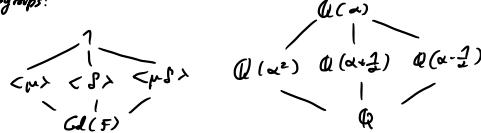
we have

$$f = (x - \alpha)(x + \alpha)(x - \frac{7}{\alpha})(x + \frac{7}{\alpha})$$

$$\text{Gal}(f) = \mathbb{Z}_2 \times \mathbb{Z}_2$$

Notice  $G(\mathbb{F}) \{ \text{id}, \delta: x \mapsto -x, \mu: x \mapsto \frac{1}{2}, \mu\delta: x \mapsto -\frac{1}{2}x \}$

Diagram of subgroups:



### Cubic polynomials

Formula:

$$\text{let } f = x^3 + a_2 x^2 + a_1 x + a_0 \in \mathbb{k}[x],$$

$$\text{Var. change } x \mapsto x - \frac{a_2}{3}$$

If  $\alpha$  is a zero of  $f(x - \frac{a_2}{3})$ ,  $\alpha + \frac{a_2}{3}$  is a zero of  $f$ .

Via this we can assume

$$f = x^3 + px + q$$

Try put  $x = u - v$ .

$$f(u-v) = u^3 - v^3 - (3uv-p)(u-v) + q$$

A sufficient cond. for  $f(u-v) = 0$  is

$$u^3 - v^3 + q = 0 \text{ and } 3uv - p = 0$$

$$\text{Second eq.: } v = \frac{p}{3u}$$

$$\Rightarrow 3^3 u^6 - p^3 + 3^3 u^3 q = 0$$

Using  $y = u^3$

$$y^2 - qy - \left(\frac{p}{3}\right)^3 = 0$$

$$\Rightarrow y = -\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3}$$

$$u = \sqrt[3]{y}$$

$$u^3 - v^3 + q = 0 \Rightarrow v = \sqrt[3]{y + q}$$

$$\text{Since } x = u + v \\ x = u - v = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3}} - \sqrt[3]{\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3}}$$

Cardano's formula.

### Solvability by radicals

For the rest of this section, let  $\mathbb{k}$  be a field of characteristic 0.

Def: A field extension  $\mathbb{k}/\mathbb{k}$  is called a radical extension if there is a chain

$$\mathbb{k} = L_0 \subset L_1 \subset \dots \subset L_n = \mathbb{k}$$

s.t.  $L_{i+1} = L(b_i)$  for all  $i$  with  $b_i$  a zero of  $x^n - a_i$  for some  $a_i \in L_i$ .

A polynomial  $f \in \mathbb{k}[x]$  is called solvable by radicals if there is a radical extension  $\mathbb{k}/\mathbb{k}$  that (is also Galois) s.t.  $f$  splits over  $\mathbb{k}$  into linear factors.

Prop: the condition that  $\mathbb{k}/\mathbb{k}$  is Galois can be removed. If there is a radical extension s.t.  $f$  splits over it, then there is a radical Galois extension with prov. ext. as intermediate.

Def: A group  $G$  is solvable if there is a chain of subgroups

$$G = G_0 \supset G_1 \supset \dots \supset G_m = \{1\}$$

s.t. for all  $i$   $G_{i+1}$  is a normal subgroup of  $G_i$ , and  $G_i/G_{i+1}$  is abelian.

Example:  $S_3$  is solvable

$$\langle (1, 2, 3) \rangle \cong S_3, \quad S_3 / \langle (1, 2, 3) \rangle \cong \mathbb{Z}_2$$

Def: Let  $G$  be a group,  $a, b \in G$ . The commutator of  $a, b$  is  $[a, b] = a^{-1}b^{-1}ab$ . Notice  $[a, b] = 1 \Leftrightarrow ab = ba$ .

The commutator subgroup  $G'$  of  $G$  is the subgroup generated by all  $[a, b] \mid a, b \in G$ .

$G$  abelian  $\Leftrightarrow G' = 1$ .

Lemma: (1)  $G'$  is a normal subgroup of  $G$   
(2)  $G/G'$  is abelian  
(3) If  $H$  is a normal subgroup of  $G$  s.t.  $G/H$  is abelian, then  $H \geq G'$ .

