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.

Conjugation $G \times \{\text{subgroups of } G\} \longrightarrow \{\text{subgroups of } G\}$

$$(g, H) \longmapsto gHg^{-1}$$

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 $N(H)$
Thus, $|H| \mid |N(H)| \mid |G|$

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

$$(c = \#\{ gHg^{-1} : g \in H \})$$

By the orbit stabilizer theorem

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

The Sylow theorems

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

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

We know: if H subgroup of G
then, $|H|$ devides $|G|$

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

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

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

This is a group under

$$\cdot : (H \times K) \times (H \times K) \to H \times K$$
$$(h_1, k_1)(h_2, k_2) \mapsto (h_1 h_2, k_1 k_2)$$

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

Theorem: Let G group. H, K subgroups of G.
Spse.
(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 $\varphi : H \times K \to G$
$(h,k) \mapsto hk$
w.t.s. φ isomorphism.
By (1) φ is surjective.
To show φ homomorphism:
Let $h \in H$, $k \in K$
$h^{-1}k^{-1}hk = h^{-1}(\underbrace{k^{-1}hk}_{\in H}) \in H$
(H normal)

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. φ is homomorphism.

To show φ injective we show $\ker \varphi = \{(1,1)\}$
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 $h^{-1} = 1$ so $h = 1$. ∎

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 $m, n \in \mathbb{Z}_{>0}$ relatively prime.

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

Pf: $[n]$ has order m in $\mathbb{Z}/mn\mathbb{Z}$
$[m]$ " " n " "
$\mathbb{Z}/mn\mathbb{Z}$ has subgroups of order n or m and their intersection is $\{[0]\}$. Also normal b/c $\mathbb{Z}/mn\mathbb{Z}$ 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 $H' \neq G$.
If $H' \neq G \Rightarrow |H'| = p$
$H \cap H'$ 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_n is a group of order $2n$, generated by a, b
$a^n = 1$, $b^2 = 1$, $bab = a^{-1}$)

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
$$bab = bab^{-1} = a^i \quad \text{for some } i.$$
$$a = b^2ab^2 = b(bab)b = ba^ib = (bab)^i = (a^i)^i = a^{i^2}$$
$\Rightarrow a^{i^2-1} = 1$, a has order p
$\Rightarrow p \mid i^2 - 1 = (i+1)(i-1) \Rightarrow p \mid i+1$ or $p \mid i-1$

If $p \mid i-1 \Rightarrow a^{i-1} = 1 \Rightarrow a^i = a$
$\Rightarrow bab^{-1} = a \Rightarrow ba = ab$ a and b 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
$$G = \langle a \rangle \times \langle b \rangle \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/2p\mathbb{Z}.$$

If $p \mid i+1 \Rightarrow a^{i+1} = 1$ i.e. $a^i = a^{-1}$
$\Rightarrow bab = a^{-1}$, $a^p = 1$, $b^2 = 1$
and $|G| = 2p$ and $G = \langle a, b \rangle$
So $G \cong D_p$. ∎

Second Sylow theorem

Let K be a subgroup of G s.t. $p \mid |K|$. 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 pSylow 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

Say G is a finite group, $|G| = p^m r$, $p \nmid r$. Let s be number of p-Sylow subgroups.
Then, s divides r and $s \equiv 1 \bmod p$.

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, $N_p \equiv 1 \bmod p$ 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.

$N_q \equiv 1 \bmod q$ and $N_q \mid p$

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

If $N_q = p$, then $p \equiv 1 \bmod q$. 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

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

■

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 $N = \binom{n}{p^m} = \frac{n(n-1)\cdots(n+p^m+1)}{p^m(p^m-1)\cdots(p^m-r)\cdots 1}$

Furthermore, $p \nmid N$.

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

To show $p \nmid N$.

Notice, whenever $p^l \mid (n-k)$ then also $p^l \mid p^m - k$ 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

$$N = |S| = \sum_{\text{orbits } \mathcal{O}} |\mathcal{O}|$$

We know $p \nmid N$. Hence there is an orbit $\mathcal{O} = G(M)$ 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,

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

Since $p \nmid |G(M)|$, 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 $S = G/H$ set of left cosets.

G acts transitively on G/H by left multiplication.

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

The stabilizer of $1 \cdot H = H$ is H.

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

Restrict this action to K.

$K \times G/H \longrightarrow G/H$

$k \cdot aH \longmapsto kaH$

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

As H is p-Sylow subgroup. $|G/H|$ is prime to p. Since $|G| = p^n r$, $|H| = p^n$, 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 $H' = aHa^{-1}$. Then H' is G_{aH} 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 $|K| = p^s \cdot \ell$

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

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

By corollary of 2nd 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 $N(H)$ normalizer.

$$S = |C(H)| = [G : N(H)]$$

by orbit stabilizer theorem.

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

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

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

Now $s \equiv 1 \bmod p$.

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

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

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

The orbit of H_i consists only of H_i $\Leftrightarrow H \subset N(H_i)$

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

$|N(H_i)|$ divides $|G| = p^n \cdot r$

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

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

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 $|H(H_i)|$ is a divisor of the number of elements of $|H| = p^n$ (and $|G(H_i)| \neq 1$)

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

Hence, $s \equiv 1 \bmod p$. ∎

Lecture 9

RING

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

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

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 call a unit element if $\forall a \in R \; 1 \cdot a = a \cdot 1 = a$.

Prop. If exist 1 is unique.

Pf: Spc. $x, y \in R$ unit elements.
Notice $x \cdot y = x = y$ ∎

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 1,
$(-1)a = a(-1) = -a$

Pf: (1) $a \cdot 0 = a \cdot (0+0) = a \cdot 0 + a \cdot 0$
$\Rightarrow a \cdot 0 = 0$
Similarly for $0 \cdot a$.

