Abstract Algebra

Felix Chen

Contents

Teacher: Xiao Liang
Email: lxiao@bicmr.pku.edu.cn
Course homepage:
http://faculty.bicmr.pku.edu.cn/~lxiao/2023fall/2023fall.html
Textbook: Dummit-Foote, Abstract Algebra

§1 Groups and Homomorphisms

§1.1 Why groups/rings/fields?

- Describe symmetry uniformly;
- Compare symmetry in different context;
- Extract the "most fundamental commmon structure".

Example 1.1.1 (Pell's equation)
Consider the equation $x^2 - Dy^2 = 1$, where D is a square-free integer greater than 1. We know from high school that general solutions come from $\pm(x_0 + \sqrt{D}y_0)^N$ for $N \in \mathbb{Z}$. They form a group $Z_2 \times \mathbb{Z}$.

Example 1.1.2 (Elliptic curves)
The set $\{(x, y) \in \mathbb{Q}^2 | y^2 = x^3 - Dx\} \cup \{\infty\}$ is like $\mathbb{Z}^? \times (torsion)$.

§1.2 Groups

Definition 1.2.1 (Groups)**.** A **group** is a pair of a nonempty set G and a binary operation $* : G \times G \to G$ such that:

- $(a * b) * c = a * (b * c)$;
- $\exists$ an element $e \in G$, called the **identity**, s.t.

$$\forall a \in G, \quad e * a = a * e = a.$$

- For any element $a \in G$, there is $a^{-1} \in G$, called the **inverse** of a, s.t. $a * a^{-1} = a^{-1} * a = e$.

The group G is called **abelian** or **commutative** if $a * b = b * a$ for all $a, b \in G$.
$\#G$ or $|G|$ is called the **order** of a group (possibly infinite).

Example 1.2.2

$(\mathbb{Z}, +)$, $(\mathbb{Q}\backslash\{0\}, \cdot)$ are abelian groups.
$(Z_n, +)$ is also a group, where $Z_n = \{\text{residue classes modulo} n\}$.
$(\mathbb{Q}\backslash\{-1\}, *)$ where $a*b = ab+a+b$ is also a group. In fact this is the same with $(\mathbb{Q}\backslash\{0\}, \cdot)$.

Given two groups $(G, *)$, $(H, \circ)$, we can form their **direct product**:

$$(G \times H, \star) \quad (g, h) \star (g', h') = (g * g', h \circ h').$$

(In algebra, g' is NOT derivative)

Proposition 1.2.3 (Basic properties of groups)

If G is a group,

- The identity element is unique;
- The inverse of $a \in G$ is unique;
- $(a^{-1})^{-1} = a$.
- $(a * b)^{-1} = b^{-1} * a^{-1}$.
- $a * u = a * v \implies u = v$, $u * b = v * b \implies u = v$. (Multiply a^{-1} on both sides)

Proof. Trivial. □

There are two conventions when writing group operations (since writing $*$ is too annoying):

- When we don't know whether G is abelian or not, write $\cdot$ for $*$, and 1 for the identity.
- When we want to emphasize G is abelian, e.g. Z_n, write $+$ for $*$, and 0 for the identity, $-a$ for the inverse of a.

Example 1.2.4 (Dihedral groups D_{2n})

The group D_{2n} := symmtry group of a regular n-gon.

The elements are

$$e = \text{identity}, \quad r = \text{rotation counterclockwise} \frac{2\pi}{n}, r^2, \dots.$$

$$s = \text{reflection about a symmetry axis}, sr, sr^2, \dots.$$

We can write $D_{2n} = \langle r, s \mid r^n = s^2 = 1, srs = r^{-1} \rangle$. This notation means: take all "words" in r, s, r^{-1}, s^{-1} subject to the given relations.

Remark 1.2.5 — We can compute $sr^i s = srs^{-1}srs^{-1} \cdots srs = r^{-i}$.

Definition 1.2.6 (Generators)**.** A subset $S = \{s_1, s_2, \dots, s_n\}$ of G is called **generators** if every element in G can be written as a finite product of elements in S and their inverses.

An equality consisting of generators and their inverses is called a **relation**.

We write $G = \langle s_1, s_2, \cdots, s_n \mid R_1, \dots, R_m \rangle$ if all relations can be deduced from $R_1, \cdots, R_m$.

e.g. $Z_6 = \langle x \mid x^6 = e \rangle = \langle r, s \mid r^2 = s^3 = e, rs = sr \rangle$.

Definition 1.2.7 (Symmetry groups)**.** Let Ω be a set. Then S_Ω := {bijective maps$\sigma : \Omega \to \Omega$} has a structure of group.

- The identity element is id_Ω;
- The group operation is composition of maps;
- The inverses are just inverse maps.

S_Ω is called the **symmetry group / permutation group** of Ω.

When $\Omega = \{1, 2, \dots, n\}$, we write S_n instead. Note that $\#S_n = n!$.

Elements of S_n:

- Expression 1: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 5 & 1 & 3 & 2 & 6 & 4 \end{pmatrix}$.
- Expression 2: Consider the cycles formed by σ: we can write $\sigma = (1743)(25)(6) = (1743)(25)$.

  More generally, call $(a_1, a_2, \dots, a_r)$ a cycle, means to map $a_i \mapsto a_{i+1}, a_r \mapsto a_1$, and fixes other numbers. (Here we require all a_i's to be distinct)

In general, every element of S_n can be written as a product of *disjoint* cycles, and disjoint cycles commute with each other.

E.g. $\sigma^2 = (1743)^2(25)^2 = (14)(73)$, $\sigma^{-1} = (25)^{-1}(1743)^{-1} = (25)(1347)$.

S_n is nonabelian if $n \geq 3$.

Problem 1.2.8. Prove that:

- S_n is generated by all **transpositions** (ij).
- S_n is generated by $(i\ i+1)$.
- S_n is generated by $(12), (123 \dots n)$.

§1.3 Group isomorphisms

Definition 1.3.1 (Group isomorphisms)**.** Two groups $(G, *)$ and $(H, \cdot)$ are called **isomorphic** if there is a bijection $\phi : G \to H$ s.t.

(1) $\phi(g * h) = \phi(g) \cdot \phi(h)$, $\forall g, h \in G$;

(2) $\phi(e_G) = \phi(e_H)$;

(3) $\phi(g^{-1}) = \phi(g)^{-1}$.

We write $G \simeq H$ or $\phi : G \xrightarrow{\simeq} H$ ($\simeq$ and $\cong$ are the same here).

Remark 1.3.2 — You can prove that (1) $\implies$ (2), (3).

Example 1.3.3

$\exp : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot)$ is an isomorphism. $Z_n \to \mu_n = \{n - th\text{roots of unity}\}$ by $a \mapsto e^{\frac{2\pi i a}{n}}$ is an isomorphism.

The basic question in group theory is to classify all groups woth certain properties, up to isomorphism. e.g. all groups of order 6 are isomorphic to either Z_6 or S_3. In paricular, $D_6 \simeq S_3$.

Definition 1.3.4 (Cyclic groups)**.** A group H is called **cyclic** if it can be generated by one element, i.e. $\exists x \in H$, s.t. $H = \{x^n \mid n \in \mathbb{Z}\}$.

There are two kinds of cyclic groups (up to isomorphism):

(1) $\#H = n$, then $H = \langle x \mid x^n = 1 \rangle$, called **cyclic group of order** n. This group is isomorphic to Z_n.

(2) $\#H = +\infty$, then $H \cong \mathbb{Z}$.

Definition 1.3.5 (Subgroups)**.** A subset H of a group G is called a **subgroup**, denoted by $H < G$, if

(1) $e \in H$;

(2) $a, b \in H \implies ab \in H$;

(3) $a \in H \implies a^{-1} \in H$.

Alternatively, a subset $H \subset G$ is a subgroup if and only if $\forall a, b \in H \implies ab^{-1} \in H$. The proof is left as exercise.

Definition 1.3.6 (Generating subgroup)**.** Let G be a group and A a subset,

$$\langle A \rangle := \text{subgroup of } G \text{ generated by} A.$$

In fact, it is defined as $\bigcap_{H \leq G, A \subseteq H} H$.

Remark 1.3.7 — When G is abelian and $A = \{a_1, \dots, a_r\}$, $\langle A \rangle = \{a_1^{d_1} a_2^{d_2} \dots a_r^{d_r} \mid d_i \in \mathbb{Z}\}$. This is an analogy of "linear combination" in linear algebra.

Definition 1.3.8 (Order of an element)**.** Let G be a group, $x \in G$. Define the **order** of x in G, denoted by $|x|$, to be the least positive integer n s.t. $x^n = 1$. If such n doesn't exist, define $|x| = +\infty$.

Note that $|x| = \#\langle x \rangle$.

Example 1.3.9

Consider $Z_{12} = \langle 1 \rangle$, it's easy to see $|2| = 6$, $|3| = 4$ and $|6| = 2$.

§1.4 Quotient groups

When people develop algebra theory, they often make analogy of different objects. If we look at concepts related to vector spaces and groups, we'll find:

Vector spaces	Groups
direct sums	direct products
subspaces	subgroups
linear isomorphisms	isomorphisms
affine spaces	cosets
quotient spaces	quotient groups
linear maps	homomorphisms

So in what follows we'll study the latter 3 concepts.

Definition 1.4.1 (Cosets)**.** Let H be a subgroup of G, a **(left) coset** is a subset of G of the form $gH := \{gh \mid h \in H\}$ for some $g \in G$.

In particular, if $g \in H$, $gH = H$.

Similarly we can define a **right coset** to be Hg for some $g \in G$.

Remark 1.4.2 — For abelian groups, $gH = Hg$, there's no distinction of the two cosets. If we use the additive convention, we write $g + H = H + g$.

Proposition 1.4.3

Two cosets g_1H, g_2H are either equal or disjoint. In fact $g_1^{-1}g_2 \in H \iff g_1H = g_2H$.

Proof. We only need to prove that

$$g_1H \cap g_2H \neq \emptyset \implies g_1^{-1}g_2 \in H \implies g_1H = g_2H.$$

If $g_1^{-1}g_2 \in H$, $g_1H = g_1(g_1^{-1}g_2)H = g_2H$.

If $h \in g_1H \cap g_2H$, say $h = g_1h_1 = g_2h_2$ for $h_1, h_2 \in H$. Then $g_1^{-1}g_2 = h_1h_2^{-1} \in H$.

Now by the trivial fact that $g_1H = g_2H \implies g_1H \cap g_2H \neq \emptyset$, the three statements are equivalent, hence we've finished the proof. □

Definition 1.4.4. Write $G/H := \{gH \mid g \in G\}$ for the set of left cosets. Similarly, $H\backslash G := \{Hg \mid g \in G\}$.

Let G be a group, H a subgroup, by the previous corollary we have

$$G = \bigsqcup_{gH \in G/H} H.$$

We call $\#(G/H) =: [G : H]$ the **index** of H as a subgroup of G.

Theorem 1.4.5 (Lagrange's theorem)
If G is a finite group, and $H \leq G$, then $\#H \mid \#G$.

Proof. In fact, $\#G = \#H \cdot [G : H]$. □

Corollary 1.4.6
If G is a finite group, then $\forall x \in G$, $|x| = \#\langle x \rangle \mid \#G$. In particular, $x^{\#G} = e_G$.

Proof. Note $|x| = \#\langle x \rangle$. □

Example 1.4.7 (Euler's theorem)
Let $G = (\mathbb{Z}/N\mathbb{Z})^\times := \{a \bmod N \mid (a, N) = 1\}$, i.e. the reduced systems modulo N. Then for $\forall a \in G$, our corollary implies:

$$a^{\#G} = a^{\varphi(N)} \equiv 1 (\mathrm{mod} N).$$

Corollary 1.4.8
If $\#G$ is a prime, then G is cyclic hence abelian.

Proof. Take $a \in G$, $a \neq e_G$. Since $|a| \mid \#G$ and $|a| \neq 1$, we must have $|a| = \#G$, therefore G is cyclic.

In fact any non-identity element in G is a generator. □

Definition 1.4.9. Let G be a group, $a, g \in G$, we call $g^{-1}ag$ the **conjugate of a by g**.

Lemma 1.4.10
If H is a subgroup of G and $g \in G$, then $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$ is a subgroup of G.

Proof. Let $a, b \in gHg^{-1}$, say $a = gh_1g^{-1}, b = gh_2g^{-1}$, then

$$ab^{-1} = gh_1g^{-1}gh_2^{-1}g^{-1} = g(h_1h_2^{-1})g^{-1} \in gHg^{-1}.$$

□

Now we're going to introduce quotient groups. Since the cosets are a little different from affine subspaces (there are left and right cosets), so the quotient group can't be defined for every subgroup.

Definition 1.4.11 (Normal subgroups)**.** A subgroup $H \leq G$ is called **normal** if

$$\forall g \in G, \quad gH = Hg.$$

This is equivalent to $gHg^{-1} = H$. We write $H \trianglelefteq G$ for normal subgroups. e.g. $\{e_G\} \trianglelefteq G, G \trianglelefteq G$.

For a normal subgroup $H \trianglelefteq G$,

$$aH \cdot bH = \{kl \mid k \in aH, l \in bH\} = a(Hb)H = abHH = abH.$$

i.e. we have a well-defined group structure on G/H. (The identity is H, the inverse of aH is $a^{-1}H$) Notice how the condition of normal subgroup works here, in fact this is the motivation of normal subgroups.

We call G/H a **quotient group**.

Proposition 1.4.12

Let H and K be subgroups of G, define $HK = \{hk \mid h \in H, k \in H\}$. When H, K are finite, $\#(HK) = \frac{\#H\#K}{\#(H\cap K)}$.

Proof. Let $HK = h_1K \sqcup h_2K \sqcup \cdots \sqcup h_nK$ be a disjoint union of cosets of K.

Claim. For the same h_i's, $H = h_1(H \cap K) \sqcup \cdots \sqcup h_n(H \cap K)$.

Proof of the claim. For every $h, h' \in H$,

$$hK = h'K \iff h^{-1}h' \in K \iff h^{-1}h' \in H \cap K \iff h(H \cap K) = h'(H \cap K).$$

Hence the conclusion holds. □

Now it's easy to see $\frac{\#HK}{\#K} = \frac{\#H}{\#(H\cap K)}$.

In fact we proved a natural bijection between HK/K and $H/(H \cap K)$ by $h(H \cap K) \mapsto hK$. □

Remark 1.4.13 — HK need not be a subgroup of G. E.g. $G = S_3$, $H = \langle(12)\rangle$, $K = \langle(13)\rangle$. We have $\#HK = 4$, so it's not a subgroup.

Lemma 1.4.14

If $HK = KH$ as a set, then HK is a subgroup of G.

Proof. For $h_1, h_2 \in H$, $k_1, k_2 \in K$,

$$h_1k_1(h_2k_2)^{-1} = h_1(k_1k_2^{-1}h_2^{-1}) = h_1h'k' \in KH.$$

In the latter equality we used $HK = KH$. □

In paricular, if H is normal, we must have $HK \leq G$.

Lemma 1.4.15
If both H and K are normal subgroups, HK is also a normal subgroup.

Proof. By $gHK = HgK = HKg$ we're done. □

§1.5 Group homomorphisms

Definition 1.5.1 (Group homomorphisms)**.** Let $(G, *)$, $(H, \circ)$ be groups. A map $\phi : G \to H$ is called a **homomorphism** if

$$\forall x, y \in G, \quad \phi(x * y) = \phi(x) \circ \phi(y).$$

Remark 1.5.2 — We have $\phi(e_G) = \phi(e_G * e_G) = \phi(e_G) \circ \phi(e_G) \implies \phi(e_G) = e_H$. Similarly we have $\phi(g^{-1}) = \phi(g)^{-1}$.

You can think of homomorphisms as "maps that preserve algebraic structures".

Example 1.5.3
When $H \trianglelefteq G$, there's a natural homomorphism

$$\pi : G \twoheadrightarrow G/H, \quad a \mapsto aH.$$

Definition 1.5.4 (Kernels)**.** For a homomorphism $\phi : G \to H$ of groups, the **kernel** is

$$\ker \phi := \{g \in G \mid \phi(g) = e_H\}.$$

Lemma 1.5.5
Let $\phi : G \to H$ be a homomorphism of groups.

- The image $\phi(G)$ is a subgroup of H;
- The kernel $\ker \phi$ is a *normal* subgroup of G.
- ϕ is injective $\iff \ker \phi = \{e_G\}$.

Proof. It's the same as linear algebra, so we only prove first two.

$$\phi(g_1)(\phi(g_2))^{-1} = \phi(g_1 g_2^{-1}) \in \phi(G).$$

Let $g_1, g_2 \in \ker \phi$,

$$\phi(g_1 g_2^{-1}) = \phi(g_1)\phi(g_2)^{-1} = e_H \implies g_1 g_2^{-1} \in \ker \phi.$$

So $\ker \phi$ is a subgroup. For any $h \in \ker \phi$,

$$\phi(ghg^{-1}) = \phi(g)\phi(g^{-1}) = e_H$$

thus $ghg^{-1} \subseteq \ker \phi$, take g^{-1} in place of g, we'll get the inverse inclusion, $\ker \phi \trianglelefteq G$. □

A question arises with homomorphisms, that is, **how to specify a homomorphism?**

Suppose $G = \langle s_1, s_2, \ldots, s_n \mid R_1, \ldots, R_m \rangle$.

To give a homomorphism $\phi : G \to H$ is equivalent to giving the values $\phi(s_1), \ldots, \phi(s_n)$ so that $\phi(R_i) = e_H$ for all i.

Example 1.5.6

Let's find all homomorphisms $\phi : D_{2n} \to \mathbb{C}^\times := (\mathbb{C}\backslash\{0\}, \cdot)$.

It's enough to specify $\phi(r), \phi(s) \in \mathbb{C}^\times$ s.t. $\phi(r)^n = \phi(s)^2 = 1$, $\phi(s)\phi(r)\phi(s) = \phi(r)^{-1}$. Since $\mathbb{C}^\times$ is abelian, we have $\phi(r)^2 = 1$.

If n is odd, $\phi(r) = 1$, $\phi(s) \in \{\pm 1\}$.

If n is even, $\phi(r), \phi(s) \in \{\pm 1\}$.

Recall that in vector spaces we have $\operatorname{Im} f \cong V/\ker f$ for linear map $f : V \to W$. The same result holds for homomorphisms:

Theorem 1.5.7 (The first isomorphism theorem)

Let $\varphi : G \to H$ be a homomorphism, then $\ker \varphi \trianglelefteq G$,

$$\operatorname{Im} \varphi \cong G/\ker \varphi.$$

Proof. We define a map $\psi : G/\ker \varphi \to \varphi(G)$ by $g \ker \varphi \mapsto \varphi(g)$.

We proceed by the following:

- ψ is well-defined.