Pf: (1)  $[a, b]^{-1} = [b, a]$

Hence, the elements of  $G'$  are elements of commutators

$$(g^{-1}[a, b]g = g^{-1}a^{-1}b^{-1}abg = g^{-1}a^{-1}gg^{-1}b^{-1}gg^{-1}agg^{-1}bg = [g^{-1}ag, g^{-1}bg]) \text{ (as } g \in G)$$

Let  $h = [a_1, b_1] \dots [a_n, b_n] \in G'$ ,  $g \in G$ .

$$\text{By } (*) \quad g^{-1}hg = g^{-1}[a_1, b_1]g \dots g^{-1}[a_n, b_n]g$$

$$= [g^{-1}a_1g, g^{-1}b_1g] \dots [g^{-1}a_ng, g^{-1}b_ng] \in G'$$

Hence,  $G'$  normal.

(2) Take,  $a, b \in G$ ,

$$aG' \cdot bG' = abG' = ba[a, b]G' = baG' = bG'aG'$$

Hence,  $G/G'$  is abelian.

$$(3) \quad aH \cdot bH = bH \cdot aH$$

$$\Leftrightarrow abH = baH$$

$$abH = ba[a, b]H$$

Thus,  $baH = ba[a, b]H$ , so  $[a, b] \in H$

Thus,  $H \geq G'$ .  $\blacksquare$

Def:  $G$  group,  $G^{(0)} = G$

$G^{(n)} := G'$ , inductively  $G^{(n+1)} = (G^{(n)})'$

Lemma:  $G$  is solvable  $\Leftrightarrow \exists m \geq 0$  s.t.  $G^{(m)} = \{1\}$

Pf: " $\Leftarrow$ " Sps.  $G = \{1\}$

We have a chain of subgroups

$$G = G^{(0)} \supset G^{(1)} \supset \dots \supset G^{(n)} = \{1\}$$

and for all  $i$ ,  $G^{(i)}$  is normal and  $G^{(i)}/G^{(i+1)}$  is abelian.

Hence  $G$  is solvable.

" $\Rightarrow$ "

Sps.  $G$  is solvable. Then we have a chain

$$G = H_0 \supset H_1 \supset \dots \supset H_m = \{1\}$$

s.t.  $H_i$  is normal and  $H_i/H_{i+1}$  abelian

Since  $H_{i+1}/H_i$  abelian,  $H_i \supset H_{i+1}$ . Thus  $H_i \supset G_i$ ,  $H_2 \supset H_1 = G^{(2)}$

Inductively  $H \supset H_{i+1} = (G^{(i+1)})' \supset G^{(i)}$ . Hence  $\{1\} = H \supset G^{(m)}$ , so  $G^{(m)} = \{1\}$ .  $\blacksquare$

Corollary: Let  $G$  be a solvable group, and  $\gamma: G \rightarrow H$  be a surjective group homomorphism. Then  $H$  is solvable.

Pf:  $a, b \in G$ ,  $\gamma([a, b]) = [\gamma(a), \gamma(b)]$

thus,  $H' = \gamma(G')$  extending to higher commutators

$$H^{(n)} = \gamma(G^{(n)}) \text{ for all } i$$

If  $G$  is solvable we have in s.t.  $G^{(m)} = \{1\}$

$$H^{(m)} = \gamma(G^{(m)}) = \gamma(\{1\}) = \{1\}$$

$\blacksquare$

Def: Let  $m \in \mathbb{Z}_{\geq 0}$ . Let  $L$  field.

An element  $\zeta \in L$  is called an  $m$ -root of unity if  $\zeta^m = 1$

And is called a primitive  $m$ -root of unity if  $\zeta^m = 1$  and  $\zeta^i \neq 1$  for all  $0 < i < m$

e.g.  $e^{2\pi i/m}$  is a primitive  $m$ -root of unity in  $\mathbb{C}$ .

Lemma: Let  $m \in \mathbb{Z}_{\geq 0}$ ,  $K$  be a field of char. 0

let  $\zeta$  be a primitive  $m$ -root of unity in an extension field of  $K$ .

then  $K(\zeta)$  is a Galois extension with abelian Galois group.