(2) $(-a) \cdot b + ab = (-a+a) \cdot b = 0 \cdot b = 0$
$\Rightarrow (-a) \cdot b = -(ab)$
Similarly for $a \cdot (-b)$.

(3) $(-a)(-b) - ab = (-a)(-b) + (-a) \cdot b = (-a) \cdot (-b+b) = (-a) \cdot 0 = 0$
$\Rightarrow (-a)(-b) = -(-ab) = ab$,
↑ uniqueness of inverses in a group.

(4) $(-1) \cdot a = -(1 \cdot a) = -a$ ∎

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. $a \cdot b = 0$.
A commutative ring with 1 an no zero divisor is called an integral domain.

Prop. (cancellation property)
Let be an integral domain. If $a,b,c \in R$, $a \neq 0$ s.t.

$$ab = ac$$

then

$$b = c$$

Pf: $ab = ac \Rightarrow a \cdot (b-c) = 0$, $a \neq 0 \Rightarrow b - c = 0 \Rightarrow b = c$ ∎

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 $p \nmid m \cdot n$, hence $m \cdot n \neq 0$ 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

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

Two polynomials

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

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

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

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

We denote $R[x]$ the set of polynomials in x with coefficients in R.

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

via this we say $R \subset R[x]$

We define a ring structure on $R[x]$

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

we define
$$f + g = \sum_{i=0}^{n} (a_i + b_i) x^i$$

and
$$f \cdot g = \sum_{r=0}^{2n} \left(\sum_{i+j=r} a_i b_j \right) x^r$$

- $0 \in R$ is the neutral element for addition in $R[x]$.
- If $1 \in R$ is the unit, 1 is also the unit in $R[x]$.
- R is a subring of $R[x]$.

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

Prop. Let R be an integral domain,

(1) $f, g \in R \setminus \{0\}$
$f \cdot g \neq 0$ and $\partial(f \cdot g) = \partial f + \partial g$

(2) $R[x]$ is an integral domain

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

Let $f = \sum_{i=0}^{n} a_i x^i$, $a_n \neq 0$, $g = \sum_{i=0}^{m} b_i x^i$, $b_m \neq 0$.

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

Notice $c_{n+m} = a_n \cdot b_m \neq 0$

Thus, $f \cdot g \neq 0$, $\partial(f \cdot g) = \partial f + \partial g$. ∎

Prop. Let R be an integral domain, then $U(R) = U(R[x])$.

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

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

$$f \cdot g = 1$$

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

Thus, $f, g \in R$ and $f \in U(R)$. ∎

Lecture 10

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

Prop: Every finite integral domain is a field.

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

$a \cdot (b + c) = a \cdot b + a \cdot c$, for all $b, c \in R$.

i.e. $a \cdot : R \to R$
$b \mapsto a \cdot b$
is a group homomorphism $(R, +) \to (R, +)$

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

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

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

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

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

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

$$\varphi(a+b) = \varphi(a) + \varphi(b)$$
$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$$

A bijective homomorphism $\varphi: A \to B$ is called an isomorphism.
And a isomorphism $\varphi: A \to A$ is called an automorphism.

Remarks: Since a ring homomorphism $\varphi: A \to B$ is also a group homomorphism $\varphi: (A, +) \to (B, +)$ we have
φ injective $\iff \ker f = \{0\}$

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

Def: Let A be a ring, A subset $I \subset A$ is an <u>ideal</u> 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 $\varphi: A \to B$ be a ring homomorphism, 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.

Pf: As I is a subgroup of $(B, +)$ and φ 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 $\varphi(a) \cdot \varphi(x) \in I$.
So, $\varphi(ax) \in \varphi^{-1}(I)$. ∎

Lemma: Let $\varphi: A \to B$ 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 $\ker \varphi$

Pf: We define the inverse map

$$\{\text{ideals of } A \text{ which contains } \ker\varphi\} \longrightarrow \{\text{ideals of } B\}$$
$$J \longmapsto \varphi(J)$$

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 $\varphi^{-1}(\varphi(J)) \supset J$
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 φ 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

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

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 $u \in U(R)$.

Pf: "$\Rightarrow$" Sps. $\langle a \rangle = \langle b \rangle$, then $b = ua$ for some $u \in R$.
also $a = wb$ for some $w \in R$.
Hence $b = awb$, so $aw = 1$ 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 $b = u^{-1}a$. 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 K be a field, $\varphi: K \to R$ be a ring homomorphism to a ring R. Then, $\varphi \equiv 0$ or φ is injective.

Pf: (1) Let $a \in I \cap U(R)$. $a^{-1} \in R$, hence $1 = a^{-1}a \in I$. Then if $x \in R$ $x = x \cdot 1 \in I$. So $R = I$.

(2) Use $U(K) = K \setminus \{0\}$. Hence either only $0 \in I$ or $I = R$.

(3) $\ker \varphi$ is an ideal of K. By (2) $\ker \varphi = \{0\}$ and φ is injective or $\ker \varphi = R$ 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

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

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

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

Pf: By normality of I as a subgroup, the well-definess of addition is given.

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

To show the product is well-defined.

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

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

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

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

and the product is well-defined.

Associativity and distributivity are inherent 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 $x, y \in R$:

$$\pi(xy) = [x \cdot y] = [x] \cdot [y] = \pi(x) \cdot \pi(y).$$

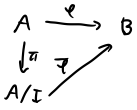
Hence π is a ring homomorphism. ∎

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

Theorem (Universal property):

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

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



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

Pf:

$\varphi = \overline{\varphi} \circ \pi$ means $\overline{\varphi}([x]) = \varphi(x)$

Hence, if $\overline{\varphi}$ exists it is unique. To prove $\overline{\varphi}$ exists we show $\overline{\varphi}([x]) = \varphi(x)$ 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 $\overline{\varphi}([x]) = \overline{\varphi}([y])$.