  If $g_1 \ker \varphi = g_2 \ker \varphi$, then $g_2^{-1} g_1 \in \ker \varphi$.

  $$\varphi(g_1) = \varphi(g_2 g_2^{-1} g_1) = \varphi(g_2).$$

- ψ is a homomorphism.

  $$\psi(g_1 \ker \varphi \cdot g_2 \ker \varphi) = \psi(g_1 g_2 \ker \varphi) = \varphi(g_1 g_2) = \psi(g_1 \ker \varphi)\psi(g_2 \ker \varphi).$$

- ψ is a bijection:

  $$\varphi(g) = \psi(g \ker \phi) \implies \psi \text{ surjective.}$$

  $$\psi(g \ker \varphi) = e_H \implies g \in \ker \varphi \implies g \ker \varphi = \ker \varphi.$$

  Thus $\ker \psi = \{\ker \varphi\}$, ψ is injective.

□

Theorem 1.5.8 (The second isomorphism theorem)

Let G be a group, and $A \leq G$, $B \trianglelefteq G$. We have AB is a subgroup of G, $A \cap B \trianglelefteq A$, and

$$AB/B \cong A/(A \cap B).$$

Proof. We've already proved $AB \leq G$. Clearly $B \trianglelefteq AB$, and $g(A \cap B)g^{-1} \in A \cap B$ for any $g \in A$, which implies $(A \cap B) \trianglelefteq A$.

Now we can construct a homomorphism $\phi : A \to AB/B$ by

$$\phi : A \hookrightarrow AB \twoheadrightarrow AB/B$$

with inclusion and projection map.

It's clear that ϕ is surjective since $abB = aB$ for any $a \in A, b \in B$.

Next we compute $\ker \phi = \{a \in A \mid aB = B\} = A \cap B$, thus by Theorem 1.5.7 we get $AB/B \cong A/(A \cap B)$. □

Theorem 1.5.9 (The third isomorphism theorem)

Let G be a group and $H \leq K$ are two normal subgroups of G, then $K/H \trianglelefteq G/H$, and

$$\frac{G/H}{K/H} \cong G/K.$$

Proof. I left it out since it's abstract nonsense. The technique is the same with the second theorem. □

Theorem 1.5.10 (The fourth isomorphisn theorem)

Let G be a group and $N \trianglelefteq G$ a normal subgroup. Then there's a 1-1 correspondence:

$$\begin{gathered}\{H \leq G \mid N \leq H\} \longleftrightarrow \{H \mid H \leq G/N\} \\ A \longmapsto A/N \\ \pi^{-1}(\overline{A}) \longleftarrow\shortmid \overline{A}\end{gathered}$$

Remark 1.5.11 (A way to think of a homomorphism from a quotient group) — Let $\phi : G \to H$ be a group homomorphism, let $N \trianglelefteq G$ be a normal subgroup.

We hope to define $\Phi : G/N \to H$ by $gN \mapsto \phi(g)$, such Φ is well-defined iff $N \subseteq \ker \phi$. In this case we say that $\phi : G \to H$ **factor through** G/N.

Example 1.5.12

All homomorphisms $\phi : \mathbb{Z} \to \mathbb{C}^\times$ are determined by $\lambda_\phi := \phi(1) \in \mathbb{C}^\times$.

To construct a homomorphism $Z_n = \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}^\times$, we need $n\mathbb{Z} \subset \ker \phi$. This is equivalent to λ_ϕ is an n-th root of unity.

§2 Classifying the groups

§2.1 Simple groups

Recall that:

Ultimate goal of group theorists: Classify all finite groups (with given properties).

Observe that if $N \trianglelefteq G$, "$G \approx N + G/N$". This leads us to study the "minimum groups", like prime numbers in number theory.

Definition 2.1.1 (Simple groups)**.** A (finite or infinite) group G is called a **simple group** if $\#G \geq 1$ and the only normal subgroups of G are $\{1\}$ and G.

Example 2.1.2

If p is a prime, Z_p is simple; $A_n \subseteq S_n$ are simple for $n \geq 5$.

There are infinite simple groups.

Holder's program:

- Classify all finite simple groups;
- Find all ways of "putting together simple groups".

People managed to complete the first step of this plan:

Theorem 2.1.3 (Simple Group Classification Theorem)

Every finite simple group is isomorphic to one in

- 18 (infinite) families of simple groups, e.g. $\mathrm{SL}_n(\mathbb{F}_{p^r})/\{rI_n\}$ except small p, $n \geq 2$;
- 26 sporadic simple groups.

Theorem 2.1.4 (Feit-Thompsen Theorem)

If G is a simple group of odd order, then $G \simeq Z_p$.

Definition 2.1.5 (composition series)**.** In a group G, a sequence of subgroups

$$\{e\} = N_0 < N_1 < \cdots < N_k = G$$

is called a **composition series** if $N_{i-1} \lhd N_i$, and N_i/N_{i-1} is simple for $1 \leq i \leq k$.

In this case, we call N_i/N_{i-1} **composition factors** or **Jordan-Holder factors** of G.

For example, $\{e\} \lhd \langle s \rangle \lhd \langle s, r^2 \rangle \lhd D_8$, $\{e\} \lhd \langle r^2 \rangle \lhd \langle r \rangle \lhd D_8$.

Theorem 2.1.6 (Jordan-Holder)

Let G be a finite group, $G \neq \{e\}$, then:

(1) G has a composition series;

(2) The composition factors are unique, i.e. if we have two composition series

$$\{e\} = M_0 \lhd \cdots \lhd M_r = G, \quad \{e\} = N_0 \lhd \cdots \lhd N_s = G.$$

Then $r = s$, and there's a bijection $\sigma : \{1, \ldots, r\} \to \{1, \ldots, s = r\}$ s.t.

$$M_i/M_{i-1} \simeq N_{\sigma(i)}/N_{\sigma(i)-1}.$$

Proof of (1). If G simple, take $\{e\} \lhd G$.

Otherwise $\exists N \lhd G$ s.t. N is not trivial. If $\{e\} = A_0 \lhd \cdots \lhd A_r = N$ and $\{e\} = B_0 \lhd \cdots \lhd B_s = G/N$, let $\pi : G \twoheadrightarrow G/N$ be the projection map.

Then we have:

$$\{e\} = A_0 \lhd \cdots \lhd A_r = \pi^{-1}(\{e\}) \lhd \cdots \lhd \pi^{-1}(B_s) = G.$$

(By the fourth isomorphism theorem) □

Definition 2.1.7 (Solvable groups)**.** A group G is **solvable** if there is a chain of subgroups

$$\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_s = G$$

s.t. G_i/G_{i+1} is abelian for $i = 1, 2, \ldots, s$.

Remark 2.1.8 — Galois and Abel proved that a polynomial equation has radical solutions iff the Galois group is solvable. That's where the name comes from.

Corollary 2.1.9

For G finite group, G solvable iff all of its J-H factors are of the form Z_p.

Proof. $\Longleftarrow$: by definition.

$\Longrightarrow$: $\exists G_i$ as in the definition of solvable group, we just need to refine G_i/G_{i-1}, which is a finite abelian group. To do this, choose $x \neq e$, $Z_n = \langle x \rangle \leq H$ repeatedly. □

Example 2.1.10

Dihedral groups D_{2n} are solvable, as $\{e\} \lhd \langle r \rangle \lhd D_{2n}$.

The group of upper triangular matrices are also solvable.

Proof of Theorem 2.1.6 (2). First we can consider a toymodel in set theory:

Claim. Let X be a set with two filtrations

$$\phi = A_0 \subset A_1 \subset \cdots \subset A_m = X,\ \phi = B_0 \subset B_1 \subset \cdots \subset B_n = X.$$

Then

$$(A_{i-1} \cup (A_i \cap B_j)) \backslash (A_{i-1} \cup (A_i \cap B_j)) = (B_{j-1} \cup (A_j \cap B_j)) \backslash (B_{j-1} \cup (A_{i-1} \cap B_j)).$$

This can be observed by drawing a graph. This is just the "blocks" between A_i, A_{i-1} and B_j, B_{j-1}.

The corresponding group theoretic version is:

Claim. Let G be a group with two filtrations

$$\{1\} = A_0 \lhd A_1 \lhd \cdots \lhd A_m = G,\ \{1\} = B_0 \lhd B_1 \lhd \cdots \lhd B_n = G.$$

Then
$$\frac{A_{i-1}(A_i \cap B_j)}{A_{i-1}(A_i \cap B_{j-1})} \simeq \frac{B_{j-1}(A_i \cap B_j)}{B_{j-1} \cap (A_{i-1} \cap B_j)}.$$

If we've proved this claim, we can refine the filtration to $A_{i-1}(A_i \cap B_j)$, but since A_{i+1}/A_i is simple, only one j s.t. $A_{i-1}(A_i \cap B_j)$ strictly increases, denote this j as $\sigma(i)$.

Proof of claim. We'll prove that these two groups are isomorphic to $\frac{A_i \cap B_j}{(A_i \cap B_{j-1})(A_{i-1} \cap B_j)}$. By symmetry we only need to prove one.

We first show the quotients is well-defined, i.e. subgroups are normal.

Note that $A_{i-1} \lhd A_i$, thus $A_{i-1} \lhd A_{i-1}(A_i \cap B_j) \subset A_i$. Hence $A_{i-1}(A_i \cap B_{j-1})$ is a subgroup, the normality can be checked directly:

$$\alpha\beta(ab)(\alpha\beta)^{-1} = \alpha \cdot \beta a \beta^{-1} \cdot \beta b \beta^{-1} \cdot \alpha^{-1} \in A_{i-1}(A_i \cap B_{j-1}).$$

Since $a \in A_{i-1}$, $\beta a \beta^{-1} \in A_{i-1}$. Also $\beta \in B_j$, $b \in B_{j-1} \implies \beta b \beta^{-1} \in B_{j-1}$.

Next we construct a homomorphism

$$\phi : A_i \cap B_j \hookrightarrow A_{i-1}(A_i \cap B_j) \twoheadrightarrow \frac{A_{i-1}(A_i \cap B_j)}{A_{i-1}(A_i \cap B_{j-1})}.$$

We know ϕ is surjective because every element on RHS is of the form $baA_{i-1}(A_i \cap B_{j-1}) = bA_{i-1}(A_i \cap B_{j-1}) = \phi(b)$.

We only need to prove the latter equality of

$$\ker \phi = A_i \cap B_j \cap (A_{i-1}(A_i \cap B_{j-1})) = (A_i \cap B_{j-1})(A_{i-1} \cap B_j).$$

This is trivial by looking at each element.

By Theorem 1.5.7 we get the result. □

□

Remark 2.1.11 — When $A \leq G, B \leq G$, if $AB \leq G$, then $AB = BA$ since $(ab)^{-1} = b^{-1}a^{-1}$.

§2.2 Alternating groups

One example of composition series is $\{e\} \lhd A_n \lhd S_n$, $n \geq 5$.

Recall that in S_n, every element is a product of transpositions, in fact the pairity of the number of transpositions is fixed for each element, thus we have a homomorphism $S_n \to Z_2$. The kernel of this homomorphism is denoted by A_n, the **alternating group**.

We also say the sign of $\sigma \in S_n$ is $\operatorname{sgn}(\sigma) \in \{\pm 1\}$. Those who are familiar with math olypiads might find this trivial. The strict definition of $\operatorname{sgn}(\sigma)$ is the sign of $\prod_{i<j}(\sigma(i) - \sigma(j))$ compared to $\prod_{i<j}(i-j)$, i.e. the number of *reversed pairs* in the permutation σ.

From the definition we know $A_n \lhd S_n$ has index 2, so $\#A_n = \frac{n!}{2}$.

Theorem 2.2.1

When $n \geq 5$, A_n is a simple group.

Remark 2.2.2 — When $n < 5$, $A_2 = \{1\}$, $A_3 = \langle(123)\rangle \simeq Z_3$, while $A_4 \triangleright \{1, (12)(34), (13)(24), (14)(23)\} \simeq Z_2 \times Z_2$ is not simple. It's known that a simple group of order 60 is isomorphic to A_5.

Proof. Call (ijk) a 3-cycle (i, j, k distinct). We claim that A_n is generated by 3-cycles.

A frequently used technique: if $\tau \in S_n$, then

$$\tau(a_1 a_1 \cdots a_m)\tau^{-1} = (\tau(a_1)\tau(a_2)\cdots\tau(a_m))$$

for any cycle $(a_1 a_2 \cdots a_m) \in S_n$.

By definition, A_n is generated by elements of the form $(ab)(cd)$ or $(ab)(ac)$. Note that $(ab)(ac) = (acb)$ is a 3-cycle, and $(ab)(cd) = (acb)(acd)$.

Step 2, if $N \triangleleft A_n$, and if N contains a 3-cycle ijk, then N contains all 3-cycles.

For any $(\sigma(i)\sigma(j)\sigma(k))$, if $\sigma \in A_n$, clearly it's $\sigma(ijk)\sigma^{-1} \in N$ by normality. Otherwise consider $\sigma \cdot (ab) \in A_n$, where a, b, i, j, k are distinct. Then $(\sigma(i)\sigma(j)\sigma(k)) = \sigma(ab)(ijk)(ab)\sigma^{-1} \in N$.

Step 3, suppose $N \triangleleft A_n$ is not trivial, we'll prove that N contains a 3-cycle.

Fix $\sigma \in N$, $\sigma \neq 1$. Decompose σ to disjoint cycles.

- If σ has a cycle length ≥ 4, let $\sigma = \tau(a_1 a_2 \cdots a_t)$, $t \geq 4$.

  $$N \ni (a_1 a_2 a_3)\sigma(a_1 a_2 a_3)^{-1} = \tau(a_2 a_3 a_1 a_4 \cdots a_t) =: \sigma'$$

  Consider $\sigma^{-1}\sigma' = (a_1 a_3 a_t) \in N$, we're done.

- Otherwise σ^2 has only 3-cycles, σ^3 has only 2-cycles, at least one of them is nontrivial.

- σ only contains 2-cycles: $\sigma = \tau(a_1 a_2)(a_3 a_4)$, then

  $$(a_1 a_2 a_3)\sigma(a_1 a_2 a_3)^{-1}\sigma = (a_1 a_3)(a_2 a_4) =: \sigma' \in N$$

  Take a_5 different from a_1, a_2, a_3, a_4,

  $$(a_1 a_2 a_5)\sigma'(a_1 a_2 a_5)^{-1} = (a_1 a_2 a_5 a_4 a_3) \in N,$$

  so we're back to the first case.

- σ only contains 3-cycles, left as exercise.

□

§2.3 Finitely generated abelian groups

Recall that a group G is **finitely generated** if there exists a finite subset $A \subseteq G$ s.t. $\langle A\rangle = G$.

Theorem 2.3.1 (Fundamental theorem of finitely generated abelian groups)
Let G be a finitely generated abelian group, then

$$G \simeq \mathbb{Z}^r \times Z_{n_1} \times \times Z_{n_s}$$

for integers $r \geq 0$, $2 \leq n_1 \mid n_2 \mid \cdots \mid n_s$, ($\mid$ means divides). Moreover, $r, n_1, \cdots, n_s$ are unique.

Remark 2.3.2 — r is called the **rank** of G, and $\mathbb{Z}^r$ is called the free part, the other part is called torsion part.

Proof. Abelian groups are just $\mathbb{Z}$-modules, so it follows from classification of finitely generated modules over PID (which we'll cover later). □

Lemma 2.3.3

If $m, n \in \mathbb{N}$ and $m, n \geq 2$, $\gcd(m, n) = 1$. Then $Z_{mn} \cong Z_m \times Z_n$.

Proof. The isomorphism is given by $a(\mathrm{mod}mn) \mapsto (a(\mathrm{mod}m), a(\mathrm{mod}n))$. By elementary number theory we know it's indeed an isomorphism. □

Example 2.3.4

We can compute

$$Z_{30} \times Z_{100} \simeq Z_2 \times Z_3 \times Z_5 \times Z_4 \times Z_{25} \simeq Z_{50} \times Z_{60}.$$

Also we can list all the abelian groups of order 72, i.e. by considering different prime factors.

This lemma implies a variance of the theorem:

Theorem 2.3.5

Keep G as above. Then

$$G \simeq \mathbb{Z}^r \times Z_{p_1^{r_{1,1}}} \times Z_{p_1^{r_{1,2}}} \times \cdots \times Z_{p_2^{r_{2,1}}} \times \cdots$$

These $r, p_i, r_{i,j}$ are unique under the condition $r_{i,1} \leq \cdots \leq r_{i,s_i}$.

§2.4 Different products of groups

A first question: how do we recognize direct products?

Theorem 2.4.1

Suppose G is a group with subgroups H and K, s.t.

- H and K are normal in G.
- $H \cap K = \{e\}$.

Then $HK \simeq H \times K$. (Typical case: $G = HK$)

Proof. Since $HK \lhd G$, HK is a subgroup of G.
Consider a map $\varphi : H \times K \to HK \leq G$ by $(h, k) \mapsto hk$.

We need to check φ is an isomorphism:

$$\varphi((h_1,k_1)(h_2,k_2)) = \varphi((h_1h_2,k_1k_2)) = h_1h_2k_1k_2 = h_1k_1h_2k_2 = \varphi((h_1,k_1))\varphi((h_2,k_2))$$

where the middle equality follows by the commtativity of H and K, which can be proved by $hkh^{-1}k^{-1} \in H \cap K$ by the normality of H and K.

Hence φ is a homomorphism. Clearly φ is surjective, and $\ker\varphi = \{hk = 1\}$, since $hk = 1 \implies h = k^{-1} \in K \implies h = 1$, similarly $k = 1$, hence φ is also injective, implying φ is an isomorphism. □

§2.4.1 Group action: a first glimpse

We've already seen in S_n that the elements of a group is a transformation on another set. Let's generalize this idea:

Definition 2.4.2 (Group action)**.** Let G be a group and X a set. A **(left) G-action on X** is a map

$$G \times X \to X, \quad (g,x) \mapsto g \cdot x$$

such that

- $\forall x \in X$, $e \cdot x = x$.
- For $g,h \in G$ and $x \in X$, $g \cdot (h \cdot x) = (gh) \cdot x$.

We sometimes write $G \curvearrowright X$ for group actions. (The teacher wrote a different arrow on the blackboard which I don't know how to type it in latex, so I use this as an alternate)

Remark 2.4.3 — The condition implies that $\forall g \in G$, $x \mapsto gx$ is a bijection with inverse given by g^{-1}.

Example 2.4.4

As we've already seen, S_n acts on $X = \{1,\dots,n\}$.

Another example is G-actions on G itself.

- Left translation: $g \in G \rightsquigarrow l_g : x \mapsto gx$.
- Right translation: $g \in G \rightsquigarrow r_g : x \mapsto xg^{-1}$.

  This one is a little interesting as it multiplies by g^{-1} instead of g. It's because we always assume the action is *left action* if we don't specify. We can check that:

  $$r_g(r_h(x)) = r_g(xh^{-1}) = xh^{-1}g^{-1} = x(gh)^{-1} = r_{gh}(x)$$

  so it's indeed a left action.

  One can check that $r'_g : x \mapsto xg$ is a right action.
- Conjugation action: $g \in G \rightsquigarrow \mathrm{Ad}_g : x \mapsto gxg^{-1}$.