Pf: Over  $K(\zeta)$  the polynomial  $x^m - 1$  splits

Take  $\{\zeta^r | 0 \leq r \leq m-1\}$  are zeros of  $x^m - 1$

Consider  $\zeta^i = \zeta^j$ ,  $0 \leq i, j \leq m-1$ . Then  $\zeta^{j-i} = 1$ . Thus  $j-i = 0$ , proving all roots are distinct.

Thus  $K(\zeta)$  is the splitting field of  $x^m - 1$ . So  $K(\zeta)/K$  is a Galois extension.

Let  $G = \text{Gal}(\mathbb{K}(x)/\mathbb{K})$

If  $\sigma \in G$ ,  $\sigma(\tau)$  is a zero of  $x^n - 1$

Thus  $\sigma(\tau) = \tau^j$  for some  $j \in \{0, \dots, n-1\}$

$G$  is a subgroup of permutations of  $\{1, 2, \dots, \tau^{n-1}\}$

Hence for  $\sigma, \tau \in G$  we have

$$\sigma(\tau) = \tau^j \text{ and } \sigma = \tau.$$

Let  $\sigma, \tau \in G$ , then

$$\sigma(\tau) = \tau^i, \tau(\tau) = \tau^j$$

$$\sigma \circ \tau(\tau) = \sigma(\tau^j) = \tau^{ij}$$

$$\tau \circ \sigma(\tau) = \tau(\tau^i) = \tau^{ij}$$

Showing  $G$  abelian.  $\blacksquare$

Theorem: Let  $n \in \mathbb{Z}_{>0}$ , let  $\mathbb{K}$  be a field that contains a primitive  $n^{\text{th}}$ -root of unity.

Let  $a \in \mathbb{K} \setminus \{0\}$  and  $L$  the splitting field of  $x^n - a$  over  $\mathbb{K}$ .

First,  $L = \mathbb{K}(\alpha)$  where  $\alpha$  is any root of  $x^n - a$

And,  $\text{Gal}(L/\mathbb{K})$  is abelian.

Pf: (1) Take a root  $\alpha$  of  $x^n - a$  in  $L$ .

Let  $\zeta$  be the  $n^{\text{th}}$  root of unity

then  $\alpha, \zeta \alpha, \dots, \zeta^{n-1} \alpha$  are zeros of  $x^n - a$  in  $\mathbb{K}(\alpha)$ .

Sps.  $\zeta^i \alpha = \zeta^j \alpha$  for  $0 \leq i, j < n$

Then  $\zeta^i = \zeta^j$  giving  $i = j$ . Hence all such roots are distinct and  $\mathbb{K}(\alpha) = L$ .

(2) For  $\sigma, \tau \in \text{Gal}(\mathbb{K}(\alpha)/\mathbb{K})$

Then  $\sigma(\zeta^i \alpha) = \zeta^i \sigma(\alpha)$ , sinn for  $\tau$

Thus elements in  $\text{Gal}(\mathbb{K}(\alpha)/\mathbb{K})$  are determined by  $\sigma(\alpha)$

and  $\sigma(\alpha) = \zeta^i \alpha$  for some  $i$

$$\tau(\alpha) = \zeta^s \alpha \text{ for } s$$

$$\sigma \circ \tau(\alpha) = \sigma(\zeta^s \alpha) = \zeta^{is} \alpha = \tau(\zeta^i \alpha) = \tau(\sigma(\alpha)).$$

$\blacksquare$

Theorem (Galois):

Let  $\mathbb{K}$  be a field of characteristic 0,  $f \in \mathbb{K}[x]$ .

$f$  is solvable by radicals  $\Leftrightarrow \text{Gal}(f) \text{ is solvable}$ .