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

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

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

Theorem (Homomorphism theorem)

If $\varphi: A \to B$ is surjective a ring homomorphism w/ $\ker \varphi = I$.
Then the map $\bar{\varphi}: A/I \to B$ 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. $M \subset I \subset R$.

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

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

Hence, $[a][b] = [a \cdot b] = 0 \iff ab \in P$
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 prev. 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 $a \in R \setminus \{0\}$, we wish to show $\exists\, b \in R/M$ s.t. $ab = 1$
$\langle a \rangle$ is an ideal, and $\langle a \rangle \neq \{0\}$.
Thus, $\langle a \rangle = R/M$, in particular $1 \in \langle b \rangle$. Proven 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 an 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 $a \mid b$ 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,

$$a \mid b \iff b \in \langle a \rangle$$
$$a \mid b,\ b \mid c \Rightarrow a \mid c$$
$$a \mid b,\ a \mid c \Rightarrow a \mid (b + c)$$

Theorem:

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

$$f = gq + r$$

PF: If $\partial f < \partial g$ we're done, $q = 0$, $r = f$.
If $\partial f \geq \partial g$ proceed by induction on $m := \partial f$.
Let a, b the leading coefficient of f, g resp.
Let $\overline{f} = f - \frac{a}{b} x^{m - \partial g} \cdot g$, since $m \geq \partial g$ we have $\frac{a}{b} x^{m - \partial g} \cdot g \in K[x]$ and has degree at most ∂g.
Also, $\partial f = m$ implying $\partial \overline{f} \leq m$.
The coeff. of x^m in $\overline{f}$ is $a - \frac{a}{b} \cdot b = 0$. Thus, $\partial \overline{f} < m$.

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

Put $r := r'$

$q := q' + \frac{a}{b} x^{m-\partial g}$

Notice $qg + r = q'g + r + \frac{a}{b} x^{m-\partial g} \cdot g$

$= \bar{f} + \frac{a}{b} x^{m-\partial g} \cdot g = f$

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

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

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

Then

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

$$\Rightarrow (q - q')\cdot g = r' - r$$

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:

$$\begin{array}{l|l} (x^3 + 4x^2 + x + 1) & x+2 \\ \quad x^3 + 2x^2 & \hline \\ \quad\quad 2x^2 + x + 1 & x^2 + 2x - 3 \\ \quad\quad 2x^2 + 4x & \\ \quad\quad\quad -3x + 1 & \\ \quad\quad\quad -3x - 6 & \\ \quad\quad\quad\quad 7 & \end{array}$$

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

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 $r \mid a_i$ 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: $s \mid r$.

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

Pf: Let $r, s \in R$ be the gcd of $a_1, \dots, a_n \in R$. Then $r \mid s$ and $s \mid r$, hence $r = u s$, for $u \in \mathcal{U}(R)$. ∎

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

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

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

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

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

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

Pf: We have $r_m \mid r_{m-1}$. Also

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

Thus $r_m \mid r_{m-2}$

Inductively, $r_m \mid r_{i+1}$ and $r_m \mid r_i$ which implies $r_m \mid r_{i-1}$ for all $i = 1, \dots, n$.
In particular $r_m \mid r_0 = f$, $r_m \mid r_1 = g$. So r_m is a common divisor.

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

$s \mid f = r_0$, $s \mid g = r_1$

Since $r_0 = q_1 r_1 + r_2$

it follows $s \mid r_2$.

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

and $s \mid r_{i-1}$, $s \mid r_i$, hence $s \mid r_{i+1}$.

Thus, $s \mid r_m$. ∎

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

Pf:
Let l be the gcd of f,g as computed by the Euclidean algo. in $K[x]$.
As l is computed by repeated division with rest it follows $l \in k[x]$.
Let h be a gcd of f,g.
Then, $h = a \cdot l$, $a \in K \setminus \{0\}$.
Let h_n, l_n be the leading coeffs. of h, l resp.
Notice $h_n = a \cdot l_n$. If $h_n \in k$, we have $a \in k$. Thus $h = a \cdot l \in k[x]$. ∎

Def: Let $f = \sum_{i=1}^{n} a_i x^i \in K[x]$. Let R be a ring that contains K subring.
For $s \in R$ let
$$f(s) = \sum_{i=1}^{n} a_i s^i \in R.$$

Obs: $(f+g)(s) = f(s) + g(s)$
$(f \cdot g)(s) = f(s) \cdot g(s)$
Hence this evaluation at s
$$\text{eval}_s : K[x] \longrightarrow R$$
$$f \longmapsto f(s)$$
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 $f = (x-a)g$, $g \in K[x]$
So, $f(a) = (a-a) \cdot g = 0$.
"$\Rightarrow$" Sps. $f(a) = 0$.
Compute f divide by $(x-a)$.
$$f = (x-a) \cdot q + r, \quad q, r \in K[x], \ \partial r < \partial (x-a) = 1$$
Since $0 = f(a) = (a-a) \cdot q + r = r$. Hence $r = 0$.
And $(x-a) \mid f$. ∎

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

Pf: If $\partial f = 0$, 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. $\partial f = n+1$.
If f has no zeros we're done.
Sps. $a \in K$ is a zero of f.
Then, $f = (x-a) \cdot g$, $g \in K[x]$, $\partial g = \partial f - 1 = n$
Notice g has at most n zeros.
If b is a zero of f
$$0 = f(b) = (b-a)\, g(b)$$
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

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

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

(2) If $b \in R\setminus(\{0\} \cup U(R))$, $a \in R\setminus\{0\}$ we have $\|ab\| \geq \|a\|$

e.x.:

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

(2) $(R[x], \|x\| = \partial x)$

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

is an ED with $\|n+mi\| = n^2 + m^2$

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

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

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

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

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

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

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

Let $r := z - (n+im)w$. Notice

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

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

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

Def: An ID R is called a principal ideal domain (PID) if every ideal of R is principal.

i.e. $\forall I \subset R$ ideal: $\exists a \in R$ s.t. $I = \langle a \rangle = \{x \cdot a \mid x \in R\}$.