The conjugation action is better than the translations because it gives isomorphisms of groups, i.e. Ad_g is an isomorphism $G \to G$ for each $g \in G$.

Futhermore, G can act on the set of all subgroups of G by $\mathrm{Ad}_g : H \mapsto gHg^{-1}$.

Remark 2.4.5 — Given a right action, we can obtain a left action by letting g acting as g^{-1}. Hence usually we only study left actions.

Proposition 2.4.6

Let G be a group acting on a set X. Then we have a natural homomorphism

$$\Phi : G \to S_X := \text{permutation group of } X.$$

which is given by $g \mapsto (\phi_g : x \mapsto gx)$.

Conversely, giving a such homomorphism is equivalent to giving a G-action on X.

Proof. Just check it manually:

$$\Phi(gh) = \phi_{gh} = \phi_g \circ \phi_h = \Phi(g) \circ \Phi(h).$$

□

Definition 2.4.7. If this homomorphism Φ is trivial, i.e. $\Phi(g) = \mathrm{id}_X$, we say that the action is **trivial**. In this case, $gx = x$ holds for all $g \in G, x \in X$.

If Φ is an injective, we call the action is **faithful**, i.e. $\forall g \in G$, if $g \neq 1$, then $\exists x \in X$ s.t. $gx \neq x$. (No nontrivial element of G fixes all elements of X)

Theorem 2.4.8 (Cayley's theorem)

Every group is isomorphic to a subgroup of a permutation group. In particular if $\#G = n$, then G is a subgroup of S_n.

Proof. Consider G acts on itself by left translation. □

Historically, the definition of groups are "subgroups of permutation groups" since groups are derived from solving equations. (We'll learn about it later) This theorem states that the abstract definition concides with "classical definition".

Also the proof of this theorem gives us the insight that we need to look at group actions to study the group better.

Definition 2.4.9 (Automorphism)**.** An **automorphism** of group G is an isomorphism $G \to G$. Let $\mathrm{Aut}(G)$ denote all the automorphisms of G, it is also a group with identity id_G, and group operation as composition of maps.

Clearly $\mathrm{Aut}(G) \leq S_G$.

Example 2.4.10

Consider the conjugation action $G \curvearrowright G$. We see that $\mathrm{Ad}_g \in \mathrm{Aut}(G)$, hence this induces a homomorphism

$$\mathrm{Ad} : G \to \mathrm{Aut}(G) \leq S_G, \quad g \mapsto \mathrm{Ad}_g\,.$$

Remark 2.4.11 — Slight generalization of the example: If X is itself a group, G acts on X preserving the group structure on X, i.e. $\forall g \in G$, $\phi_g : X \to X$ is a group homomorphism. Therefore the corresponding map $\Phi : G \to \mathrm{Aut}(G) \leq S_G$.

§2.4.2 Semi-direct products

First we give a prototypical example:

$$B = \begin{pmatrix} \mathbb{R}^\times & \mathbb{R} \\ 0 & 1 \end{pmatrix}, T = \begin{pmatrix} \mathbb{R}^\times & 0 \\ 0 & 1 \end{pmatrix}, N = \begin{pmatrix} 1 & \mathbb{R} \\ 0 & 1 \end{pmatrix}.$$

It's clear that $N \lhd B$, $T \leq B$ not normal. We can see that $T \cap N = \{1\}$ and $B = TN$.

Under conjugation, T acts on N by

$$\begin{pmatrix} t & \\ & 1 \end{pmatrix} \begin{pmatrix} 1 & n \\ & 1 \end{pmatrix} \begin{pmatrix} t & \\ & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & tn \\ & 1 \end{pmatrix}.$$

We write this relation by "$B = N \rtimes T$". Now we hope to reconstruct B given N, T and the action $T \curvearrowright N$.

Definition 2.4.12 (Semi-direct products)**.** Let N and H be groups and $\varphi : H \to \mathrm{Aut}(N)$ a homomorphism. For $h \in H$ write $\varphi_h := \varphi(h)$ the corresponding automorphism.

Define the **semi-direct product** $N \rtimes H := N \rtimes_\varphi H$ to be

$$\{(n, h) \mid n \in N, h \in H\}, \quad (n_1, h_1) \cdot (n_2, h_2) = (n_1 \varphi_{h_1}(n_2), h_1 h_2).$$

Check the associativity:

$$\begin{aligned} ((n_1, h_1)(n_2, h_2))(n_3, h_3) &= (n_1 \varphi_{h_1}(n_2), h_1 h_2)(n_3, h_3) \\ &= (n_1 \varphi_{h_1}(n_2) \varphi_{h_1 h_2}(n_3), h_1 h_2 h_3) \\ &= (n_1 \varphi_{h_1}(n_2 \varphi_{h_2}(n_3)), h_1 h_2 h_3) \\ &= (n_1, h_1)(n_2 \varphi_{h_2}(n_3), h_2 h_3) \\ &= (n_1, h_1)((n_2, h_2)(n_3, h_3)) \end{aligned}$$

The sets $N = \{(n, 1) \mid n \in N\} \lhd N \rtimes H$, and $H\{(1, h) \mid h \in H\} \leq N \times H$, since the projection map $\pi : N \rtimes H \to H$ has kernel N.

Remark 2.4.13 (On notation $\rtimes$) — Since N is normal, $N \rtimes H$ indicates N is normal (the triangle part of $\rtimes$).

Another interpretation is that since $H \curvearrowright N$, we can change the arrow so that it looks like $N \rtimes H$ or $H \ltimes N$.

Remark 2.4.14 (On working with $N \rtimes H = NH$) — The definition of $N \rtimes H$ requires a homomorphism $\varphi : H \to \mathrm{Aut}(N)$. Then every element in NH is of the form nh, with the relation $hnh^{-1} := \varphi_h(n)$.

Proposition 2.4.15 (Recognizing semi-direct product)

Let G be a group, $N \lhd G$, $H \leq G$ s.t. $N \cap H = \{1\}$. Then $NH = HN$ is a subgroup of G isomorphic to $N \rtimes H$.

Proof. Since N is normal, the conjuation action of H on N preserves N. We can check semi-direct product $N \rtimes_{\mathrm{Ad}} H \simeq NH$ by $(n,h) \mapsto nh$. □

Example 2.4.16

The group $Z_n^\times$ acts on Z_n by multiplication. The group $Z_n \rtimes Z_n^\times$ can be visualized by the matrix group $\begin{pmatrix} Z_n^\times & Z_n \\ & 1 \end{pmatrix}$.

Take $\{\pm 1\} \subset Z_n^\times$, then $Z_n \rtimes \{\pm 1\} \simeq D_{2n}$ by $(a,1) \mapsto r^a$, $(0,-1)$ mapsto s.

Another example is the group with order pq with p, q prime, $p \mid q-1$. By the fact that $Z_q^\times$ is a cyclic group of order $q-1$, it admits a subgroup of order p. Under the conjugation action, $Z_q \rtimes Z_p$ is a group of order pq.

An explicit example is $Z_7 \rtimes Z_3$, there are homomorphisms $\varphi_2 : Z_3 \to Z_7^\times : b \mapsto 2^b \bmod 7$ and $\varphi_4 : b \mapsto 4^b \bmod 7$.

Hence in $Z_7 \rtimes_{\varphi_2} Z_3$, $(a_1,b_1)(a_2,b_2) = (a_1 + 2^{b_1}a_2, b_1+b_2)$.

And in $Z_7 \rtimes_{\varphi_4} Z_3, (a_1,b_1)(a_2,b_2) = (a_1 + 4^{b_1}a_2, b_1+b_2)$.

In fact these two groups are isomorphic by $(a,b) \mapsto (a,2b)$.

§2.5 More on group actions

Definition 2.5.1 (Orbit)**.** Let G be a group acting on a set X (sometimes we call X a G-set). For each $x \in X$ write

$$\mathrm{Stab}_G(x) := \{g \in G \mid gx = x\}$$

called the **stabilizer subgroup** of x.

For each $x \in X$, write $\mathrm{Orb}_G(x) := G \cdot x = \{gx \mid g \in G\}$, called the **orbit** of x.

Proposition 2.5.2

The stabilizer $\mathrm{Stab}_G(x)$ is a subgroup of G.

Proof. For all $g, h \in \mathrm{Stab}_G(x)$, $h^{-1}x = h^{-1}hx = x$, so $gh^{-1}x = gx = x \implies gh^{-1} \in \mathrm{Stab}_G(x)$. □

Proposition 2.5.3

For $x, y \in X$, either $\mathrm{Orb}_G(x) = \mathrm{Orb}_G(y)$ or $\mathrm{Orb}_G(x) \cap \mathrm{Orb}_G(y) = \emptyset$. So we have

$$X = \bigsqcup_{orbits \mathcal{O}} \mathcal{O}.$$

Proof. If $z \in \mathrm{Orb}_G(x) \cap \mathrm{Orb}_G(y)$, suppose $z = gx$, $z = hy$ for $g, h \in G$, then $\forall k \in G$,

$$kx = kg^{-1}z = kg^{-1}hy \in \mathrm{Orb}_G(y).$$

□

Example 2.5.4

Let $H \leq G$, H acts on G by left translation. Given $g \in G$, $\mathrm{Orb}_H(g) = H \cdot g$ is a right coset of H. Similarly the right translation will give left cosets of H.

Proposition 2.5.5

For $y \in \mathrm{Orb}_G(x)$, say $y = gx$, then

$$\mathrm{Stab}_G(x) = g^{-1} \mathrm{Stab}_G(y) g.$$

Namely, the stabilizers at different elements of one orbit are conjugate to each other.

Proof. Since $h \in \mathrm{Stab}_G(y) \iff hy = y \iff hgx = gx \iff g^{-1}hg \in \mathrm{Stab}_G(x)$. □

Our next goal is to understand the structure of $\mathrm{Orb}_G(x)$.

Definition 2.5.6. Let G be a group acting on both sets X and Y. We say a map $\phi : X \to Y$ is G-equivariant if it preserves the group action, i.e. $\phi(gx) = g\phi(x)$.

Remark 2.5.7 — This is another example of algebraic structure on a set $\rightsquigarrow$ maps preserving structures.

Definition 2.5.8. Let $G \curvearrowright X$, we say the action is **transitive**, if $\forall x, y \in X$, $\exists g \in G$ s.t. $y = gx$.

In this case, for every $x \in X$, denote $H := \mathrm{Stab}_G(x)$. Then $\varphi : G/H \xrightarrow{\sim} X$ is a G-equivariant bijection by $gH \mapsto gx$.

Proof. Indeed, φ is well-defined if $g_1H = g_2H \implies g_1 = g_2h$ for some $h \in H$, thus $g_1x = g_2hx = g_2x$.

φ is surjective because G-action is transitive. It is injective because if $g_1x = g_2x \implies g_1^{-1}g_2 \in H \implies g_1H = g_2H$.

Clearly φ is G-equivariant so we're done. □

In general, let $\mathcal{O}$ be an orbit, since G acts transitively on $\mathcal{O}$, $\mathcal{O} = \mathrm{Orb}_G(x) \simeq G/\mathrm{Stab}_G(x)$. Thus

$$X \simeq \bigsqcup_{orbits \mathcal{O} = Gx} G/\mathrm{Stab}_G(x).$$

Definition 2.5.9. Two elements $a, b \in G$ are called **conjugate** if $a = gbg^{-1}$ for some $g \in G$, i.e. a, b lies in the same orbit under G-conjugation action. Orbits of G under conjugation action are called **conjugacy classes**.

The **centralizer** of g is defined as the stabilizer of g under conjugation action:

$$C_G(g) := \{h \in G \mid hg = gh\}.$$

This notation can be used for general subset, i.e. $C_G(S)$ for some $S \subset G$. Clearly $C_G(S) = \bigcap_{s \in S} C_G(s)$.

We say the **center** of G is $Z(G) = \{g \in G \mid gh = hg, \forall h \in G\}$, i.e. $C_G(G)$.

Alternative point of view: the conjugation action induces $\mathrm{Ad} : G \to S_n$, the center $Z(G)$ is precisely the kernel of Ad.

Finally if $H \leq G$ is a subgroup, define the **normalizer** of H to be

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

Obviously $C_G(H) \leq N_G(H)$, $H \lhd G \iff N_G(H) = G$. $N_G(H)$ is the stabilizer of H under conjugation action on the subgroups of G.

Example 2.5.10

If G is abelian, each conjugacy class contains only one element.

In $\mathrm{GL}_n(\mathbb{C})$, the conjugacy classes $\leftrightarrow$ the Jordan canonical form with nonzero eigenvalues.

In S_n, the conjugacy classes $\leftrightarrow$ the partitions of n into sum of positive integers.

Theorem 2.5.11

Let G be a finite group (acting on itself by conjugation).

(1) For each $g \in G$, the number of elements in its conjugacy class $\mathrm{Orb}_G^{\mathrm{Ad}}(g) = \mathrm{Ad}_G(g)$ is

$$\#\,\mathrm{Ad}_G(g) = \frac{\#G}{\#C_G(g)} = [G : C_G(g)].$$

(2) We have the Class equation: If $g_1, \cdots, g_r$ are representatives of conjugacy classes of G, then

$$\#G = \sum_{i=1}^{r} [G : C_G(g_i)]$$

(3) (A more useful version) In the above formula, Orbit $\mathrm{Ad}_G(g_i)$ is a singleton $\iff \forall h \in G, hg_i = g_i h$, i.e. $g_i \in Z(G)$.

$$\#G = \#Z(G) + \sum_{\text{nontriv. orbits}} [G : C_G(g_i)].$$

Proof. Trivial. □

Let's look at an example of this theorem. Let p be a prime number, a finite group G is called a **p-group** if $\#G$ is a power of p.

Theorem 2.5.12

For a nontrivial p-group G, $Z(G)$ is nontrivial.

Proof. By the class equation, $\#G = \#Z(G) + \sum_{\text{nontrivial conj class}} [G : C_G(g_i)]$.

Since $p \mid \#G$ and $p \mid [G : C_G(g_i)]$ we get $p \mid \#Z(G)$. So $Z(G)$ is nontrivial. □

Automorphism group revisit:

Recall that $\mathrm{Ad} : G \to \mathrm{Aut}(G)$ by $g \mapsto \mathrm{Ad}_g$. We already know $\ker(\mathrm{Ad}) = Z(G)$, and $\mathrm{im}(\mathrm{Ad}) =: \mathrm{Inn}(G)$ is called the group of **inner automorphisms**.

Proposition 2.5.13
$\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$.

Proof. Need to show if $\sigma : G \xrightarrow{\sim} G$ is an automorphism, then $\sigma \,\mathrm{Inn}(G)\sigma^{-1} = \mathrm{Inn}(G)$.
Take $g \in G$, we claim that $\sigma \circ \mathrm{Ad}_g \circ \sigma^{-1} = \mathrm{Ad}_{\sigma(g)}$. Indeed,

$$\sigma \circ \mathrm{Ad}_g \circ \sigma^{-1}(h) = \sigma(g\sigma^{-1}(h)g^{-1}) = \sigma(g)h\sigma(g)^{-1} = \mathrm{Ad}_{\sigma(g)}(h).$$

Hence we get $\sigma \,\mathrm{Inn}(G)\sigma^{-1} \subset \mathrm{Inn}(G)$. The reversed inclusion follows by changing σ to σ^{-1}. □

The quotient $\mathrm{Out}(G) := \mathrm{Aut}(G)/\mathrm{Inn}(G)$ is called the group of **outer automorphisms** of G.

Example 2.5.14
Consider $G = \mathrm{GL}_n(\mathbb{Q})$ and the conjugation action Ad.
We know that $\ker(\mathrm{Ad}) = Z(\mathrm{GL}_n(\mathbb{Q})) = \{a \cdot I_n\} \cong \mathbb{Q}^\times$.
Thus $\mathrm{Inn}(G) = \mathrm{GL}_n(\mathbb{Q})/\mathbb{Q}^\times =: \mathrm{PGL}_n(\mathbb{Q})$, the projective general linear group.
As for non-inner automorphism, there is essentially one: $\psi : A \mapsto (A^t)^{-1}$. (It changes eigenvalues, so it's not inner)
Therefore $\mathrm{PGL}_n(\mathbb{Q}) \rtimes \{1, \psi\}$with $\psi \cdot g = (g^t)^{-1}$ acts on $\mathrm{GL}_n(\mathbb{Q})$ as automorphisms.

Remark 2.5.15 — Fact: $\mathrm{Aut}(\mathrm{SL}_n(\mathbb{Q})) = \mathrm{PGL}_n(\mathbb{Q}) \rtimes \{1, \psi\}$ for $n \geq 3$, and $\mathrm{Aut}(\mathrm{SL}_2(\mathbb{Q})) = \mathrm{PGL}_2(\mathbb{Q})$.
The map ψ is the "dual map" in projective space $\mathbb{P}^n$, i.e. mapping lines to hyperplanes.

Another example of non-inner automorphism is: $\psi : S_6 \to S_6$ as $(12) \mapsto (12)(34)(56)$. Fact: $\mathrm{Aut}(S_6) = S_6 \rtimes \{1, \psi\}$.

§3 Sylow's theorems and applications

The main idea of Sylow's theorem is to use an abstract method to study finite groups, and we think of group action as a way to represent the group.

§3.1 Sylow's theorem

Definition 3.1.1. Fix a prime nunmber p,

- A **p-group** is a finite group whose order is a power of p.
- If G is a group with order $n = p^r \cdot m$, $p \nmid m$. A subgroup H of G of order p^r is called **Sylow p-subgroup**.

We write $Syl_p(G)$ to denote all the Sylow p-subgroups of G, $n_p := \#Syl_p(G)$.

Theorem 3.1.2 (Sylow's theorems)

Let G be a finite group with $\#G = p^r m$ with $p \nmid m$,

1. Sylow p-subgroups always exist.
2. If P is a Sylow p-subgroup of G, and $Q \leq G$ is a p-group, then there exists $g \in G$, s.t. $Q \leq gPg^{-1}$. This implies all Sylow p-subgroups are conjugate.
3. $n_p \equiv 1 (\mathrm{mod} p)$ and $n_p \mid m - 1$.

Proof of 1st Sylow. Induction on $\#G = n$, when $r = 0$, $\{e\} \leq G$ is the Sylow p-subgroup.

Now assume 1st Sylow is proved with smaller n.

- Case 1, if $p \mid \#Z(G)$. Note $Z(G)$ is a finite abelian group, by classification theorem $Z(G)$ has Sylow p-subgroup $Z(G)_p \neq \{e\}$.

  Consider $\pi : G \twoheadrightarrow G/Z(G)_p = \overline{G}$, by induction hypo, suppose $\overline{H} \leq \overline{G}$ is a Sylow p-subgroup, then $\pi^{-1}(\overline{H})$ is a Sylow p-subgroup of G. (Counting the elements)

- Case 2. $p \nmid \#Z(G)$, use the class equation

$$\#G = \#Z(G) + \sum_{\text{nontriv orbit}} \#(G/\operatorname{Stab}_i).$$

  There exists some Stab_i s.t. $p \nmid \#G/\#\operatorname{Stab}_i$. Thus $\nu_p(\#G) = \nu_p(\#\operatorname{Stab}_i) = r$ and by induction hypo, $\exists H \leq \operatorname{Stab}_i$ s.t. $\#H = p^r$, i.e. H is a Sylow p-subgroup of G.