Pf: " $\Rightarrow$ "

Let  $L$  be the splitting field of  $f$  over  $\mathbb{K}$ . So  $\text{Gal}(f) = \text{Gal}(L/\mathbb{K})$

Since  $f$  is solvable by radicals there exists a sequence

$$\mathbb{K} = \mathbb{K}_1 \subset \mathbb{K}_2 = \mathbb{K}_1(\alpha_2) \subset \dots \subset \mathbb{K}_m = \mathbb{K}_m(\alpha_m)$$

s.t. for all  $i$  there exists  $a_i \in \mathbb{K}_i$  and  $r_i \in \mathbb{Z}_{\geq 0}$  s.t.  $\alpha_i = a_i^{r_i}$

in a way that  $f$  splits over linear factor over  $\mathbb{K}_m$

Moreover, we can assume  $\mathbb{K}_m/\mathbb{K}$  is Galois.

We have  $L \subset \mathbb{K}_m$ . Let  $m$  be the smallest common multiple of all  $r_i$

let  $\zeta$  be a primitive  $m^{\text{th}}$ -root of unity in some extension of  $\mathbb{K}$ .

Let  $F = \mathbb{K}(\zeta)$ , note  $\zeta^{m/i}$  is a primitive  $r_i^{\text{th}}$ -root of unity

thus,  $F$  contains primitive  $r_i^{\text{th}}$  roots of unity for all  $i = 1, \dots, m$

Put  $F_0 = \mathbb{K}, F_1 = F, F_i = F_{i-1}(\alpha_i)$  for  $i \geq 2$ .

thus we have a new chain

$$\mathbb{K} = F_0 \subset F_1 = F \subset F_2 \subset \dots \subset F_m$$

As  $F_i = F_{i-1}(\alpha_i)$ ,  $\alpha_i^{r_i} = a_i \in F_{i-1}$ . Thus, by prov. theorem,  $F_i/F_{i-1}$  is Galois and  $\text{Gal}(F_i/F_{i-1})$  is abelian.  
Furthermore,  $L \subset F_m$

Since  $\mathbb{K}_m/\mathbb{K}$  is Galois,  $\mathbb{K}_m$  is the splitting field of  $g \in \mathbb{K}[x]$

And, thus,  $F_m$  is the splitting field of  $g(x^{m-1})$  over  $\mathbb{K}$

Thus,  $F_m/\mathbb{K}$  is a Galois extension. Showing  $F_m/F_i$  is a Galois extension for all  $i = 0, \dots, m$ .

$F_2$  and all  $F_i$  contains all  $r_i^{\text{th}}$ -roots of unity.

thus  $F_i/F_{i-1} = F_i(\alpha_i)/F_{i-1}$  is a Galois extension and  $\text{Gal}(F_i/F_{i-1})$  is abelian.

We also have  $F_i/F_0$  is also Galois with abelian Galois group.

By second part of the fundamental theorem of Galois theory it follows that

$\text{Gal}(F_n/F_0)$  is a normal subgroup  $\text{Gal}(F_n/F_{n-1})$  and  $\text{Gal}(F_n/F_{n-1})/\text{Gal}(F_n/F_0) = \text{Gal}(F_0/F_{n-1})$

Since the latter is abelian we get that

$$\text{Gal}(F_n/F_0) \supset \text{Gal}(F_n/F_1) \supset \dots \supset \text{Gal}(F_n/F_{n-1}) \supset \text{Gal}(F_n/F_n) = \{1\}$$

is a chain that shows  $\text{Gal}(F_n/F_0)$  is solvable.

We have that  $L \subset F_n$ , and thus  $\text{Gal}(L/F_0) = \text{Gal}(F_n/F_0)/\text{Gal}(F_n/L)$

Thus there is a surjective homomorphism  $\text{Gal}(F_n/F_0) \rightarrow \text{Gal}(L/F_0)$

Hence also  $\text{Gal}(L/F_0)$  is solvable. ■

Theorem:  $S_n$  is solvable  $\Leftrightarrow n \leq 4$

Theorem: Let  $p$  be a prime number and let  $f \in \mathbb{Q}[x]$  irreducible s.t.  $f$  has  $p-2$  zeros in  $\mathbb{R}$

then  $\text{Gal}(f)$  is  $S_p$ . Hence such a polynomial with  $p \geq 5$  is not solvable by radicals.

Example:  $f = 2x^5 - 10x + 5$  has 3 real roots

Hence this polynomial is not solvable by radicals.