Theorem: Every ED is a PID.

Pf: If $I = \{0\}$, then $I = \langle 0 \rangle$.

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:

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

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

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

Hence $I = \langle a \rangle$. ∎

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. ∎

Irreducibility of Polynomials

Def: Let R be an ID.
An element $q \in R \setminus \{0\}$ is called <u>irreducible</u> if $q \notin U(R)$ and if

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

Then $a \in U(R)$ or $b \in U(R)$.
Otherwise (if $\exists a, b \in R \setminus U(R)$ s.t. $q = ab$) q 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 $ax + b = f \cdot g$, $f, g \in k[x]$, $0 = \partial(ax+b) = \partial f + \partial g$, so $\partial f = 0$ or $\partial g = 0$.
Thus, $f \in U(k[x])$ or $g \in U(k[x])$.

Prop: Let R be a PID, $p \in R$ irreducible element.
Then $\langle p \rangle$ 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 PID, $I = \langle a \rangle$, $a \in R$.
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 $k[x] \xrightarrow{\pi} k[x]/\langle p \rangle$ 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: Proof. Suppose $f \cdot g$ not primitive. Write

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

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_i, a_i.
Let i be minimal s.t. p does not divide a_i
j " " s.t. p does " " b_j.
Let c_{i+j} be the coeffs of x^{i+j} in $f \cdot g$.
Then

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

Since $i + j - k < j$ $(k > i)$, $p \mid b_{i+j-k}$
and $p \mid a_k$ $(k < i)$
Hence,

$$p \mid c_{i+j} - a_i b_j$$

But $p \nmid a_i b_j$
And $p \nmid c_{ij}$. ↯ ∎

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, "$\Leftarrow$" is proven.

"$\Rightarrow$" Sps $f = gh$, $g, h \in \mathbb{Q}[x]$ 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 new coeffs.

So

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

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

Also

$$bf = ag'h'$$

Both f, $g'h'$ are primitive

gcd of coeffs of bf is b, and the gcd of $ag'h'$ is a.

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

So $f = g'h'$ 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.

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

but $p^2 \nmid a_0$.

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

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

Let

$$f = \sum_{i=0}^{k} b_i x^i, \quad g = \sum_{i=0}^{\ell} c_i x^i \qquad k, \ell \neq 0,$$

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. sps. $p \mid b_0$ and $p \nmid c_0$.

Notice $n = r + \ell$, $a_n = b_r \cdot c_\ell$

Since $p \nmid a_n$, $p \nmid b_k$.

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

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

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

By our choice of j

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

Thus, $p \nmid a_j$. 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 $\partial g = 1$ or $\partial h = 1$ 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 $a \in \mathbb{Q}$ is a zero of f. Then $a \in \mathbb{Z}$, $a \mid a_0$ in $\mathbb{Z}$.

Thus, if $f \in \mathbb{Z}[x]$ is monic, $\partial f \geq 3$, 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 $k[x] \iff f(x+a)$ is irreducible over k

Indeed: $\sigma_a : k[x] \to k[x]$

$g \mapsto g(x+a)$

is clearly an isomorphism (with inverse σ_{-a})

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

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

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

Notice

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

$x \cdot \sigma_1(f) = (x+1)^p - 1$

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 $\varphi : K \to L$ 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 $\cdot : k \times L \to L$.

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

dist. laws: $(a+b) \cdot x = a \cdot x + b \cdot x$

$a \cdot (x+y) = a \cdot x + a \cdot y$

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

ident. $x = 1 \cdot x$

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 s.t. $L \subset K$. 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 conv. $\infty = \infty \cdot \infty = n \cdot \infty = \infty \cdot n$, for $n \in \mathbb{Z}_{>0}$)

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

So sps both finite.

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

Let $x_1, \ldots, x_n$ basis of L/k, $y_1, \ldots, y_m$ basis of K/L

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

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

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

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

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

Again, x_i linearly independent over k, so

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

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 $a \in K$ is called algebraic over k, if there is some not-null polynomial

$$f = \sum_{i=1}^{n} b_i x^i \in k[x]$$

with $f(a) = 0$, i.e. $0 = \sum_{i=1}^{n} b_i a^i \in K$.

Otherwise, a is called transcendental.

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

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

i " " " " " " " " $x^2 + 1$

π 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 $a \in K$ be algebraic over k, then $k(a)$ 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 $a \in E$ algebraic over k.

Let $ev_a : k[x] \to E$

$$f \mapsto f(a)$$

As a is algebraic, the kernel of f is not $\{0\}$.

As $k[x]$ is PID, $\ker(ev_a)$ is principal, so there is a unique monic polynomial f_a s.t.

$$\ker(ev_a) = \langle f_a \rangle$$

This polynomial is called the minimal polynomial of a over k

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

Pf: Let f_a be the min. poly. of a over k.

Spc. $f_a = gh$, $g, h \in E[x]$.

$f_a(a) = 0$, hence

$$g(a)h(a) = 0$$

Wlg. spc. $g(a) = 0$. Have $g \in \ker(ev_a)$, and so $g = l \cdot f_a$ for $l \in k[x]$.

$$f_a = l \cdot f_a \cdot h \Rightarrow l \cdot h = 1$$
$$\Rightarrow h \in U(k[x]) = U[k] \subset k$$

Hence f_a irreducible.

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

$g \in \ker(ev_a) = \langle f_a \rangle$. Hence $g = l f_a$, $l \in k[x]$. By the irreducibility of g, $l \in U(k)$. Since g monic, $l = 1$.