□

Proof of 2nd Sylow. WLOG Q is nontrivial.

Consider Q acting on cosets G/P by left translation. Set $\#Q = p^{r'}$,

$$\#(G/P) = \sum_{\text{orbits } \mathcal{O}} \#\mathcal{O}.$$

Since $\mathcal{O} = Q/\operatorname{Stab}_i$, so $\#\mathcal{O}$ is either 1 or a multiple of p. But $p \nmid \#(G/P)$, there must be some $\mathcal{O}$ with 1 element.

Therefore if $\mathcal{O} = \{gP\}$, then $\forall q \in Q$,

$$qgP = gP \implies g^{-1}qgP = P \implies q \in gPg^{-1}.$$

□

Corollary 3.1.3

All Sylow p-subgroups are conjugate. In particular, there's only one Sylow p-subgroup $\iff$ a Sylow p-subgroup is normal.

Corollary 3.1.4

If P is a Sylow p-group, $N_G(P) = N_G(N_G(P))$, and $N_G(P)$ contains a unique Sylow p-subgroup.

Proof. Note that $P \trianglelefteq N_G(P)$ and P is a Sylow p-subgroup of $N_G(P)$, so clearly $N_G(P)$ does not contain other Sylow p-subgroups.

Take $n \in N_G(N_G(P))$, then $nN_G(P)n^{-1} = N_G(P)$. Therefore $nPn^{-1} \lhd nN_G(P)n^{-1}$ is another Sylow p-subgroup, by the uniqueness of Sylow p-subgroup of $N_G(P)$, $nPn^{-1} = P$. This is saying $n \in N_G(P)$, and we're done. □

Proof of 3rd Sylow. Consider $G \curvearrowright \mathrm{Syl}_p(G)$ by conjugation. By the second Sylow's theorem, this action is transitive.

$$n_p = \#G/\#N_G(P)$$

Since $\#G = p^r m$, and $\#N_G(P) = p^r k$ for some integer k, this gives $n_p \mid m$.

Consider $P \curvearrowright \mathrm{Syl}_p(G)$ by conjugation, where P is a Sylow p-subgroup. Now

$$n_p = \sum_{\text{orbits } \mathcal{O}} \#\mathcal{O}.$$

Again, $\#\mathcal{O}$ is either 1 or a multiple of p. If $\#\mathcal{O} = 1$, i.e. $P = \mathrm{Stab}_i$. Say $\mathcal{O} = \{Q\}$, then $P \subseteq N_G(Q) \implies P = Q$ by previous corollary.

Hence exactly one orbit (namely $\{P\}$) has only 1 element, so taking modulo p we get $n_p \equiv 1 (\mathrm{mod} p)$. □

Some easy applications:

Example 3.1.5

A group of order 132 cannot be a simple group. Since $132 = 3 \times 4 \times 11$, suppose G is a simple group of order 132, $n_2, n_3, n_{11} > 1$.

But $n_{11} \equiv 1 (\mathrm{mod} 11)$, $n_{11} \mid 12 \implies n_{11} = 12$. $n_3 \equiv 1 (\mathrm{mod} 3), n_3 \mid 44 \implies n_3 = 4, 22$.

Note that any two Sylow 11-subgroup must has trivial intersection (they are isomorphic to $\mathbb{Z}_{11}$), thus there are at least $12 \times 10 = 120$ elements of G if order exactly 11.

Similarly there are at least $4 \times 2 = 8$ elements of order exactly 3.

Consider the Sylow 2-subgroups H_1, H_2, so $\#(H_1 \cup H_2) \geq 6$, but $120 + 8 + 6 > 132$, contradiction!

Example 3.1.6

Consider a group G of order pq, $p < q$. By 3rd Sylow, $n_q = 1$, therefore the Sylow q-subgroup Q is normal.

Now since $n_p \mid q$ and $p \mid n_p - 1$, if $n_p = 1$, $G = P \times Q \simeq \mathbb{Z}_{pq}$.

Otherwise $n_p = q$, we must have $p \mid q - 1$, we have $G \simeq \mathbb{Z}_p \ltimes \mathbb{Z}_q$ (we've seen this group before). This group is unique up to isomorphism.

Example 3.1.7

Let G be a finite group, $\#G = p^r m$, $N \lhd G$ and $\#N = p^s n$. Let $\pi : G \twoheadrightarrow G/N = \overline{G}$ and P a Sylow p-subgroup of G.

Now $\pi(P) = \overline{P} \leq \overline{G}$, and $P \cap N \leq N$. These two groups are both Sylow p-subgroups since $s + \nu_p(\#\overline{G}) = r$, and $\ker(\pi|_P) = P \cap N$. By counting elements of $\#P = \#P \cap N \cdot \#\overline{P}$ we'll get the desired.

§3.2 Commutator subgroups

Definition 3.2.1 (Commutators)**.** For $x, y \in G$, define $[x, y] = x^{-1}y^{-1}xy$, the **commutator** of x and y. Note that $[x, y] = 1 \iff xy = yx$.

It's easy to see that $g[x, y]g^{-1} = [gxg^{-1}, gyg^{-1}]$.
Let the **derived subgroup** of G be

$$G^{der} := G' = \langle [x, y] : x, y \in G \rangle ,$$

also called the **commutator subgroup** of G.

Remark 3.2.2 — Caveat: It's not true that every element of G' is itself a commutator.

This G' is a normal subgroup of G since the conjugates of commutators are still commutators. Moreover G/G' is abelian because $xG' \cdot yG' = yG' \cdot xG' \iff x^{-1}y^{-1}xy \in G'$. In fact, G/G' is the "maximal abelian quotient of G".

Lemma 3.2.3
If A is an abelian group, and $\varphi : G \to A$ a homomorphism, then $G' \subset \ker \varphi$.

Proof. Because $\varphi(x^{-1}y^{-1}xy) = 1$ in A. □

Thus φ factors as $\varphi : G \twoheadrightarrow G/G' \to A$, where the latter map is $\overline{\varphi} : xG' \mapsto \varphi(x)$.
In other words, we have a bijection

$$\mathrm{Hom}_{gp}(G, A) \to \mathrm{Hom}_{gp}(G/G', A), \quad \varphi \mapsto \overline{\varphi}.$$

Example 3.2.4
Let $G = D_{2n}$, then G' contains $[r, s] = r^{-2}$. Therefore $\langle r^2 \rangle \leq G'$.
If n is odd, $\langle r^2 \rangle = \langle r \rangle$, consider a homomorphism $\psi : G \to \{\pm 1\}$ by $\psi(r) = 1, \psi(s) = -1$. Hence G' is contained in $\ker \psi$, so $G' = \langle r \rangle$.
If n is even, consider a homomorphism $\psi : G \to \{\pm 1\} \times \{\pm 1\}$, by $\psi(r) = (1, -1)$, $\psi(s) = (-1, 1)$. Again by our lemma, $G' \subset \ker \psi = \langle r^2 \rangle$, so $G' = \langle r^2 \rangle$.

Recall that we defined solvable groups earlier,

Definition 3.2.5. For any group G, define the following sequence of subgroups inductively,

$$G^{(0)} := G, G^{(1)} = [G, G], \ldots, G^{(i+1)} = [G^{(i)}, G^{(i)}], \quad \forall i \in \mathbb{N}^*.$$

This is called the **derived series** or the **commutator series** of G.

Remark 3.2.6 — There's an indexing convention: We use upper scripts ($G^\bullet$) for increasing filtrations, and subscripts ($G_\bullet$) for decreasing filtrations.

An example is the group of upper triangular matrices.

Proposition 3.2.7

A group is solvable if and only if $G^{(n)} = \{1\}$ for some $n \in \mathbb{N}^*$.

Proof. Note that $G^{(i+1)} \lhd G^{(1)}$ and $G^{(i)}/G^{(i+1)}$ is abelian. This proves one side of the proposition.

Conversely, if H_i is a filtration in the definition of solvable groups, note that $[H_i, H_i] \leq H_{i-1}$. Let $G = H_r$, $G^{(1)} = [G, G] \leq H_{r-1}$, similarly $G^{(2)} \leq H_{r-2}$ and so on, then $G^{(r)} \leq H_0 = \{1\}$, which proves the result. □

Remark 3.2.8 — The smallest $n \in \mathbb{Z}_{>0}$ for which $G^{(n)} = \{1\}$ is called the **solvable length** of G.

Definition 3.2.9 (Characteristic subgroup)**.** Let H be a subgroup of G, H is a **characteristic subgroup** if for any automorphism ϕ of G, $\phi(H) = H$.

E.g. if G has only one subgroup of some order $\implies$ it is characteristic.

Note that $\forall g \in G$, Ad_g is an automorphism, so characteristic subgroups are always normal.

Lemma 3.2.10

All $G^{(i)}$ are normal subgroups of G. (Moreover, all $G^{(i)}$ are characteristic subgroups)

Proof. If $\phi : G \xrightarrow{\sim} G$ is an automorphism,

$$\phi(G^{(1)}) = \left\langle \phi(x)^{-1}\phi(y)^{-1}\phi(x)\phi(y) : x, y \in G \right\rangle = G^{(1)}.$$

We can inductively prove that

$$\phi(G^{(i)}) = [\phi(G^{(i-1)}, \phi(G^{(i-1)}))] = [G^{(i-1)}, G^{(i-1)}] = G^{(i)}.$$

□

Proposition 3.2.11

Some properties of derived subgroups:

- If $H \leq G$, then $H^{(i)} \leq G^{(i)}$. So G is solvable $\implies$ H is solvable.
- If $\pi : G \twoheadrightarrow K$ is a surjective homomorphism, then $\pi(G^{(i)}) = K^{(i)}$, so G is solvable $\implies$ K is solvable.
- If $N \lhd G$ and N, G/N both solvable, then G is solvable.

§3.3 Nilpotent groups

Definition 3.3.1 (Nilpotent groups)**.** For a group G, define

$$G^0 := G, G^1 = [G, G], G^{i+1} = [G, G^i], \quad \forall i \in \mathbb{N}^*.$$

Clearly $G^0 \rhd G^1 \rhd \ldots$, this is called the **lower central series** of G, and each G^i is characteristic in G, and $G^i \geq G^{(i)}$.

A group is called **nilpotent** if $G^c = \{1\}$ for some $c \in \mathbb{N}^*$.

The upper triangular matrix group is a standard example which is solvabel but not nilpotent. While the upper triangular matrices with diagonal entries all 1 is nilpotent.

There's a "dual picture" of nilpotent groups.

Definition 3.3.2. Let G be a group, $Z_0(G) = \{1\}$, $Z_1(G) = Z(G)$. Consider $\pi : G \twoheadrightarrow G/Z(G) =: \overline{G}$, define $Z_2(G) = \pi^{-1}(Z(\overline{G}))$. (exercise: $Z_2(G) \lhd G$)

Inductively, let $\pi_i G \to G/Z_i(G)$, and define $Z_{i+1}(G) = \pi_i^{-1}(Z(G/Z_i(G)))$. We get a sequence $Z_0(G) \lhd Z_1(G) \lhd \dots$, called the **upper central series** of G.

Theorem 3.3.3

A group G is nilpotent if and only if $Z_c(G) = G$ for some $c \in \mathbb{Z}_{>0}$. More precisely, for $c \in \mathbb{Z}_{>0}$, $G^c = \{1\} \iff Z_c(G) = G$. In this case, $G^{c-i} \leq Z_i(G)$ for $i = 0, 1, \dots, c$.

Proof. Some complicated commutative diagrams. □

In fact, by upper central series we know all p-groups are nilpotent, since its center is always nontrivial.

Theorem 3.3.4

Let P be a p-group.

- $Z(P) \neq \{1\}$.
- If $\{1\} \neq H \lhd P$ is normal, then $H \cap Z(P) \neq \{1\}$.
- If H is a proper subgroup of P, then H is also a proper subgroup of $N_P(H)$.

For nilpotent groups, we have the following large theorem.

Theorem 3.3.5 (Structure theorem for nilpotent groups)

Let G be a finite group of order $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, and $P_i \in \mathrm{Syl}_p(G)$. TFAE:

(1) G is nilpotent.

(2) If H is a proper subgroup of G, then H is strictly contained in $N_G(H)$.

(3) All Sylow p_i-subgroups are normal.

(4) $G = P_1 \times P_2 \times \dots \times P_r$.

Proof. Clearly (3) $\implies$ (4), by criterion of direct product. Also (4) $\implies$ (1) is easy, since all p-groups are nilpotent.

For (2) $\implies$ (3), recall that for a Sylow p_i-subgroup, $N_G(N_G(P_i)) = N_G(P_i)$. But by (2) we must have $N_G(P_i) = G$, thus P_i is normal.

At last, (1) $\implies$ (2) is the same with last theorem, we proceed by induction on $\#G$, and take the center of G each time.

If $Z(G) \not\subset H$, then $Z(G) \subset N_G(H)$ is larger. On the other hand, since $Z(G)$ must be nontrivial, we can reduce the problem to $G/Z(G)$. □

At last we introduce an interesting theorem, whose proof is too long that we'll not include here:

Theorem 3.3.6 (Schur-Zassenhaus Theorem)
If G is a finite group, $N \lhd G$ a normal subgroup. Suppose $\gcd(\#N, \#G/N) = 1$, then $\exists H \leq G$ s.t.

$$H \hookrightarrow G \twoheadrightarrow G/N$$

is an isomorphism $H \xrightarrow{\sim} G/N$. In other words, $G = N \rtimes G/N$.

§4 Rings

Definition 4.0.1 (Rings)**.** A **ring** is a set together with two binary operators $+$ and $\cdot$, satisfying

1. $(R, +)$ is an abelian group (with 0 the additive unit).
2. $\cdot$ is associative, i.e. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
3. The **distribution** law holds in R, i.e. $\forall a, b, c \in R$,

$$(a + b) \cdot c = a \cdot c + b \cdot c, \quad a \cdot (b + c) = a \cdot b + a \cdot c.$$

4. R is **unital**, i.e. $\exists$ an element $1_R \in R$, $1_R \neq 0_R$ s.t. $1_R \cdot a = a \cdot 1_R = a$, $\forall a \in R$.

We say a ring is **commutative** if $a \cdot b = b \cdot a$, $\forall a, b \in R$.

Remark 4.0.2 — In some cases one may not require a ring is unital. But in this course we always assume R is unital.

Definition 4.0.3 (Fields)**.** A ring is called a **division ring** or a **skew field** if every nonzero element $a \in R$ has a multiplicative inverse.

A commutative division ring is called a **field**.

Example 4.0.4

Examples of rings:

- $\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.
- $\mathbb{Z}[\frac{1}{N}] := \{\frac{a}{N^r} \in \mathbb{Q}, a \in \mathbb{Z}, r \in \mathbb{N}\}$.
- The polynomial ring of a ring R,

$$R[x] := \left\{ \sum_{n \geq 0} a_n x^n, a_n \in R \right\}$$

  is a ring. (Here we require the sum is finite sum)
- If R is a ring, then $Mat_{n\times n}(R)$ is a ring.
- The **Hamiltion quaternion** $\mathbb{H} = \{a + bi + cj + dk, a, b, c, d \in \mathbb{R}\}$. The multiplication is given by $i^2 = j^2 = k^2 = -1, ij = -ji = k, jk = -kj = i, ki = -ik = j$. We also have conjugation and norm in quaternion:

$$\overline{a + bi + cj + dk} = a - bi - cj - dk, \quad Nm(z) := z\overline{z} = a^2 + b^2 + c^2 + d^2.$$

  If $z \neq 0$, then $z^{-1} = \frac{\overline{z}}{Nm(z)}$, so $\mathbb{H}$ is a division ring.

Remark 4.0.5 — More generally, we can define

$$\mathbb{H}_{\mathbb{Q},A,B} := \{a + bi + cj + dk, a, b, c, d \in \mathbb{Q}\}$$

with the relation $i^2 = A, j^2 = B, ij = -ji = k$. The others can be implied by these three relation.

Definition 4.0.6 (Groupring)**.** Let R be a (commutative) ring and G a (finite) group, say $G = \{g_1 = e, \ldots, g_n\}$. Define $R[G]$ to be the formal linear combination of elements of G,

$$R[G] = \{a_1 g_1 + \cdots + a_n g_n, a_i \in R\}.$$

We can define the multiplication on it naturally, with $1_{R[G]} = 1_R \cdot e_G$.

Example 4.0.7

When $G = Z_n$,

$$R[G] = \{a_0 + a_1\sigma + \cdots + a_{n-1}\sigma^{n-1}, a_i \in R, \sigma^n = 1\}.$$

When $G = \mathbb{Z}$ infinite, we require the sum to be finite.

§4.1 Homomorphisms

Definition 4.1.1. Let R and S be rings, a **ring homomorphism** is a map $\varphi : R \to S$ satisfying

- $\varphi(a + b) = \varphi(a) + \varphi(b)$.

- $\varphi(ab) = \varphi(a)\varphi(b)$.
- $\varphi(1_R) = 1_S$.

We need to pay extra attention to the last condition.

The **kernel** of φ is $\ker\varphi = \varphi^{-1}(0_S)$. Similarly, φ injective iff $\ker\varphi = \{0_R\}$. φ is an **isomorphism** if φ is a bijective homomorphism.

Example 4.1.2

The modulo operation $\varphi : \mathbb{Z} \to Z_n$ is a homomorphism.

If R is a commutative ring, $\forall r \in R$, $\phi_r : R[x] \to R$ by evaluation at r is a homomorphism. When R is not commutative, this is not true.

Definition 4.1.3. Let R be a ring.

- $0 \neq a \in R$ is called a **zero-divisor** if $\exists 0 \neq b \in R$, s.t. either $ab = 0$ or $ba = 0$.
- $u \in R$ is called a **unit** in R if $\exists v \in R$ s.t. $uv = vu = 1$.

The set of units in R is $R^\times$ which admits a group structure under multiplication.

Clearly the units are not zero-divisor. A *commutative* ring R with no zero-divisors is called an **integral domain**. In this case if $a \neq 0$ and $ab = ac$, we can imply $a(b-c) = 0 \implies b = c$.

Lemma 4.1.4

A finite integral domain R is a field.

Proof. Consider $m_a : R \to R$ by $x \mapsto ax$, this is a homomorphism of abelian groups, and $\ker m_a = \{0\}$.

Since R finite, m_a is bijective, thus a must have an inverse. □

In analogy of $\mathbb{Z} \to \mathbb{Q}$, we introduce the franction field. Let R be an integral domain, define the **fraction field** to be

$$\mathrm{Frac}(R) = \{(a, b) \in R \times (R \setminus \{0\})\}/\sim$$

where $(a, b) \sim (c, d) \iff ad = bc$.

Clearly $\mathbb{Q} = \mathrm{Frac}(\mathbb{Z})$, and $k(x) := \mathrm{Frac}\, k[x]$ is the rational functions in k.

§4.2 Ideals and quotient rings

In groups we have normal subgroups to construct quotients, and the corresponding concept in rings is the ideals.

Definition 4.2.1 (Ideals)**.** A subset $I \subset R$ is called a **left ideal** if

- $\forall a, b \in I$, $a + b \in I$.
- $\forall a \in I, x \in R$, $xa \in I$.

Say I is a **right ideal** if the second condition is replaced by right multiplication, and a **two-sided ideal** if it is both left and right. When R is commutative, there is no difference between left or right ideals, hence we just say "ideal".

Remark 4.2.2 — Caveat: An ideal is *almost never* a subring! If $1 \in I \implies \forall x \in R$, $x \cdot 1 = x \in I \implies I = R = (1)$.

Remark 4.2.3 (Notations of ideals) — Let R be a commutative ring, $(a_j)_{j\in J} \subset R$ is a subset. Define

$$(a_j, j \in J) = \left\{ \sum_{j\in J} x_j a_j, x_j \in R \right\}$$

to be the **ideal generated by** $(a_j)_{j\in J}$, as usual we require the sum to be finite. It's the minimum ideal that contains all $(a_j)_{j\in J}$.

Example 4.2.4

When $R = \mathbb{Z}$, $n\mathbb{Z} = (n)$ is an ideal for each $n \in \mathbb{Z}$. Note that for example $(4, 6) = 2\mathbb{Z} = (2)$, so we have $(a_1, \ldots, a_n) = (\gcd(a_1, \ldots, a_n))$.

Definition 4.2.5 (Quotient ring)**.** Let R be a ring, I a two-sided ideal and $I \neq R$. Define the **quotient ring** $R/I := \{x \in I \mid x \in R\}$, with operations

$$(x + I) + (y + I) := (x + y) + I, \quad (x + I) \cdot (y + I) := xy + I.$$

We need to check multiplication is well-defined. If $x' = x + a$, $y' = y + b$, $a, b \in I$, then

$$x'y' + I = (x + a)(y + b) + I = xy + I$$

since $xb, ay, ab \in I$ by the definition of ideals.

There exists a surjective homomorphism $\pi : R \twoheadrightarrow R/I$, such that $\ker \pi = I$.

Theorem 4.2.6 (Isomorphism theorems)

If $\varphi : R \to S$ is a homomorphism of rings, then $\ker \varphi$ is a two-sided ideal of R and $\varphi(R)$ is a subring of S. Moreover, φ induces an isomorphism $R/\ker \varphi \xrightarrow{\sim} \varphi(R)$, by $x + \ker \varphi \mapsto \varphi(x)$.

Proof. Same as groups. □

The others also holds, but I won't bother to write them all down.

Remark 4.2.7 — This can be viewed as the motivation of the definition of ideals, since we want to make it as the kernel of some homomorphism. One can see that the conditions of ideals are exactly the same as the kernel of a homomorphism.

Example 4.2.8

We have $\varphi : R[G] \to R$ by $\sum a_g g \mapsto \sum a_g$, with $\ker \varphi = (g-1, g \in G)$, called the augmentation ideal of $R[G]$.

Remark 4.2.9 (Meaning of quotients) — We can think of quotient rings as "imposing relations" in original rings. e.g. $\mathbb{R}[x]/(x-1) \cong \mathbb{R}$ and the projection map is "evaluation at $x=1$". We can think of this as imposing the relation $x=1$.

Similarly $\mathbb{R}[x,y,z]/(x-y^2, y-z^3)$ is the same as imposing $x=y^2, y=z^3$ in $\mathbb{R}[x,y,z]$.

Definition 4.2.10 (Operations on ideals)**.** Let I, J be two sided ideals of R,

- Define $I+J = \{a+b \mid a \in I, b \in J\}$.
- Define $IJ = \{\sum a_i b_i \mid a_i \in I, b_i \in J\}$, where the sum is finite. The reason we're adding the summation is to make it closed under addition.

Note that the generators of $I+J$ or IJ is just the sums / products of generators of I and J.

Remark 4.2.11 — Not every element of IJ are of the form ab where $a \in I, b \in J$. E.g. $I = (2, x) \subset \mathbb{Z}[x]$ and $4 + x^2 \in I^2$.

Example 4.2.12

Consider $\phi : \mathbb{R}[x] \to \mathbb{C}$ by $x \mapsto i$, clearly it's surjective and $\ker \phi = (x^2+1)$, so we have $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$.

Like we said, this quotient is requiring $x^2+1=0$ in $\mathbb{R}[x]$. But also note that ϕ' with $x \mapsto -i$ has the same kernel. So somehow the quotient is more intrinsic than the explicit isomorphism.

§4.3 Chinese Remainder Theorem

We all know the classical version of this theorem in number theory.

If we look at this at a higher perspective, this is saying that the ring homomorphism

$$\phi : \mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$$

$$a \mapsto (a \bmod n_1, \ldots, a \bmod n_r)$$

is a surjection, and the kernel is $n_1\mathbb{Z} \cap \cdots \cap n_r\mathbb{Z} = n_1 n_2 \cdots n_r \mathbb{Z}$. So

$$\mathbb{Z}/n_1 \cdots n_r\mathbb{Z} \simeq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}.$$

If we want to generalize this theorem to rings, first we need to say what is "coprime" in rings.

Definition 4.3.1. We say two ideals I and J of a *commutative* ring R are **comaximal** if $I+J=R$, i.e. $1 \in R$ can be written as $1 = a+b$ for $a \in I$, $b \in J$.

Theorem 4.3.2

Let $I_1, \ldots, I_k$ be ideals of a commutative ring R.

(1) Then the natural map $\varphi : R \to R/I_1 \times \cdots \times R/I_k$ by $x \mapsto (x+I_1, \ldots, x+I_k)$ is a ring homomorphism, with kernel $I_1 \cap I_2 \cap \cdots \cap I_k$.

(2) If $I_1, \ldots, I_k$ are pairwise comaximal, then φ is surjective, and $I_1 \cap \cdots \cap I_k = I_1 \cdots I_k$. This implies that

$$\overline{\varphi} : R/I_1 \cdots I_k \xrightarrow{\sim} R/I_1 \times \cdots \times R/I_k$$

Proof. (1) is trivial. First we assume $k = 2$.

Clearly $I_1I_2 \subset I_1 \cap I_2$, since $1 = a_1 + a_2$ for $a_i \in I_i$, $b \in I_1 \cap I_2 \implies b = a_1b + ba_2 \in I_1I_2$. Hence $I_1I_2 = I_1 \cap I_2$.

Consider $\varphi(a_1) = (a_1+I_1, a_1+I_2) = (I_1, 1+I_2)$ (since $a_1 = 1-a_2$). Similarly $\varphi(a_2) = (1+I_1, I_2)$. Therefore $\varphi(x_1a_2 + x_2a_1) = (x_1 + I_1, x_2 + I_2)$, i.e. φ surjective.

For general k, we use induction

$$\varphi : R \twoheadrightarrow R/I_1 \times R/I_2 \cdots I_k \twoheadrightarrow R/I_1 \cdots I_k.$$

We only need to check I_1 and $I_2 \cdots I_k$ are comaximal. Write $1 = b_i + a_i$ with $b_i \in I_1$, $a_i \in I_i$ for $i = 2, \ldots, k$. Multiplying these together we get

$$1 = \prod_{i=2}^{k}(b_i + a_i) = B + a_2 \cdots a_k.$$

Note that B is a sum of terms which contains at least one b_i, thus $B \in I_1$. □

Here we need to introduce some logics (set theory) to prove a useful proposition.

Definition 4.3.3 (Partial order)**.** A **partial order** on a nonempty set A is a relation $\preccurlyeq$ on A which is reflexive, antisymmetric and transitive. Sometimes we say A is a **poset**.

A **chain** is a subset $B \subset A$ when $\forall x, y \in B$, either $x \preccurlyeq y$ or $y \preccurlyeq x$.

Theorem 4.3.4 (Zorn's lemma (This is an axiom!))

If A is a partially ordered set in which every chain B has an upper bound, i.e. $\exists m \in A$ s.t. $b \preccurlyeq m$ for every $b \in B$. then A has a maximal element x, i.e. no element y s.t. $y \succ x$.

This is equivalent to the axiom of choice, and we assume it is true most of the time.

We introduce the Zorn's lemma just to prove one proposition.

Definition 4.3.5 (Maximal ideals)**.** If R is a ring, a two-sided ideal $\mathfrak{m} \times R$ is called **maximal** if $\mathfrak{m} \neq R$ and the only two-sided ideals containing $\mathfrak{m}$ are $\mathfrak{m}$ and R.

E.g. $p\mathbb{Z} \subset \mathbb{Z}$ is a maximal ideal for prime p.

We can see that the maximal ideals are a generalization of primes.

Proposition 4.3.6

Every proper ideal $I \subset R$ is contained in a maximal ideal of R.

Proof. Let $\mathscr{S}$ be the set of all proper ideals of R containing I. This is partially ordered by set inclusion.

We want to apply Zorn's lemma here, so we need to check the condition. For any increasing chain of ideals $\cdots \subset J_i \subset \ldots$, $i \in S$, take $J = \bigcup_{i \in S} J_i$ as the upperbound. Obviously it is an ideal containing I, and $1 \notin J_i, \forall i$, so $1 \notin J \implies J \neq R$.

Hence by Zorn's lemma there's a maximal element, which is just the desired maximal ideal. □

Now we can forget about Zorn's lemma and continuing discussing rings.

Proposition 4.3.7

Suppose R is commutative, then an ideal $\mathfrak{m} \subset R$ is maximal iff $R/\mathfrak{m}$ is a field.

Proof. By isomorphism theorems, $\mathfrak{m}$ is maximal iff $\overline{R} := R/\mathfrak{m}$ has only two ideals (0), (1). This is equivalent to $\overline{R}$ is a field, i.e. every element has a multiplicative inverse.

Because $\forall a \in \overline{R}$, $a \neq 0$,

$$(a) \neq (0) \implies (a) = (1) \iff \exists b \in \overline{R}, ab = 1.$$

□

Example 4.3.8

When $R = \mathbb{Z}[x]$, (p) is not a maximal ideal, since $(p, g(x))$ for g irreducible mod p is a larger ideal. We can see that $\mathbb{Z}[x]/(p) \simeq \mathbb{F}_p[x]$ is not a field.

When G is a finite group, $R = \mathbb{C}[G] \supseteq I_G = \langle g - 1, g \in G \rangle$ is a maximal two-sided ideal, moreover $R/I_G \simeq \mathbb{C}$.

§4.4 Prime ideals

Assume R is a commutative ring.

Definition 4.4.1 (prime ideals)**.** A proper ideal $\mathfrak{p} \subseteq R$ is called a **prime ideal** if for any $a, b \in R$, $ab \in \mathfrak{p} \implies a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.

This is also a generalization of primes, but these two properties yields different ideals for general rings.

Proposition 4.4.2

An ideal $\mathfrak{p} \subset R$ is prime iff $R/\mathfrak{p}$ is an integral domain.

Proof. Let $\pi : R \to R/\mathfrak{p} =: \overline{R}$. If $a, b \in R$,

$$ab \in \mathfrak{p} \implies \overline{ab} = 0 \implies \overline{a}\overline{b} = 0 \implies \overline{a} = 0 \text{ or } \overline{b} = 0.$$

Suppose $R/\mathfrak{p}$ is not an integral domain, $\exists \overline{a}, \overline{b} \in \overline{R}$, s.t. $\overline{a}, \overline{b} \neq 0$, and $\overline{a}\overline{b} = 0$.
This means $a \notin \mathfrak{p}, b \notin \mathfrak{p}$ but $ab \in \mathfrak{p}$, so $\mathfrak{p}$ is not a prime ideal. □

Corollary 4.4.3

A maximal ideal is a prime ideal.

Example 4.4.4

When $R = \mathbb{Z}[x]$, (p) is a prime ideal, but not maximal.

Proposition 4.4.5 (Prime avoidance)

Let R be a commutative ring.

- Let $I_1, \dots, I_n$ be ideals and let $\mathfrak{p}$ be a prime ideal containing $\bigcap_{i=1}^n I_i$. Then $\mathfrak{p} \supseteq I_i$ for some i. In particulat, if $\mathfrak{p} = \bigcap_{i=1}^n I_i$, then $\mathfrak{p} = I_i$ for some i.
- Let $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ be prime ideals and let I be an ideal contained in $\bigcup_{i=1}^n \mathfrak{p}_i$, then $I \subset \mathfrak{p}_i$ for some i.

Proof. Suppose $\exists a_i \in I_i \setminus \mathfrak{p}$ for each i. Consider $a_1 \cdots a_n \in \bigcap_{i=1}^n I_i$, this gives a contradtion since it's not in $\mathfrak{p}$. If $\mathfrak{p} = \bigcap I_i$, then $\mathfrak{p} \subset I_j, \forall j$. Now since $\mathfrak{p} \supseteq I_i$, we have $\mathfrak{p} = I_i$.

For the latter statement, we prove by induction on n that

$$I \not\subseteq \mathfrak{p}_i, \forall i \implies I \not\subseteq \bigcup_{i=1}^n \mathfrak{p}_i.$$

When $n = 1$, this is trivial. Suppose we proved this for $n - 1$.

By induction hypo, $\forall i$, $\exists x_i \in I$ s.t. $x_i \notin \bigcup_{j \neq i} \mathfrak{p}_j$. Assume that $x_i \in \mathfrak{p}_i$ (otherwise we're done), consider

$$y = \sum_{i=1}^n x_1 \cdots x_{i-1} x_{i+1} \cdots x_n \in I.$$

Since $x_1 \in \mathfrak{p}_1$ and $x_2, \dots, x_n \notin \mathfrak{p}_1$, $y \notin \mathfrak{p}_1$. Similarly $y \notin \mathfrak{p}_i$ for all i. □

Let $f : R \to S$ be a homomorphism of commutative rings.

- If $J \subset S$ is an ideal, then $f^{-1}(J)$ is an ideal in R. (contraction of ideals)
- If $I \subset R$ is an ideal, $f(I)S$ is an ideal in S. Note that $f(I)$ may not be an ideal. (extension of ideals)

Lemma 4.4.6

If $J \subset S$ is a prime ideal, then $f^{-1}(J)$ is also a prime ideal of R.

Proof. Let $\varphi : R \xrightarrow{f} S \twoheadrightarrow S/J$ be a homomorphism. Then $\ker \varphi = f^{-1}(J)$.

We have $R/f^{-1}(J) \hookrightarrow S/J$, and S/J is an integral domain. Also note that any subring of an integral domain is also an integral domain, so $R/f^{-1}(J)$ is an integral domain, which means $f^{-1}(J)$ is prime. □

§4.5 Principal ideal domain

Again our models for rings are $\mathbb{Z}$ and $\mathbb{Z}[i]$. Since the two definitions of primes end up in different ideals in general rings, we wonder when they are the same.

Definition 4.5.1 (PID)**.** A **Principal Ideal Domain (PID)** is an integral domain in which every ideal is **principal**, i.e. can generated by one element.

The rings $\mathbb{Z}$, $k[x]$ for a field k and Gaussian integer ring $\mathbb{Z}[i]$ are all PIDs.
While $\mathbb{Z}[\sqrt{-5}]$ is not a PID since $(3, 1 + 2\sqrt{-5})$ is not principal.

Proposition 4.5.2

Every non-zero prime ideal in a PID is maximal.

Proof. Let (p) be a prime ideal in R, if $M = (m) \supseteq (p)$ is a larger ideal containing (p), then $p = ms$ for some $s \in R$. Therefore $ms \in (p) \implies s \in (p)$ or $m \in (p)$.

If $m \in (p)$, then $(m) = (p)$. If $s \in (p)$, let $s = pt$, we have $mpt = p \implies mt = 1$, so $(m) = R$. □

Next we're going to introduce more special rings.

$$\text{Rings} \supseteq \text{Integral domains} \supseteq \text{UFD} \supseteq \text{PID} \supseteq \text{ED} \supseteq \text{Fields}$$

Definition 4.5.3 (ED)**.** An integral domain R is said to be an **Euclidean domain** if there's a norm $N : R \to \mathbb{Z}_{\geq 0}$, s.t.

- $N(0) = 0$,
- $\forall a, b \neq 0 \in R$, $\exists q, r \in R$ s.t. $a = bq + r$, and $r = 0$ or $N(r) < N(b)$.

Note: q, r need not be unique. The second property induces the Euclidean algorithm to find "gcd".

Example 4.5.4

All fields F are ED, since we can take $N(a) = 0$ for all $a \in F$. Clearly $\mathbb{Z}$ and $F[x]$ are also EDs. Moreover the ring of Gaussian integers are ED with $N(a + bi) = a^2 + b^2$.

Another example is $\mathbb{Z}[\zeta_3]$, with ζ_3 being the 3rd root of unity.

Proposition 4.5.5

EDs are PIDs.

Proof. If $I \subset R$ is a nonzero ideal, take the nonzero element in I with the smallest norm, say $b \in I$. We claim that $I = (b)$.

Clearly $(b) \subset I$. Conversely, for any $a \in I$, take $a = bq + r$ for some $q, r \in R$. If $N(r) < N(b)$, since $r \in I$, this contradicts with the minimality of b. Hence $r = 0$, this means $a \in (b)$. □

Definition 4.5.6. Let R be an integral domain.

- For $a, b \in R$ with $a \neq 0$, we write $a \mid b$ if $b = ac$ for some $c \in R$. (i.e. $b \in (a)$)
- A nonzero, nonunit element $p \in R$ is called a **prime element** if (p) is a prime ideal. (i.e. $p \mid ab \implies p \mid a$ or $p \mid b$)
- Suppose $r \in R$ is nonzero and nonunit. Then r is called an **irreducible element** if $r = ab \implies$ either a or b is a unit.
- Two elements $a, b \in R$ are said to be **associate** if $a = bu$ for some $u \in R^\times$.

Proposition 4.5.7

Prime elements are always irreducible. Moreover if R is a PID, then irreducible elements are prime elements.

Proof. Let $p \in R$ be a prime element, and $p = uv$. We have either u or v is in (p). WLOG $u = ps$. Therefore $p = uv = psv \implies 1 = sv \implies v$ is a unit.

If R is a PID, p irreducible implies (p) is maximal, then (p) is a prime ideal. □

Definition 4.5.8 (UFD)**.** A **unique factorization domain** is an integral domain R, in which $\forall r \neq 0 \in R$ satisfies

- r is a product of irreducibles $p_i \in R$, i.e. $r = p_1 \cdots p_m$.
- The factorization is unique up to associates.

Two main theorems:

- PID $\implies$ UFD,
- R UFD $\implies$ $R[x]$ UFD.

Example 4.5.9

Typical nonexample of UFD is $\mathbb{Z}[\sqrt{-5}]$, where $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.