Thus, $g = f_a$. ∎

e.g. Let p be a prime number, $n \in \mathbb{Z}_{>0}$

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

Theorem (description of the simple algebraic extensions)

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

Then,

(1) $\mathbb{K}(a) \cong \mathbb{K}[x]/\langle f_a \rangle$

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

Pf:

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

$g \longmapsto g(a)$

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.

$$L \cong \mathbb{K}[x]/\langle f_a \rangle.$$

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, $ev_a : \mathbb{K}[x] \to \mathbb{K}(a)$ 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 $\partial g \geq m$, we have

$$g = q \cdot f_a + r \quad , \quad q, r \in \mathbb{K}[x], \ \partial r < m.$$

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 $b \in \langle 1, \cdots, a^{m-1} \rangle$.

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

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

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

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

But $\partial g < \partial f_a$. Hence $g = 0$, so $b_i = 0$ for $i = 0, \cdots, m-1$. Proving $1, \cdots, a^{m-1}$ 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.x.: $\mathbb{C} = \mathbb{R}(i)$, 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 $a_1, \cdots, a_m \in L$ s.t. $L = \mathbb{K}(a_1, \cdots, a_m)$

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

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

So, there are $b_0, \cdots, b_m \in \mathbb{K}$ 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 $a_1, \cdots, a_m$ be a basis for L over $\mathbb{K}$. Then,

$$\mathbb{K}(a_1, \cdots, a_m) = L.$$

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

Sps. $L = \mathbb{K}(a_1, \cdots, a_{m+1})$

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

We know a_{m+1} alg. over $\mathbb{K}$ and, thus, over L'.

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

Extensions of field homomorphism.

Fix K/k field extension

Def: Let $\varphi: k \to k'$ be a field isomorphism.
Let L/k, L'/k' be field extensions.
Then an isomorphism $\bar{\phi}: L \to L'$ is called an extension of ϕ if
$\bar{\phi}|_k = \varphi$.

Remark: If $\varphi: k \to k'$ is an isomorphism, then
$\varphi_*: k[x] \to k'[x]: \sum_{i=0}^{n} a_i x^i \mapsto \sum_{i=0}^{n} \varphi(a_i) x^i$
is a ring isomorphism.

Theorem: Let $\varphi: k \to k'$ be a ring isomorphism. L/k, L'/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
$\bar{\phi}: k(a) \to k'(a')$
with $\bar{\phi}(a) = a'$, $\bar{\phi}|_k = \varphi$.

Pf: (Uniqueness)
Let $\phi: k(a) \to k'(a')$ be such an extension
Note $k(a) = \{ g(a) \mid g \in k[x] \}$
$k'(a') = \{ h(a') \mid h \in k'[x] \}$.
Thus, $b \in k(a)$, $b = g(a)$, $g \in k[x]$.

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

$$\phi(b) = \phi(g(a)) = \phi\left(\sum_{i=0}^{n} b_i a^i\right) = \sum_{i=0}^{n} \phi(b_i)\phi(a)^i =$$
$$= \sum_{i=0}^{n} \varphi(b_i) a'^i$$
$$= \varphi_*(g)(a')$$

(Existence)
Define $\phi: k(a) \to k'(a')$
$g(a) \mapsto (\varphi_* \circ g)(a)$
Clearly, ϕ is a ring homomorphism and surjective, since $\varphi_*: k[x] \to k'[x]$ isomorphism.
Thus, ϕ is an isomorphism, since $\ker \phi$ is an ideal of a field, and, by the surjectivity, is not trivial.
For $b \in k$, $\phi(b) = \varphi_*(b) = \varphi(b)$.
So $\phi|_k = \varphi$, also $\phi(a) = \varphi_*(x(a)) = x(a') = a'$. ∎

Corollary: Let L/k be a field extension. Take $a, a' \in L$ with the same min. pol. Then there is a unique k-isomorphism
$\phi: k(a) \to k(a')$
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.

$$\exists\, b, a_1, \dots, a_n \in L \text{ s.t. } f = b(x-a_1)\cdots(x-a_n)$$

Pf of equiv.

(2) $\Rightarrow$ (1) is clear

(1) $\Rightarrow$ (2)

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

$$f = (x-a)g, \quad g \in L[x], \quad \partial g = \partial f - 1$$

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

e.g.: $\mathbb{Q}$ is not alg. cl., $x^2 - 3$ has no roots over $\mathbb{Q}$
$\mathbb{R}$ " " " ", $x^2 + 1$ " " " $\mathbb{R}$
$\mathbb{Q}[i]$ is alg. closed.

Def: A field L/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 k, then there exists a k-isomorphism

$$\varphi: k \to L$$

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

Splitting field:

Theorem: Let $f \in k[x]$, irreducible. Then there is a simple algebraic extension L/k s.t. f has a zero in L.
The $[L : k] = \partial f$.

Pf: f is irreducible. Hence $\langle f \rangle$ is a max. ideal in PID $k[x]$.
Thus $L = k[x]/\langle f \rangle$ is a field extension of k.
Notice $0 = [f]$ in L. Write

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

Hence, f has a zero in L, namely $[x]$.
$L = k([x])$, b/c for $g \in k[x]$ we have $[g] = g([x])$.
f is irreducible over $k[x]$, by dividing by the leading coeff., can sps. f monic.
Then f is the minimal pol. of $[x]$. ∎

When creating a field extension in this way, we say we formally adjoint a root to k.

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

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

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

$$k \subset F \subsetneq L$$

Corollary: Let $f \in k[x]$ monic.

(1) If L/k is a field extension s.t. f splits in L into linear factors

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

then, $k(a_1, \dots, a_n)$ is splitting field of f over k.

(2) There exists a splitting field L/k of f of degree $[L : k] \leq \partial f!$

(3) Let L/k be a splitting field of f over k. Let F/k be an intermediate field
Then L is also a splitting field of f over F.