Proposition 4.5.10

In a UFD, irreducible elements are prime elements.

Proof. Suppose p irreducible and $p \mid ab$. Therefore $pr = ab$, we can factor both sides into products of irreducibles. By uniqueness of factorization, a or b contains an irreducible factor which is associate to p. □

Proposition 4.5.11

In a UFD, one can define for $a, b \in R$, a gcd of a and b as an element d s.t. $d \mid a$, $d \mid b$, if $d' \mid a$, $d' \mid b$, then $d' \mid d$.

Equivalently, we can use the language of factorization. (If d is gcd, then du is gcd, $\forall u \in R^\times$)

Theorem 4.5.12

PIDs are UFDs.

Proof. Existence of factorization:

Suppose $r \neq 0 \in R$ nonunit, is not finite product of irreducible elements. Clearly r is not irreducible, so $r = a_1 b_1$ with $a_1 b_1$ nonunit.

WLOG b_1 is not a fin prod of irred elts, continuing this argument with $b_1 = a_2 b_2, \cdots$, we can write $r = a_1 a_2 b_2 = \cdots$ (this needs Axiom of choice)

Then $(r) \subset (b_1) \subset (b_2) \subset \cdots$, so $\bigcup_{n \geq 0} (b_n)$ is an ideal, PID implies it equals some (b). Therefore $b \in (b_n)$ for some n, $(b_{n+1}) = (b_{n+2}) = \cdots$, i.e. a_{n+1} is a unit, contradiction!

Uniqueness of factorization: induction on number of factors in $r = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_n$. Since irreducible elements are prime elements in PID, WLOG $p_1 \mid q_1$, so $q_1 = p_1 u$ with u unit. Therefore by induction we're done. □

§4.6 Quadratic integer rings

Definition 4.6.1 (Quadratic integer ring)**.** Let D be a square-free integer, $D \neq 1$.

$$\mathcal{O} := \begin{cases} \mathbb{Z}\left[\sqrt{D}\right] = \left\{x + y\sqrt{D} : x, y \in \mathbb{Z}\right\}, & D \equiv 2, 3 (\mathrm{mod} 4) \\ \mathbb{Z}\left[\dfrac{1+\sqrt{D}}{2}\right] = \left\{\dfrac{x + y\sqrt{D}}{2} : x, y \in \mathbb{Z}\right\}, & D \equiv 1 (\mathrm{mod} 4) \end{cases}$$

This is an analog of $\mathbb{Z} \subset \mathbb{Q}$ for $\mathcal{O} \subset \mathbb{Q}[\sqrt{D}]$.

We can define the conjugate and norm on $\mathcal{O}$ as $\overline{x + y\sqrt{D}} = x - y\sqrt{D}$ and $N(x + y\sqrt{D}) = x^2 - Dy^2$. ($N(a) = a \cdot \overline{a}$ for all $a \in \mathcal{O}$) Note that $N(\mathcal{O}) \subset \mathbb{Z}$ even if $D \equiv 1 (\mathrm{mod} 4)$.

The reason we're setting this difference is that elements of $\mathcal{O}$ can be classified as roots of some monic integer coefficient polynomial.

Lemma 4.6.2

For an element $u \in \mathcal{O}$, $u \in \mathcal{O}^\times \iff N(u) = \pm 1$.

Proof. Trivial. Use $N(u) = u\overline{u}$. □

As you might guess, this ring is closely related to *Pell's equation* in number theory. Since

$$x^2 - Dy^2 = \pm 1 \iff N(x + y\sqrt{D}) = \pm 1 \iff x + y\sqrt{D} \in \mathcal{O}^\times,$$

so solutions of Pell's equation corresponds to $\mathcal{O}^\times$, which is a group. From math olympiads we know when $D > 0$, $\mathcal{O}^\times = \pm(x_0 + y_0\sqrt{D})^{\mathbb{Z}}$ for a fundamental unit $x_0 + y_0\sqrt{D}$.

Remark 4.6.3 — Fact. For quadratic $\mathcal{O}$, $\mathcal{O}$ UFD $\iff$ PID.

A theorem states that when $D < 0$, only 9 D s.t. $\mathcal{O}_D$ is UFD/PID. A conjecture states that when $D > 0$, there are infinitely many D s.t. $\mathcal{O}_D$ is UFD/PID.

Theorem 4.6.4

A prime p is the sum of two squares of integers $p = x^2 + y^2$ for $x, y \in \mathbb{Z}$ if and only if $p = 2$ or $p \equiv 1 (\mathrm{mod} 4)$.

In fact, the irreducible elements in $\mathbb{Z}[i]$ are (up to associate)

- $1 + i$ with norm 2;
- the primes $p \equiv 3 (\mathrm{mod} 4)$ with norm p^2.
- $x + yi$ and $x - yi$ if $x^2 + y^2 = p$ for $x, y \in \mathbb{Z}$ and $p \equiv 1 (\mathrm{mod} 4)$ a prime, with norm p.

Proof. Step 1. If $\pi \in \mathbb{Z}[i]$ has norm $N(\pi) = p$ a prime, then π is irreducible. (triv.)

Step 2. For every irreducible element $\pi \in \mathbb{Z}[i]$, $N(\pi) = p$ or p^2 for some prime p.

Look at $(\pi) \cap \mathbb{Z}$, a prime ideal of $\mathbb{Z}$. (this is $i^{-1}((\pi))$ for inclusion map i) Say $(p) = (\pi) \cap \mathbb{Z}$, then $p = \pi a$ for some $a \in \mathbb{Z}[i]$. Hence $N(p) = p^2 = N(\pi)N(a)$.

- $N(\pi) = p^2 \implies N(a) = 1 \implies \pi$ is an associate of p.
- $N(\pi) = p \implies p = \pi\overline{\pi}$, both π and $\overline{\pi}$ are irreducible elements in $\mathbb{Z}[i]$.

Step 3. Look at the case $p = 2$, $p \equiv 3 (\mathrm{mod} 4)$ and $p \equiv 1 (\mathrm{mod} 4)$ separately to get the result.

In fact we only need to show $p \equiv 1 (\mathrm{mod} 4)$ is not irreducible. (This reduce to the elementary number theory)

We can take $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ of order 4 (need the existence of primitive roots), so $p \mid a^2 + 1 = (a + i)(a - i)$. But clearly $p \nmid a \pm i$, p must not be irreducible. □

Remark 4.6.5 — The norm map is actually the determinant of the linear map

$$N(x + yi) = \det(\mathbb{Q}(i) \to \mathbb{Q}(i) : z \mapsto (x + yi)z).$$

as a 2-dimensional vector space over $\mathbb{Q}$. From this we can easily deduce some properties of norm.

When we're dealing with non-UFD's, such as $\mathbb{Z}[\sqrt{-5}]$, we know $6 = 2\times3 = (1+\sqrt{-5})(1-\sqrt{-5})$, people wonder whether we can write $2 = ab, 3 = cd, 1 + \sqrt{-5} = ac, 1 - \sqrt{-5} = bd$ for some "numbers" a, b, c, d. It turns out that such numbers don't exist, so people used to call it "ideal numbers", and this is how the name "ideal" come from.

Using the ideals, we can indeed write

$$p_1 = (2, 1 + \sqrt{-5}), p_2 = (2, 1 - \sqrt{-5}), p_3 = (3, 1 + \sqrt{-5}), p_4 = (3, 1 - \sqrt{-5}).$$

So we'll get $(2) = p_1p_2$ and so on. In light of this we introduce:

Definition 4.6.6 (Dedekind domains)**.** We say an integral domain R is a **Dedekind domain** if every ideal can be written as a product of prime ideals.

We can prove that every quadratic integer ring is a Dedekind domain. This kind of rings has significant position in number theory.

Theorem 4.6.7

Let R be an integral domain. Then R is UFD $\iff$ $R[x]$ is UFD.

Proof. Assume $R[x]$ is UFD. Let $r \in R$ is nonzero and nonunit. Then $r = p_1 \cdots p_m$ for $p_i \in R[x]$ irreducible.

By comparing the degree of both sides, we get $p_i \in R$ since they must be constant polynomial. Also they are irreducible in $R[x]$, so clearly they are irreducible in R.

The uniqueness also follows from the uniqueness in $R[x]$.

Conversely, first we prove a lemma.

Lemma 4.6.8 (Gauss' Lemma)

Let R be a UFD, $F = \mathrm{Frac}(R)$. Let $p(x) \in R[x]\backslash\{0\}$ be reducible in $F[x]$, then it's also reducible in $R[x]$.

More precisely, if $p(x) = A(x)B(x)$ in $F[x]$, there exists $r \in F^\times$ s.t. $rA(x), r^{-1}B(x) \in R[x]$.

Proof of lemma. Take $d_1, d_2 \in R\backslash\{0\}$ such that $d_1A(x), d_2B(x) \in R[x]$. Let $d = d_1d_2$, we have $dp(x) = a(x)b(x)$ in $R[x]$.

If $d \in R^\times$, then we're done. Otherwise write $d = p_1 \cdots p_n$, $p_i \in R$ irreducible. Since p_i are primes, $R/(p_i)$ is integral. Hence $(R/(p_i))[x]$ is an integral domain as well.

Therefore $0 = \overline{a}(x)\overline{b}(x)$ modulo (p_i), by properties of integral domain, WLOG $\overline{a}(x) = 0$, this means $p_i^{-1}a(x) \in R[x]$. (Here $p_i^{-1} \in F$.)

We can do this for each p_i, so we can cancel out all the p_i's, which induces $p(x)$ reducible in $R[x]$. □

Returning to the theorem, let $a(x) \in R[x]$ nonzero and nonunit.

Let d be a gcd of coefficients of $a(x)$, $a(x) = da_1(x)$. Since $d \in R$, which is a UFD, we only need to factor $a_1(x)$.

Now we use the fact that $F[x]$ is UFD, $a_1(x) = A_1(x) \cdots A_r(x)$ in $F[x]$.

By Gauss' Lemma, we can adjust $A_i(x)$ to $B_i(x) \in R[x]$ s.t. $a_1(x) = B_1(x) \cdots B_r(x)$, which is a factorization in $R[x]$.

By the gcd of coefficients is 1 and $B_i(x)$ irreducible in $F[x]$ we deduce $B_i(x)$ are irreducible in $R[x]$, which proves the existence part.

As for the uniqueness, we can use the uniqueness in $F[x]$ and the uniqueness in R. □

Corollary 4.6.9

Let R be a UFD, then $R[x_1, \ldots, x_n] = R[x_1, \ldots, x_{n-1}][x_n]$ is a UFD.

Next we'll introduce some methods to determine whether a polynomial is irreducible or not.

Let F be a field. Let $f \in F[x]$ with degree 2 or 3. Clearly f irreducible $\iff$ f has no roots in F.

Recall that in elementary number theory, we have a criterion for rational roots.

Proposition 4.6.10

Let $f(x) = a_nx^n + \cdots + a_0 \in \mathbb{Z}[x]$. If $f(\frac{r}{s}) = 0$ with $r, s \in \mathbb{Z}$, $\gcd(r, s) = 1$, then $r \mid a_0$, $s \mid a_n$.

Proposition 4.6.11 (Eisenstein's criterion)

Let R be an integral domain. $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0 \in R[x]$. Suppose there exists a prime ideal $\mathfrak{p}$ of R s.t. $c_0, \ldots, c_{n-1} \in p$, but $c_0 \notin \mathfrak{p}^2$, then f is irreducible.

Proof. Assume by contradiction f is reducible, say $f(x) = a(x)b(x)$.

Taking modulo $\mathfrak{p}$ we get $x^n = \overline{a(x)} \cdot \overline{b(x)}$ in $(R/\mathfrak{p})[x]$, which is integral.

By uniqueness of factorization in $\mathrm{Frac}(R/\mathfrak{p})[x]$, we know $\overline{a(x)}, \overline{b(x)}$ are of the form x^r.

Specifically, the constant term of $a(x)$ and $b(x)$ are in $\mathfrak{p}$ $\implies$ $c_0 \in \mathfrak{p}^2$, contradiction! □

Example 4.6.12

Let p be a prime, write $\Phi_p(x) = \frac{x^p-1}{x-1}$ be the cyclotomic polynomial of order p. $\Phi_p(x)$ is irreducible in $\mathbb{Z}[x]$, since $\Phi_p(x+1) = \frac{(x+1)^p-1}{x}$. By Eisenstein's criterion we know it's irreducible.

Proposition 4.6.13

Let F be a field.

- $f(x) \in F[x]$ irreducible $\iff$ $F[x]/(f(x))$ is a field.
- $f(x) = p_1(x)^{n_1} \cdots p_r(x)^{n_r}$, by CRT we have

$$F[x]/(f(x)) \cong F[x]/(p_1(x)^{n_1}) \times \cdots \times F[x]/(p_r(x)^{n_r}).$$

- If $f(x)$ has root $\alpha_1, \ldots \alpha_k \in F$, then $(x-\alpha_1)\cdots(x-\alpha_k) \mid f(x)$. So the number of roots is no more than the degree of f.

Proof. Note that $f(x)$ irreducible $\iff$ $f(x)$ prime $\iff$ $(f(x))$ is a prime ideal $\iff$ $(f(x))$ is a maximal ideal $\iff$ $F[x]/(f(x))$ is a field. ($F[x]$ is a PID) □

Corollary 4.6.14

Let F be a field. Then any finite subgroup G of $F^\times$ is cyclic.

Proof. Since G is abelian, we can write

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \mathbb{Z}/n_r\mathbb{Z}, \quad n_i \mid n_{i+1}.$$

If G is not cyclic, $n_r < \#G$. Therefore $\forall x \in G$, $x^{n_r} = 1 \implies x^{n_r}$ has $\#G$ roots in F, contradiction! □

There's a missing lecture note on November 16, Thursday, it's about modules and the classification theorem of finitely generated modules on PIDs.

§4.7 Fundamental theorem of finitely generated modules over a PID

Theorem 4.7.1

Let R be a PID and M a finitely generated R-module. Then

$$M \simeq R^{\oplus r} \oplus R/(a_1) \oplus \cdots \oplus R/(a_n)$$

with $a_1 \mid \cdots \mid a_n$, $a_i \in R$. Such $r, a_1, \ldots, a_n$ are unique (up to associates).

We previouly proved that

Lemma 4.7.2

Let R be a PID, M a free R-module of rank m and N a submodule of M. Then

- N is free of rank n, $n \leq m$.
- There exists a basis $y_1, \ldots, y_m$ of M so that $a_1 y_1, \ldots, a_n y_n$ is a basis of N and $a_i \in R$ satisfying $a_1 \mid \cdots \mid a_n$.

Proof of Theorem 4.7.1. Existence:

Suppose M fin. gen., then there exists a surjective homomorphism $\phi : R^{\oplus m} \twoheadrightarrow M$. Applying our lemma to $\ker \phi \subset R^{\oplus m}$, write $R^{\oplus m} = Ry_1 \oplus \cdots \oplus Ry_m$, and $\ker \phi = Ra_1 y_1 \oplus \cdots \oplus Ra_n y_n$, then we have

$$M = R^{\oplus m} / \ker \phi = \frac{Ry_1}{Ra_1 y_1} \oplus \cdots \oplus \frac{Ry_n}{Ra_n y_n} \oplus Ry_{n+1} \oplus \cdots \oplus Ry_n.$$

For the uniqueness part, by CRT we know that for $a \in R$ nonzero, nonunit, if it factors as $a = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ in R, then

$$R/(a) \simeq R/(p_1^{\alpha_1}) \times \cdots \times R/(p_r^{\alpha_r}).$$

Thus we have an alternative version of this theorem in prime powers, it suffices to deal with each prime element p.

We can compute $p^r M / p^{r+1} M$ to get the results. Fact:

Lemma 4.7.3

If $p, q \in R$ are prime elements, $(p) \neq (q)$, $r, s \in \mathbb{N}$.

- If $M \simeq R$, then $M/p^r M \simeq R/(p^r)$, $p^r M / p^{r+1} M \simeq (p^r)/(p^{r+1}) \simeq R/(p)$.
- If $M \simeq R/(p^s)$, then $p^r M = p^r R / p^s R$ if $r < s$ and 0 otherwise.
- If $M \simeq R/(q^s)$, $p^r M = M$. (This is trivial since $(p^r, q^s) = (1)$.)

Applying the lemma, let $F_i = R/(p_i)$ be a field. consider $\dim_{F_i}(M/p_i M)$, it is equal to $r + \#\{\alpha_{ij} \geq 1\}$. Similarly $\dim_{F_i}(p_i^\beta M / p_i^{\beta+1} M) = r + \#\{\alpha_{ij} \geq \beta\}$, so α_{ij}'s are unique. □

§5 Fields

§5.1 Basics

Definition 5.1.1 (characteristics)**.** The **characteristic** of a field F, denoted by $\mathrm{char}(F)$, is the smallest positive integer p s.t. $p \cdot 1_F = 0$ if such p exists, and 0 other wise.

Remark 5.1.2 — If $\mathrm{char}(F) > 0$, then it must be a prime. because if $\mathrm{char}(F) = mn$, then $mn = 0$ in F, which implies m or n is 0 in F.

Definition 5.1.3. The **prime field** of a field F is the smallest subfield of F containing 1_F.

It is $\mathbb{F}_p$ if $\mathrm{char}(F) = p > 0$ or $\mathbb{Q}$ if $\mathrm{char}(F) = 0$.

If $F \subseteq K$ is a subfield, we say K is a **field extension** of F. Sometimes we call F the **base field**. Any field E s.t. $F \subseteq E \subseteq K$ is called an **intermediate field**.

Often we'll write $K/E/F$ for this relation. (K over E over F)

Definition 5.1.4. Note that if $F \subseteq K$, then K is an F-vector space. The **degree** of a field extension K/F is $[K : F] = \dim_F K$.

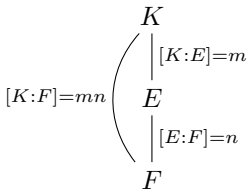
The extension is finite / infinite if $[K : F]$ is finite / infinite.

Theorem 5.1.5 (Tower law)

Let $F \subseteq E \subseteq K$ be field extensions. Then $[K : F] = [K : E] \cdot [E : F]$.

Proof. Let $m = [K : E]$, $n = [E : F]$.

Let $\beta_1, \ldots, \beta_m$ be an E-basis of K, $\alpha_1, \ldots, \alpha_n$ be an F-basis of E. Just write every element of K explicitly as linear combinations of $\alpha_j\beta_i$, and check that $\alpha_j\beta_i$'s are linearly independent.



□

Lemma 5.1.6

All homomorphisms between fields are injective.

Proof. Let $\eta : F \to E$ a homomorphism of fields. Since $\ker \eta$ is an ideal of F, it must be $\{0\}$ or F. But we require $\eta(1_F) = 1_E$, thus $\ker \eta = \{0\}$, hence η is injective. □

From this we know any homomorphism $\eta : F \to E$ realize E as an extension of F.

Let F be a field, we can construct field extensions by polynomials. Let $p(x) \in F[x]$ be an irreducible polynomial of degree n, since $(p(x))$ is a prime ideal hence maximal ideal, $K := F[x]/(p(x))$ is a field containing F.

Setting $\theta := x \bmod (p(x))$, then

$$K = \{a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1} \mid a_i \in F\},$$

so $\dim_F K = \deg p(x) = n$. Note that $p(z) = 0$ has a zero θ in K.

Example 5.1.7

Consider $\mathbb{R}[x]/(x^2 + 1) \xrightarrow{\sim} \mathbb{C}$. Note that $x^2 + 1$ has two roots in $\mathbb{C}$, so there are two isomorphisms $\eta_1 : ax + b \mapsto ai + b$ and $\eta_2 : ax + b \mapsto -ai + b$.

Hence in practice we view $\mathbb{R}[x]/(x^2 + 1)$ as an abstract extension of $\mathbb{R}$, it has two "realizations" η_1, η_2 to be isomorphic to $\mathbb{C}$.

Another example is $K = \mathbb{Q}[x]/(x^3 - 2)$, it has 3 realizations into $\mathbb{C}$, i.e.

$$\mathbb{Q}(\sqrt[3]{2}) \simeq \mathbb{Q}(e^{\frac{2\pi i}{3}}\sqrt[3]{2}) \simeq \mathbb{Q}(e^{\frac{4\pi i}{3}}\sqrt[3]{2})$$

A third example is $K = \mathbb{F}_2/(x^2 + x + 1)$, it is a field with 4 elements.

Definition 5.1.8. Let K be a field extension of F,r and let $\alpha_1, \dots, \alpha_n \in K$. $F(\alpha_1, \dots, \alpha_n)$ is defined as the smallest subfield of K containing F and $\alpha_1, \dots, \alpha_n$, called the field **generated** by $\alpha_1, \dots, \alpha_n$.

If $K = F(\alpha)$ for some $\alpha \in K$, we say K/F is a **simple extension**. E.g. $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ is a simple extension.

Theorem 5.1.9

Let K/F be a field extension and let $\alpha \in K$. We have a *dichotomy*:

- $1, \alpha, \alpha^2, \dots$ are linearly independent over F, in this case, $F(\alpha) \simeq F(x) = \mathrm{Frac}(F[x])$.
- They are linearly dependent over F. Then there exists a unique *monic* polymonial $m_\alpha(x) \in F[x]$, that is irreducible over F and $m_\alpha(\alpha) = 0$.

  This m_α is called the **minimal polynomial** of α. In this case $F(\alpha) \simeq F[x]/(m_\alpha(x))$ and the degree is $\deg m_\alpha$.

Proof. Case 1: $\phi : F[x] \to K$ is an injective homomorphism by $x \mapsto \alpha$. This extends to a homomorphism $\phi : \mathrm{Frac}(F[x]) \to K$, since $g(\alpha) \neq 0$ whenever $g \neq 0$. So $F(\alpha) = \mathrm{Im}\,\phi \simeq F(x)$.

Case 2: $\phi : F[x] \to K$ is not injective. Then $\ker \phi = (p(x))$ for some $p(x) \in F[x]$. But $F[x]/(p(x)) \subset K$ is an integral domain, $p(x)$ must be a prime element. □

§5.2 Algebraic extensions

Definition 5.2.1. In the above theorem, if the first case occurs, we say α is **transcendental over** F. Otherwise we say α is **algebraic over** F.

We say that extension K/F is **algebraic** if every element of K is algebraic over F, i.e. $\forall \alpha \in K$, $[F(\alpha) : F]$is finite.

It seems that algebraic extensions are finite in some sense.

Example 5.2.2

The field $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \dots)$ is an algebraic extension but not finite.

Theorem 5.2.3

The following are equivalent for a field extension K/F.

(1) K/F is finite.

(2) K/F is finitely generated and algebraic.

Proof. (1) $\implies$ (2) is trivial since K is a finite dimensional vector space over F. (In fact we have a corollary $[F(\alpha) : F] \mid [K : F]$.)

The converse statement needs some lemma. □

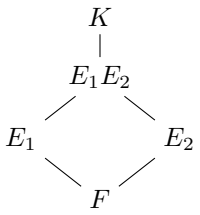
Lemma 5.2.4

Given $K \ni \alpha$, then $\deg m_{\alpha,E} \leq \deg m_{\alpha,F}$. ($K/E/F$ are field extensions)

Proof. Since $m_{\alpha,F}(\alpha) = 0$, view it in $E[x]$ implies $m_{\alpha,F} \in (m_{\alpha,E}(x))$, thus $m_{\alpha,E} \mid m_{\alpha,F}$ in $E[x]$. □

Corollary 5.2.5
$[E(\alpha) : E] \leq [F(\alpha) : F]$.

Definition 5.2.6. Let K/F be field extension and E_1, E_2 are intermediate fields. Define E_1E_2 to be the minimal field that contains both E_1 and E_2, called the **composite** of E_1 and E_2.



Lemma 5.2.7
Suppose $[E_i : F] < \infty$. Then $[E_1E_2 : F] \leq [E_1 : F] \cdot [E_2 : F]$.

Proof. Write $E_1 = F(\alpha_1, \ldots, \alpha_n)$. By corollary, $[E_2(\alpha_1) : E_2] \leq [F(\alpha_1) : F]$, $[E_2(\alpha_1, \alpha_2) : E_2(\alpha_1)] \leq [F(\alpha_1, \alpha_2) : F(\alpha_1)]$, ...

Multiplying them together, by tower law we get $[E_1E_2 : E_2] \leq [E_1 : F]$. □

Proof of (2) $\implies$ (1). Let $K = F(\alpha_1, \ldots, \alpha_n)$ be an algebraic extension. Then

$$[K : F] \leq \prod [F(\alpha_i) : F] < +\infty.$$

□

Corollary 5.2.8
Suppose in a field extension K/F, $\alpha, \beta \in K$ are algebraic over F. Then $\alpha + \beta, \alpha - \beta, \alpha\beta, \frac{\alpha}{\beta}$ are all algebraic over F.

Proof. They are all in $F(\alpha, \beta)$ which is finite over F. □

So $\{\alpha \in K : \alpha \text{ algebraic over } F\}$ is a subfield of K, called the **algebraic closure of F in K**.

Example 5.2.9
Consider $\mathbb{C}/\mathbb{Q}$, the algebraic closure is denoted by $\mathbb{Q}^{alg}$. It consists of zeros of monic polynomials of $f(x) \in \mathbb{Q}[x]$.

Thus similarly we can define the *algebraic integers* $\mathbb{Z}^{alg}$ to be the zeros of monic polynomials of $f(x) \in \mathbb{Z}[x]$, which coincides with previous definition of $\mathcal{O}_K$ of quadratic integer rings.

Theorem 5.2.10

If K/E and E/F are algbraci extensions, then K/F is algebraic.

Proof. Let $\alpha \in K$, its minimal polynomial $m_\alpha(x)$ over E is $x^n + c_{n-1}x^{n-1} + \cdots + c_0$. Since each $c_i \in E$ are algebraic over F, and $F(c_0, \ldots, c_{n-1})/F$ is finite, so $F(\alpha, c_0, \ldots, c_{n-1})/F$ is finite. □

§5.3 Splitting fields and normal extensions

Definition 5.3.1. Given a field F and a polynomial $f(x) \in F[x]$ of degree n. A field extension K/F is called a **splitting field** of $f(x)$, if

- $f(x)$ splits completely in $K[x]$, i.e. $f(x) = c(x-\alpha_1)\cdots(x-\alpha_n)$ for $c \in K^\times$, $\alpha_1, \ldots, \alpha_n \in K$.
- $K = F(\alpha_1, \ldots, \alpha_n)$.

Example 5.3.2

$\mathbb{Q}(\sqrt{d})$ is the splitting field of $x^2 - d$.

But if $f(x) = x^3 + Ax + B$, $\mathbb{Q}[x]/(f(x))$ is typically not a splitting field. If $f(x) = x^3 - 2$, then $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ is a splitting field of $f(x)$. Note that it's also a splitting field of the minimal polynomial of $\sqrt[3]{2} + \zeta_3$, which is of degree 6.

Remark 5.3.3 — If E is a finite extension of F inside K and K/F is a splitting field of $f(x) \in F[x]$. Then K is a splitting field of $f(x)$ over E.

Theorem 5.3.4

For any field F and $f(x) \in F[x]$ of degree n, a splitting field K of $f(x)$ over F exists. Moreover $[K : F] \leq n!$.

Proof. Use induction on $\deg f = n$. The case $n = 1$ is trivial.

Suppose the theorem is proved for $1, \ldots, n-1$. Let $p(x)$ be an irreducble factor of $f(x)$.

Then $E := F[x]/(p(x))$ is a field extension of F of degree $\deg p \leq n$ over which $p(x)$ has a zero. Thus $f(x) = (x - \theta) \cdot g(x)$ in $E[x]$, where $\deg g = n - 1$, by induction hypo we're done. (take a splitting field K/E of $g(x)$) □

Example 5.3.5

The splitting field of $x^n - 1$ is $\mathbb{Q}(\zeta_n)$, the n-th cyclotomic field. We'll see later $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.

We can discuss the "uniqueness" of splitting field.

Lemma 5.3.6

If $\eta : F \xrightarrow{\sim} \widetilde{F}$ is an isomorphism of fields, and $p(x) \in F[x]$ irreducible, then $\widetilde{p}(x) := \eta(p(x))$ is irreducible in $\widetilde{F}[x]$. Moreover $F[x]/(p(x)) \xrightarrow{\sim} \widetilde{F}[x]/(\widetilde{p}(x))$.

Proof. Trivial. □

Example 5.3.7

Let $\eta : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ by $a + b\sqrt{2} \mapsto a - b\sqrt{2}$.

Using the lemma we can get

$$\mathbb{Q}\left(\sqrt{5+\sqrt{2}}\right) \simeq \mathbb{Q}\left(\sqrt{2}\right)[x]/\left(x^2 - 5 - \sqrt{2}\right) \xrightarrow{\sim} \mathbb{Q}\left(\sqrt{2}\right)[x]/\left(x^2 - 5 + \sqrt{2}\right) \simeq \mathbb{Q}\left(\sqrt{5-\sqrt{2}}\right).$$

Lemma 5.3.8

Let $\eta : F \xrightarrow{\sim} \widetilde{F}$ be an isomorphism and $f(x) \in F[x]$. If E is a splitting field of $f(x)$ over F, and $\widetilde{E}$ is a splitting field of $\widetilde{f}(x)$ over $\widetilde{F}$.

Then there exists an isomorphism $\sigma : E \to \widetilde{E}$ restricting to $F \to \widetilde{F}$.

Proof. Will prove for the splitting field K constructed earlier, we have the following diagram

$$\begin{array}{ccccc} E & \xleftarrow{\sim} & K & \xrightarrow{\sim} & \widetilde{E} \\ | & & | & & | \\ F & \longleftarrow & F & \longrightarrow & \widetilde{F} \end{array}$$

Claim 5.3.9. If $\eta : F \xrightarrow{\sim} \widetilde{F}$ is an isomorphism, and $\widetilde{E}$ an extension of $\widetilde{F}$ on which $\eta(f(x))$ splits completely. Then η extends to $\sigma : K \to \widetilde{E}$.

Proof. Induction on $\deg f = n$. At each step, since $\eta(p(x))$ has a zero in $\widetilde{E}$, say α.

Thus exists a homomorphism $\sigma_L : L = F[x]/(p(x)) \to \widetilde{E}$ by $x \mapsto \alpha$. Repeating this step we're done. □

By claim we get $\sigma : K \hookrightarrow \widetilde{E}$. Since $\widetilde{f}(x)$ splits in $\sigma(K)$, it must be an isomorphism. □

This lemma tells us that different splitting fields are isomorphic.

Observe that if K/F are extensions, $E, \widetilde{E}$ are intermediate fields which splits a polynomial $f(x) \in F[x]$. Then $E = \widetilde{E}$ because $f(x)$ splits in E as $c(x - \alpha_1)\cdots(x - \alpha_n)$, and in $\widetilde{E}$ as $c'(x - \beta_1)\cdots(x - \beta_n)$. View this in K we know the roots are the same, hence $E = \widetilde{E}$.

Another observation is that, if $K/E/F$ are field extensions, E is a splitting field of some polynomial of $f(x) \in F[x]$, then $\forall$ automorphism $\sigma : K \xrightarrow{\sim} K$ s.t. $\sigma|_F = \mathrm{id}$, we have $\sigma(E) = E$. (because $\sigma(E)$ splits $\sigma(f) = f$.)

An intrinsic definition of splitting field gives normal extensions:

Definition 5.3.10. An algebraic extension K/F is called **normal** if for any irreducible polynomial $f(x) \in F[x]$ that has a zero in K, $f(x)$ splits completely in K.

Theorem 5.3.11

A finite extension K/F is normal if and only if it is the splitting field of some $f(x) \in F[x]$.

Proof. Let $K = F(\alpha_1, \dots, \alpha_r)$ for $\alpha_1, \dots, \alpha_r \in K$. Since the minimal polynomial $m_{\alpha_i}(x) \in F[x]$ splits in K, K is the splitting field of $f(x) = \prod m_{\alpha_i}(x)$.

Conversely, assume that K/F is the splitting field of $f(x) \in F[x]$, if $p(x) \in F[x]$ is an irreducible polynomial that has a zero α in K.

Let L be the splitting field of $p(x)$ over K, hence also the splitting field of $p(x)f(x)$ over F. Let $\beta \neq \alpha$ be another zero of $p(x)$ in L.

$$\exists \eta : F(\alpha) \xrightarrow{\sim} F(\beta), \quad \alpha \mapsto \beta$$

which is an isomorphism s.t. $\eta|_F = \mathrm{id}$. But L is a splitting field of $f(x)p(x)$ over both $F(\alpha)$ and $F(\beta)$, there exists an isomorphism $\sigma : L \xrightarrow{\sim} L$ extending η.

But K/F is a splitting field, $\sigma(K) = K$ by previous observation. In particular $\sigma(\alpha) = \beta \in K$, so $L = K$. □

Corollary 5.3.12

If K/F is finite and normal, then for any intermediate field E, K/E is normal.

Proof. Because K/F is the splitting field of $f(x)$, K/E is the splitting field of the same polynomial. □

Remark 5.3.13 — This does not imply E/F is normal in above theorem, e.g. $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$.

Definition 5.3.14. If K/F is an algebraic extension, a **normal closure** of K/F is a field extension L/K s.t.

- L/F is normal;
- If $L \supseteq L' \supseteq K$ is such that L'/F is normal, then $L = L'$.

Lemma 5.3.15

A normal closure of a finite extension K/F exists and is unique up to (some) isomorphism.

Proof. Existence: say $K = F(\alpha_1, \dots, \alpha_r)$ and $f = \prod m_{\alpha_i}$. Take L to be the splitting field of f over K.

Uniqueness: If L' is another normal closure of K/F. Since $f(x)$ splits completely in L', L is a splitting field of f over K, $\exists L \hookrightarrow L'$. By the minimality we get $L = L'$. □

Remark 5.3.16 — For algebraic extension K/F, we can take the union of all finite normal closures to prove the theorem.

Example 5.3.17

Splitting field of $x^p - t$ over $F = \mathbb{F}_p(t)$.

§5.4 Separable extensions and finite fields

Recall that a field F of $\operatorname{char} F = p > 0$ is perfect if the Frobenius map $\sigma : F \to F, x \mapsto x^p$ is an isomorphism.

The typical non-example is $F = \mathbb{F}_p(t)$, then t cannot written as a p-th power of an element.

Let $K = \mathbb{F}_p(t^{\frac{1}{p}})$, we see that the minimal polynomial of $t^{\frac{1}{p}}$ is $x^p - t$, it factors as $(x - t^{\frac{1}{p}})^p$ in K, so the non-perfectness comes from the multiple roots.

To determine whether a polynomial has multiple roots, we'll make use of the derivatives.

Definition 5.4.1 (Formal derivative)**.** Let F be a field, $f(x) = a_0 + a_1x + \cdots + a_nx^n \in F[x]$ is a polynomial. Define $D(f)(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1}$ to be the **formal derivative** of f.

Note that this formal derivative satisfies Lebniz's law.

If $f(x) = x(x - \alpha_1)^{e_1} \cdots (x - \alpha_r)^{e_r} \in F[x]$ with α_i pairwise distinct, we say α_i is a zero of $f(x)$ with multiplicity e_1.

Just like we do in real or complex numbers, we have:

Theorem 5.4.2

Let $f(x) \in F[x]$ with $\deg f \geq 1$, it has no repeated roots in its splitting field K if and only if $(f(x), D(f)(x)) = (1)$.

Proof. On one hand, since

$$f(x)p(x) + D(f)(x)q(x) = 1 \in K[x]$$

If $(x - \alpha)^2 \mid f(x)$, we have $(x - \alpha) \mid D(f)(x)$, which implies $(x - \alpha) \mid 1$ in $K[x]$, contradiction!

On the other hand, suppose $(d(x)) = (f(x), D(f)(x))$. Therefore $d(x) \mid f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$ with α_i distinct. But $D(f)(\alpha_i) = \prod_{j \neq i}(\alpha_i - \alpha_j) \neq 0$, $d(x)$ must be a constant, i.e. $(d(x)) = (1)$. □

Corollary 5.4.3

If $f(x)$ is an irreducible polynomial in $F[x]$. Then either

- $f(x)$ has repeated roots in its splitting field, this is equivalent to $D(f)(x) = 0$.
- or $f(x)$ has no repeated roots, call f **separable**.

Proof. If $f(x)$ has repeated roots, then $(f(x), D(f)(x)) \neq (1)$. But $f(x)$ irreducible, thus $f(x) \mid D(f)(x)$. However $\deg D(f)(x) < \deg f(x)$, $D(f)(x)$ must be 0. □

Corollary 5.4.4

If $\operatorname{char} F = 0$, all irreducible polynomials are separable. (since they must have nonzero derivatives)

Next let's look at when will the derivative $D(f)(x) = 0$. Clearly, we have

Corollary 5.4.5

If $\operatorname{char} F = p > 0$, and $f(x)$ is inseparable, then $f(x) = g(x^p)$ for some $g \in F[x]$ irreducible.

Moreover, this can happen only when F is imperfect.

Proof. Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ irreducible. When $p \nmid i$, since $D(f)(x) = 0 \implies ia_i = 0 \implies a_i = 0$. Thus $f(x) = g(x^p)$, and g irreducible since f irreducible.

If the field F is perfect, write $a_{ip} = b_i^p \in F$, we can factorize $f(x)$ as

$$\sum a_{ip} x^{ip} = \sum b_i^p x^{ip} = \left(\sum b_i x^i\right)^p.$$

By isomorphism given by Frobenius map. □

Corollary 5.4.6

If $\operatorname{char} F = p > 0$, all irreducible polynomials in $F[x]$ are of the form $f(x) = g(x^{p^e})$ for a separable g. $f(x)$ in its splitting field has $\deg g(x)$ distinct zeros.