Pf: (1) let L/k s.t.

$f = (x-a_1)\cdots(x-a_n)$ over L.

Clearly, f splits over $F/k = k(a_1,\dots,a_n)$

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

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

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

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

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

Hence $k(a_1,\dots,a_n) \subset M$.

(2) By prev. corollary there exist an extension of K_1/k of degree at most ∂f s.t. f has a zero $a_1 \in K_1$.

Let $g = f/(x-a_1) \in K_1[x]$ 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 $[k(a_1,\dots,a_n)] \leq [F : k] \leq n!$

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

Since f does not splits 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 spli.. field of f over k

(2) Spitting 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 spitting field of f over $\mathbb{Q}$.

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

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

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

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

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

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

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

Extension of field isomorphisms to splitting fields

Theorem: Let $\varphi : k \to k'$ 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

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

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

$L = k$. Then, f splits over k. Since φ isomorphism f' also splits over k'!

φ 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. ext.

By prev. thr. there exists an isomorphism

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

$[L : k(a)][k(a) : k] = [L : k]$, where $[k(a) : k] = \partial g > 1$

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

By induction there is a field isomorphism

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

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 on $\mathbb{Q}(\sqrt[3]{2})$

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 β 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

$$\varphi: k(\alpha) \to k(\beta), \quad \varphi(\alpha) = \beta$$

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 spitting fields.

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

In particular, $\phi|_k = id_k$

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

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

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

Proving 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.

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

Let $f = f_1 \cdot \dots \cdot f_n$. f clearly splits over L.

And L is the splitting field of f over L. ∎

Characteristic of a field:

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

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

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

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

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

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

Note, by dist. law

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

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

PF: Let r be the order of the root a. Then

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

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

Thus

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

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.
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, if $f' \neq 0$, $\partial f' \geq \partial f$. But $\partial f' < \partial f$, proving $f' \equiv 0$.

Corollary: Every field of characteristic 0 is perfect.

PF: If $\mathrm{char}(K) = 0$. Then if $f \in K[x] \setminus K$, then

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

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. $\mathrm{char}\, K = 0$)
As $[L : K]$ finite we know

$$L = K(a_1, \dots, a_n) \quad \text{for some } a_1, \dots, a_n \in L.$$

Proceed by induction. Clearly th. holds trivially if $n = 1$.
Sps. by induction $K(a_1, \dots, a_{n-1}) = K(a)$ for some $a \in L$.
Thus, we part from the assump.

$$L = K(a, b) \qquad a, b \in L.$$

We can choose $c = a + zb$, for suitable $z \in K$.
Let f be the minimal polynomial of a over K
g " " " " " b over K.
Let F/L be a field extension s.t. both f and g splits over linear factors on F.
Let $x_1 = a, \dots, x_n$ be the roots of f over F with multiplicity,
$y_1 = b, \dots, y_m$ " " " " g over F " " .
As L/K is separable extension we have that all roots x_i are pairwise distinct. Same for y_i
Thus for $i = 1, \dots, n$, $j = 2, \dots, m$

$$z_{ij} = \frac{x_i - a}{b - y_j} \quad \text{is the unique element of } F$$

s.t. $a + z_{ij} b = x_i + z_{ij} y_j \left(\iff z_{ij} b - z_{ij} y_j = x_i - a \iff z_{ij} = \frac{x_i - a}{b - y_j} \right)$

Let $z \in k$ be different from z_{ij} $(i=1,\dots,n;\ j=1,\dots,m)$

Thus $a+zb \neq x_i + z y_j$ for all $i=1,\dots,n;\ j=1,\dots,m$.

Claim: $k(c) = k(a,b) = L$

Clearly, $k(c) \subset k(a,b)$, since $c = a+zb$.

To show $b \in k(c)$, let $h \in k(c)[x]$ be defined by

$$h(x) = f(c - zx)$$

So $h(b) = f(c-zb) = f(a) = 0$

Thus, b is a zero of h, so $(x-b) \mid h$.

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 $(x-y_j)$ is a zero of h iff $h(y_j)=0$

and $f(y_j) = f(c - z y_j) = f(a+zb - z y_j)$, by def. of z, $a+zb-zy_j \neq x_i$ for all zeros of f.

Thus, $(x-b)$ is the gcd of h and g.

As h and g both in $k(c)[x]$ then its gcd also in $k(c)[x]$.

Proving $b \in k(c)$.

So, $a = zb - c \in k(c)$. Proving $k(c) = k(a,b) = L$. □

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, those 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 on its splitting group over F.

Pf: If $a \in F$ is a root $x^q - x$

$$(x^q - x)(a) = 0$$
$$(x^q - x)'(a) = (q p^{n-1} - 1)(a) = -1 \neq 0,$$

Lemma: There exist a field of $q = p^n$ elements.

Pf: Let $\mathcal{K}$ be the splitting field of $x^q - x$ over F_p

Let $F := \{a \in \mathcal{K} \mid a^q - a = 0\}$, by prev. lemma $|F| = q$.

For $a, b \in F$:

- $(a^q - a)(b^q - b) = 0 \Rightarrow ab \in F$
- $(a^{-1})^q = (a^q)^{-1} = a^{-1} \Rightarrow a^{-1} \in F$
- $(a \pm b)^q = \sum_{i=0}^{q} \binom{q}{i} a^i b^{q-i}$, since $\binom{q}{i} = 0$ if $i \neq 0$ and $i \neq q$ and 1 otherwise

$$= a^q \pm b^q = (a \pm b)$$

$\Rightarrow a \pm b \in b$

- $1 \in F$

Hence, F is a field of q elements. ■

Remark: If F is a finite field of characteristic p.

Then F contains $F_0 := \{n \cdot 1 \mid n \in \mathbb{Z}\}$ and it is a subset

and $F_0 \cong F_p$. 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 to 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 $L/\mathcal{K}$ be a field extension. Then the Galois group of L over $\mathcal{K}$, denoted $Gal(L, \mathcal{K})$ is the group of $\mathcal{K}$-automorphism of L.

Theorem: Let $\mathcal{K}(a)/\mathcal{K}$ a simple algebraic extension of degree n. Let $f \in \mathcal{K}[x]$ be the minimal polynomial. Let $R = \{ b \in \mathcal{K}(a) \mid f(b) = 0 \}$. Then $Gal(\mathcal{K}(a), \mathcal{K})$ acts simply transitively on R. In particular, $Gal(\mathcal{K}(a), \mathcal{K})$ is isomorphic to a subgroup of $S(R)$ and $|Gal(\mathcal{K}(a), \mathcal{K})| = |R| \leq n$

Pf: Let $\varphi \in Gal(\mathcal{K}(a), \mathcal{K})$

If $f = \sum_{i=0}^{n} a_i x^i \in \mathcal{K}[x]$ and $b \in R$

$$0 = \varphi(f(b)) = \varphi\left(\sum_{i=0}^{n} a_i b^i\right) = \sum_{i=0}^{n} a_i (\varphi(b))^i = f(\varphi(b)).$$

Thus $\varphi(b) \in R$.

And we have, $\varphi|_R$ maps to R itself injectively. Since R finite, $\varphi|_R$ bijective. Prove $\varphi|_R \in S(R)$.

This allows us to define a group homomorphism

$$res_R : Gal(\mathcal{K}(a), \mathcal{K}) \longrightarrow S(M)$$

$$(\varphi \circ \psi|_R = \varphi|_R \circ \psi|_R)$$

By the existence and uniqueness theorem of field isomorphism extension:
For all $b_1, b_2 \in R$, $\exists! \varphi \in Gal(\mathcal{K}(a), \mathcal{K}) : \varphi(b_1) = \varphi(b_2)$.
Thus $Gal(\mathcal{K}(a), \mathcal{K})$ acts simply transitively on R.
Which implies $res_R : Gal(\mathcal{K}(a), \mathcal{K}) \to S(R)$ is injective.
As $Gal(\mathcal{K}(a), \mathcal{K})$ acts simply transitively

$$|Gal(\mathcal{K}(a), \mathcal{K})| = |R| \leq n. \blacksquare$$

Example: (1) $Gal(\mathbb{Q}(\sqrt{2}), \mathbb{Q})$, $f = x^2 - 2$ is min. poly.

$$\{ id, a + b\sqrt{2} \mapsto a - b\sqrt{2} \}$$

(2) $Gal(\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}) = \{ id \}$
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 $L/\mathcal{K}$ be a Galois extension of degree n. Then, $Gal(L/\mathcal{K})$ is isomorphic to a subgroup of S_n which acts simply transitively on the number $1, \dots, n$. In particular, $|Gal(L/\mathcal{K})| = [L : \mathcal{K}]$.

Pf: By the primitive element theorem, there is an element $a \in L$ s.t. $L = \mathcal{K}(a)$. Let f be the minimal polynomial of a over $\mathcal{K}$. As $L/\mathcal{K}$ is normal, f splits over L in linear factors. Hence, by sep. of L, all roots of L in L are distinct. Hence, R, the set of roots of f in L, has n elements. ■

Prop: Let $L/\mathcal{K}$ be a Galois extension. Let $a, b \in L$. Then there is a $\varphi \in Gal(L/\mathcal{K})$ with $\varphi(a) = b \iff a$ and b have the same minimal polynomial over $\mathcal{K}$.

Pf "$\Leftarrow$" Sps. a, b have same minimal poly.
By unique extension of field isom. of simple alg. extensions there is a $\mathcal{K}$-isomorphism $\varphi : \mathcal{K}(a) \to \mathcal{K}(b)$ with $\varphi(a) = \varphi(b)$.
As $L/\mathcal{K}$ is normal, L is the splitting field of some polynomial in $f \in \mathcal{K}[x]$ over $\mathcal{K}$, thus L is also the splitting field of f over $\mathcal{K}(a)$ and $\mathcal{K}(b)$.
By extension of isom. to splitting fields there exist an isomorphism $\Phi : L \to L$ with $\Phi|_{\mathcal{K}(a)} = \varphi$.

As $\Phi|_{k(a)} = \varphi$, $\varphi|_k = id_k$, $\Phi \in Gal(L/k)$ sending a to b.

"$\Rightarrow$"

Sps. $\varphi \in Gal(L/k)$ s.t. $\varphi(a) = b$.

Let $f \in k[x]$ be the min. pol. of a.
$g \in k[x]$ be the min. pol. of b.

$0 = \varphi(f(a)) = f(\varphi(a)) = f(b)$

Thus, b is a root of f. Hence $g \mid f$.

Conversely,

$0 = \varphi^{-1}(g(b)) = g(\varphi^{-1}(b)) = g(a)$

Hence, $f \mid g$. Proving $f = g$. ∎

Def: Let L/k be a Galois extension. Let G be a subgroup of $Gal(L/k)$.
Let $Fix(G) = \{ a \in L \mid \varphi(a) = a \ \forall \varphi \in G \}$

Theorem: Let L/k Galois extension. Then $Fix(Gal(L/k)) = k$.

Pf: "$\supset$" All elements of k are fixed, since elements of the Galois group are k-automorphisms.

"$\subset$" Let $\varphi(a) = a$, $\forall \varphi \in Gal(L/k)$.

Let f the min. poly. of a over k.
As L/k normal, f splits in L
Let b be a root of f in L.
Then, by above, $\exists \varphi \in Gal(L/k) : \varphi(a) = b$.
Hence, $a = b$.
Since L/k separable, f has no multiple roots.
Hence, $\deg f = 1$, proving $a \in k$. ∎

Def: Let $f \in k[x] \setminus k$. Let L be the splitting field of f over k.
The Galois group $Gal(f) := Gal(L/k)$.

Prop: Let $f \in k[x] \setminus k$ of degree n. Let R be the set of roots of f over its splitting field L.

(1) $Gal(f)$ is isomorphic to a subgroup of $S(R)$ and $|Gal(f)|$ divides $n!$.
(2) If all roots of f are simple then f is irreducible iff $Gal(f)$ acts transitively on R.

Pf: $Gal(f) = Gal(L/k)$, $\varphi \in Gal(f)$

(1) If $a \in R$, $f(\varphi(a)) = \varphi(f(a)) = \varphi(0) = 0$, i.e. $\varphi(a) \in R$.
Thus restriction to R:

$(\varphi : L \to L) \mapsto (\varphi|_R : R \to R)$

gives a group homomorphism $res : Gal(f) \to S(R)$.

If $\varphi \in \ker(res)$, i.e. $\varphi|_R = id$. Then $\varphi = id_L$, b/c $L = k(R)$.
Hence res is injective. Proving $Gal(f) \cong Im(res) \leq S(R)$.
Thus, $|Gal(f)|$ divides $|S(R)| = |R|!$ divides $n!$

(2) "$\Leftarrow$" Sps. $Gal(f)$ acts transitively on R and f reducible.

Then there exists g_1, g_2 irreducible in $k[x]$ s.t. $g_1 g_2 \mid f$.
Since $Gal(f)$ 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

$\exists \varphi \in Gal(L/k) : \varphi(a_1) = a_2$

Then, $0 = \varphi(g_1(a_1)) = g_1(\varphi(a_1)) = g_1(a_2)$
Similarly $g_2(a_1) = 0$.
Hence, up to multiplication by a constant, g_2 is the minimal polynomial of a_2 over k. Thus $g_2 \mid g_1$.
And also $g_1 \mid g_2$. Hence $g_1 = g_2$.
So $g_1^2 \mid f$. But then f has multiple zeros.
Thus, by contrapositive, this direction is proven.

"$\Rightarrow$" Sps 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 $\mathbb{k}$-automorphism $\psi: \mathbb{k}(a) \to \mathbb{k}(b)$ s.t. $\psi(a) = b$.
Notice L is also the splitting field of f over $\mathbb{k}(a)$ and over $\mathbb{k}(b)$.
By the extension of isom. to splitting fields there exists an isom. $\phi: L \to L$ s.t. $\phi|_{\mathbb{k}(a)} = \psi$.
Hence, $\phi|_{\mathbb{k}} = id$.
So, $\phi \in Gal(f)$ and $\phi(a) = b$. ■

Remark: If $L/\mathbb{k}$ is a Galois extension, then L is the splitting field of some $f \in \mathbb{k}[x]$.
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) $L/\mathbb{k}$ is a simple algebraic extension. By the primitive element theorem
$L = \mathbb{k}(\alpha)$, for some $\alpha \in L$.
Let g be the minimal polynomial of α over $\mathbb{k}$.
Let Σ be the set of roots of g in L.
Let $N := \partial g$, then $|\Sigma| = N$ (b/c $L/\mathbb{k}$ is normal, namely g splits, and separable, namely g has only simple roots).
Then $Gal(L/\mathbb{k})$ is isomorphic to a subgroup of S_N which acts simply transitively on Σ.

Example: $f = x^4 + 1 \in \mathbb{Q}[x]$
If α is a root of f, also $-\alpha$, $\frac{1}{\alpha}$, $-\frac{1}{\alpha}$ are roots.
So $\mathbb{Q}(\alpha)$ is the splitting field of f over $\mathbb{k}$.
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.
If $g = \sum_{i=0}^{N} a_i \alpha^i$ is send to $g(-\alpha) = \sum_{i=0}^{N} a_i (-\alpha)^i$

this is compatible with the operation, thus $(\alpha \mapsto -\alpha) \in Gal(f)$
Also $(\alpha \mapsto 1) \in Gal(f)$
this 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 $L/\mathbb{k}$ be a Galois extension. For a subgroup $H \subset Gal(L, \mathbb{k})$, the fixed field is

$$Fix(H) = \{ a \in L \mid \varphi(a) = a \quad \forall \varphi \in H \}$$

It can be proven that $Fix(H)$ is an intermidiate field of $L/\mathbb{k}$.

Recall: $Fix(Gal(L/\mathbb{k})) = \mathbb{k}$.

Remark: If F is an intermidiate field of $L/\mathbb{k}$
$Gal(L/F) = \{ \varphi \in Gal(L/\mathbb{k}) \mid \varphi|_F = id_F \}$
So, $Gal(L/F) \leq Gal(L/\mathbb{k})$

Theorem: Let L/k be a Galois extension with Galois group G

(1) Let $\mathcal{H} = \{H \leq G\}$ the set of subgroups of G

$\mathcal{I}$ be the set of intermediate fields of L/k.

We define maps

$$\mathcal{H} \longrightarrow \mathcal{I} \qquad\qquad \mathcal{I} \longrightarrow \mathcal{H}$$
$$H \longmapsto \mathrm{Fix}(H) \qquad\qquad F \longmapsto \mathrm{Gal}(L/F)$$

are bijections (and the inverse of each other)

That is, $\mathrm{Fix}(\mathrm{Gal}(L/F)) = F$ for all $F \in \mathcal{I}$

$\mathrm{Gal}(L/\mathrm{Fix}(H)) = H$ for all $H \in \mathcal{H}$

(2) $[L : \mathrm{Fix}(H)] = |H|$, $[\mathrm{Fix}(H) : k] = [G : H]$

(3) $[L : F] = |\mathrm{Gal}(L/F)|$, $[F : k] = [G : \mathrm{Gal}(L/F)]$