Definition 5.4.7. Let K/F be an algbraic extension. Say $\alpha \in K$ is **separable/inseparable** if $m_\alpha(x)$ is separable/inseparable.

Say K/F is a **separable extension** if every element $\alpha \in K$ is separable over F. Otherwise we say this extension is **inseparable**.

Some easy properties: Given a tower of extension $K/E/F$ and $\alpha \in K$. Clearly α is separable over $F \implies \alpha$ is separable over E. (since $m_{\alpha,E}(x) \mid m_{\alpha,F}(x)$)

Theorem 5.4.8

Let $K/E/F$ be field extensions, $\alpha \in K$.

(1) If α is separable over F, then $F(\alpha)$ is a separable extension over F.

(2) If K/E and K/F are both separable, then K/F is separable.

The idea of the proof is that, if K/F is finite and M/F is any normal extension that contains K.

Consider all possible homomorphisms $\varphi : K \to M$ fixing F, denote this set by $\operatorname{Hom}_F(K, M)$.

E.g. $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt[3]{2})$, $M = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$. Then $\varphi : K \to M$ has only 3 choices, $\varphi_0 = \mathrm{id}$, $\varphi_1 : \sqrt[3]{2} \mapsto \sqrt[3]{2}\zeta_3$, $\varphi_2 : \sqrt[3]{2} \mapsto \sqrt[3]{2}\zeta_3^2$. Note that $\#\operatorname{Hom}_F(K, M) = [K : F]$ in this example.

Lemma 5.4.9

Let $K = F(\alpha)$ with $m_{\alpha,F}(x) = g(x^{p^e})$, where $g \in F[x]$ is an irreducible and separable polynomial.

Then $\#\operatorname{Hom}_F(K, M) = \deg g(x) \le [F(\alpha) : F]$. The equality holds iff α is separable.

Proof. Since $\varphi : K \to M$ is determined by $\varphi(\alpha)$, and $m_\alpha(\alpha) = 0 \implies m_\alpha(\varphi(\alpha)) = 0$. Recall that m_α has $\deg g(x)$ distinct roots, we have $\#\operatorname{Hom}_F(K, M) = \deg g(x)$.

Since $[K : F] = \deg m_{\alpha,F} = p^e \deg g(x)$, the latter inequality holds with equailty at $e = 0$, i.e. m_α is separable. □

This lemma provides a different perspective of separablilty.

Corollary 5.4.10

Let K/F be a finite extension, M/F a normal extension containing K, then

$$\#\operatorname{Hom}_F(K, M) \leq [K : F]$$

Moreover the following are equivalent:

(1) $K = F(\alpha_1, \ldots, \alpha_n)$ with each α_i separable over F.

(2) The equality holds.

(3) K/F is separable.

Proof. By our lemma, $\#\operatorname{Hom}_F(F(\alpha_1), M) \leq [F(\alpha_1) : F]$. For each embedding $F(\alpha_1) \hookrightarrow M$, we have

$$\#\operatorname{Hom}_{F(\alpha_1)}(F(\alpha_1, \alpha_2), M) \leq [F(\alpha_1, \alpha_2) : F(\alpha_1)].$$

By induction we get the desired inequality.

The same induction on equality condition gives (1) $\implies$ (2).

For (2) $\implies$ (3), if there exists $\alpha \in K$ inseparable, then $\#\operatorname{Hom}_F(F(\alpha), M) < [F(\alpha), F]$. For each embedding $F(\alpha) \hookrightarrow M$, we have

$$\#\operatorname{Hom}_{F(\alpha)}(K, M) \leq [K : F(\alpha)]$$

Therefore $\#\operatorname{Hom}_F(K, M) < [K : F]$, contradiction!

Since (3) $\implies$ (1) is trivial, we're done. □

Thus the first half of Theorem 5.4.8 is proved.

Proof of (2) of Theorem 5.4.8. Take $\alpha \in K$ with $m_{\alpha,E} = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, $a_i \in E$.

Consider $K' = F(a_{n-1}, \ldots, a_0, \alpha)$, $E' = F(a_{n-1}, \ldots, a_0)$. They are all finite, so if we take M a normal extension over F containing K', for each embedding $E' \hookrightarrow M$,

$$\#\operatorname{Hom}_{E'}(K', M) = [K' : E'] \implies \#\operatorname{Hom}_F(K', M) = [K' : F]$$

Thus K' is separable over F, α is separable over F. □

Theorem 5.4.11 (Primitive element theorem)

A finite separable extension is generated by one element.

Another stronger version is that if $K = F(\alpha, \beta)$ with α, β algebraic over F and β separable over F. Then $K = F(\gamma)$ for some $\gamma \in K$.

Example 5.4.12

Typical non-example when α, β both inseparable:

Let $K = \mathbb{F}_p(x^{\frac{1}{p}}, y^{\frac{1}{p}})$, $F = \mathbb{F}_p(x, y)$. For all $\alpha \in K$, $\alpha^p \in F$, thus $[F(\alpha) : F] \leq p$ but $[K : F] = p^2$.

Proof. The idea is that most $\theta = \alpha + c\beta$ should work. We need to avoid the bad c.

Now assume $\#F = \infty$. Let $f(x), g(x)$ be the minimal polynomials of α, β over F. Let E be the splitting field of $f(x)g(x)$, $\alpha = \alpha_1, \dots, \alpha_r, \beta = \beta_1, \dots, \beta_s$ be the distinct zeros of $f(x)$ and $g(x)$.

Take $c \in F$ so that $\alpha_i + c\beta_1 \neq \alpha_k + c\beta_j$, for all i, k as long as $j \neq 1$. (This rules out finitely many c, so we can always take one)

Set $\theta = \alpha_1 + c\beta_1$, want to solve α, β in $F(\theta)$. Consider $f(\theta - cx)$ and $g(x)$. They have common zero if $\theta - c\beta_j = \alpha_i \iff \alpha_1 + c\beta_1 = \alpha_i + c\beta_j$. But this can only happen when $\beta_j = \beta_1$, i.e. $x = \beta_1$.

Therefore in $E[x]$, $(f(\theta - cx), g(x)) = (x - \beta_1)$. Here we used the fact that $g(x)$ has only simple roots. This implies $(f(\theta - cx), g(x)) = (x - \beta_1)$ in $F(\theta)[x]$ as well (since computing gcd is an algebraic process).

Hence $\alpha, \beta \in F(\theta)$. □

When the field is finite, we prove a stronger result.

Theorem 5.4.13

If F is a finite field, $\operatorname{char} F = p > 0$ for a prime p and $\#F = p^n$ for $n = [F : \mathbb{F}_p]$.

Moreover for each p^n there is a unique field F of p^n elements. It is the splitting field of $x^{p^n} - x \in \mathbb{F}_p[x]$.

Proof. Clearly $\#F = p^n$ since it's a vector space over $\mathbb{F}_p$.

If F is a finite field of p^n elements, $F^\times$ is a finite group of order $p^n - 1$. Hence $\forall a \in F^\times$, $a^{p^n - 1} = 1$, this implies $a^{p^n} - a = 0$, $\forall a \in F$.

But $\#F = p^n = \deg(x^{p^n} - x)$, so F is indeed the splitting field.

Conversely if F is the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$. Note that $D(x^{p^n} - x) = -1$ in F, so it is separable, i.e. has only simple roots in F, there are exactly p^n of them.

We claim that these roots elements form a subfield of F. (Hence equals to F)

$\forall \alpha, \beta$, clearly $\alpha \pm \beta, \alpha\beta, \frac{\alpha}{\beta}$ are all zeros of $x^{p^n} - x$ since $\alpha^{p^n} = \alpha$ and $\beta^{p^n} = \beta$. □

§6 Galois theory

§6.1 Galois groups

Recall: Given a finite field extension K/F and L a normal extension of F containing K. Then $\#\operatorname{Hom}_F(K, L) \leq [K : F]$, and the equality holds if and only if K/F is separable.

Definition 6.1.1 (Galois extensions)**.** We say that an algebraic extension K/F is **Galois** if it is separable and normal. Define

$$\operatorname{Gal}(K/F) := \operatorname{Aut}_F(K) := \{\phi : K \xrightarrow{\sim} K, \phi|_F = \mathrm{id}_F\}.$$

called the **Galois group** of K over F.

Consider the above case with $L = K$. We get that $\#\operatorname{Hom}_F(K, K) = \#\operatorname{Gal}(K/F) = [K : F]$.

Example 6.1.2

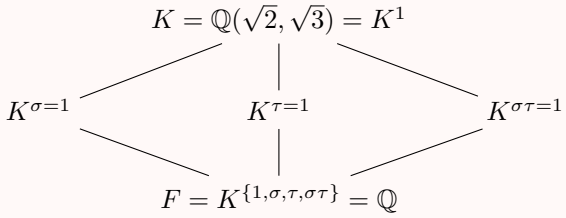
Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ be a *biquadratic extension* of $F = \mathbb{Q}$. Then $\mathrm{Gal}(K/F) = \{1, \sigma, \tau, \sigma\tau\}$, where

$$\sigma : \sqrt{2} \to -\sqrt{2},\ \sqrt{3} \to \sqrt{3},\ \sqrt{6} \to -\sqrt{6}$$
$$\tau : \sqrt{2} \to \sqrt{2},\ \sqrt{3} \to -\sqrt{3},\ \sqrt{6} \to -\sqrt{6}$$
$$\sigma\tau : \sqrt{2} \to -\sqrt{2},\ \sqrt{3} \to -\sqrt{3},\ \sqrt{6} \to \sqrt{6}$$

If we look at the elements which are fixed by σ or τ, we'll get

$$K^{\sigma=1} = \mathbb{Q}(\sqrt{3}), \quad K^{\tau=1} = \mathbb{Q}(\sqrt{2}), \quad K^{\sigma\tau=1} = \mathbb{Q}(\sqrt{6}).$$

Hence they gives the intermediate fields of the extension.



Remark 6.1.3 — If a group H acts on a field K by automorphisms, then $K^H = \{x \in K \mid h(x) = x,\ \forall h \in H\}$ is a subfield.

§6.2 Galois theorem and some examples

Theorem 6.2.1 (Galois Theory)

Let K/F be a finite Galois extension with Galois group $G = \mathrm{Gal}(K/F)$.

(1) There's a one-to-one correspondence between

$$\{\text{intermediate fields } K/E/F\} \longleftrightarrow \{\text{subgroups } H \leq G\}$$
$$K^H \longleftarrow\!\shortmid\ H$$
$$E \shortmid\!\longrightarrow \mathrm{Gal}(K/E)$$

(2) The correspondence is inclusion-reversive: $H_1 \leq H_2 \implies K^{H_1} \supseteq K^{H_2}$.

(3) $\#H = [K : K^H]$, $[G : H] = [K^H : F]$.

(4) If $E \leftrightarrow H$ is a corresponding pair, then $\forall g \in G$, $g(E) \leftrightarrow gHg^{-1}$.

(5) $H \leq G$ is a normal subgroup iff K^H is a normal (and separable) extension of F. In this case $\mathrm{Gal}(K^H/F) \simeq G/H$.

Proof of (2), (3), (4). (2): Clearly $H_1 \leq H_2 \implies K^{H_2} \subset K^{H_1}$, and $E_1 \subset E_2 \implies \mathrm{Gal}(K/E_1) \supseteq \mathrm{Gal}(K/E_2)$.

(3): Since K separable and normal over F, K/K^H is separable and normal. Thus $\#H = \#\operatorname{Gal}(K/K^H) = [K : K^H]$, $\#G\#\operatorname{Gal}(K/F) = [K : F]$, which implies $[G : H] = [K^H : F]$.

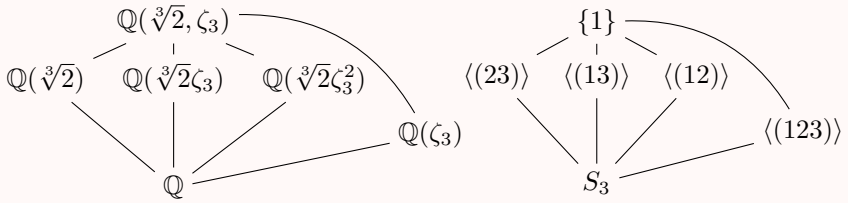
(4):

$$x \in K^{gHg^{-1}} \iff gHg^{-1}x = x \iff Hg^{-1}x = g^{-1}x \iff g^{-1}x \in K^H = E \iff x \in g(E).$$

□

Example 6.2.2

Consider $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$, the splitting field of $x^3 - 2$.



Note that $\langle(123)\rangle \lhd S_3$ and $\mathbb{Q}(\zeta_3)$ is a normal extension of $\mathbb{Q}$.

The elements of S_3 is the permutation of $\sqrt[3]{2}$, $\sqrt[3]{2}\zeta_3$, and $\sqrt[3]{2}\zeta_3^2$.

Proof of (5). If K^H is a normal extension of F, for all automorphism $\sigma : K \to K$ s.t. $\sigma|_F = \mathrm{id}$, σ stabilizes K^H. Hence $\sigma(K^H) = K^H \implies \sigma H \sigma^{-1} = H \implies H \lhd G$.

Conversely, if $f(x)$ is an irreducible polynomial in $F[x]$ that has a zero α in K^H. We want to show that $f(x)$ splits in K^H.

Lemma 6.2.3 (Useful lemma)

If K/F is finite Galois, and $f(x) \in F[x]$ is an irreducible polynomial that splits in K. Assume that α is a root of $f(x)$, then all other zeros of $f(x)$ are exactly $\{\sigma(\alpha) : \sigma \in \operatorname{Gal}(K/F)\}$.

Proof. First, each $\sigma(\alpha)$ is a root of $\sigma(f) = f$.

Now we show $f(x)$ has no other zeros. Let $g(x) = \prod_{\sigma \in \operatorname{Gal}(K/F)}(x - \sigma(\alpha)) \in F[x]$. (Because all coefficients are invariant under $\operatorname{Gal}(K/F)$)

In $K[x]$, $(f, g) \neq (1)$, this implies $(f, g) \neq (1)$ in $F[x]$ as well. But $f(x)$ is irreducible in $F[x]$, thus $f(x) \mid g(x)$, i.e. all zeros of f are contained in $\{\sigma(\alpha)\}$. □

By lemma the roots of α are $\sigma(\alpha)$'s, which all lies in K. Since $\alpha \in K^H$, $\sigma(\alpha) \in K^{\sigma H \sigma^{-1}} = K^H$, by the normality of K^H, which shows that $f(x)$ splits in $K^H[x]$.

As for the quotient group G/H, note that $\sigma(K^H) = K^H$ for all $\sigma \in \operatorname{Gal}(K/F)$,

$$\begin{array}{c} K \\ G\left(\begin{array}{c} |_H \\ K^H \\ | \end{array}\right. \\ F \end{array} \qquad \begin{aligned} \eta : \operatorname{Gal}(K/F) &\longrightarrow \operatorname{Gal}(K^H/F) \\ (\sigma : K \xrightarrow{\sim} K) &\longmapsto \sigma|_{K^H} \end{aligned}$$

This is a homomorphism of group, and $\ker \eta = \{\sigma|_{K^H} = \mathrm{id}\} = H$.

Therefore η induces the injective homomorphism $G/H \hookrightarrow \operatorname{Gal}(K^H/F)$. For the surjectivity, we can simply count the number of elements or by "extensions of automorphism". □

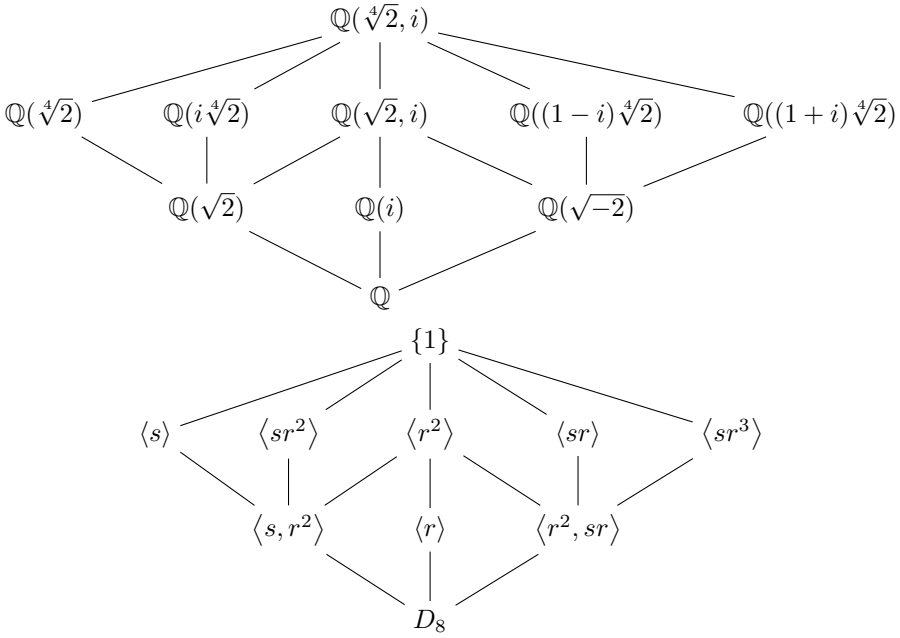
Theorem 6.2.4 (Galois Theory, continued)
Let K/F be a finite Galois extension with Galois group $G = \mathrm{Gal}(K/F)$.

(6) If $E_1, E_2 \leftrightarrow H_1, H_2$, then $E_1E_2 \leftrightarrow H_1 \cap H_2$, $E_1 \cap E_2 \leftrightarrow \langle H_1, H_2\rangle$.

Proof. By definition and the correspondence it's easy to check. □

Remark 6.2.5 (What about non-Galois (separable) extension?) — Slogan: Take a normal closure L/F of K/F. Properties of K/F corresponds to properties of the coset G/H. ($G = \mathrm{Gal}(L/F)$, $H = \mathrm{Gal}(L/K)$)

Example 6.2.6
Let $\theta = \sqrt[4]{2}$, consider the normal closure of $\mathbb{Q}(\sqrt[4]{2})$, i.e. $\mathbb{Q}(i, \sqrt[4]{2}) =: K$.
Let $s : i \mapsto -i, \sqrt[4]{2} \to \sqrt[4]{2}$, $r : \sqrt[4]{2} \to i\sqrt[4]{2}, i \to i$.
We can check that $rsrs = \mathrm{id}$, hence $\mathrm{Gal}(K/\mathbb{Q}) = D_8$.
We can find all the intermediate fields using the subgroups of D_8, note that some intermediate fields are hard to find directly, like $\mathbb{Q}((1-i)\sqrt[4]{2})$.



§6.2.1 Cyclotomic fields

For finite fields, let $q = p^r$, $\mathbb{F}_q$ be the field with q elements. Clearly $\mathbb{F}_{q^n}$ is a normal (separable) extension of $\mathbb{F}_q$. (splitting field of $x^{q^n} - x$.)

Let $\phi_q : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ takes a to a^q. We say the q-Frobenius element is the fixed points of ϕ_q.
Note that

$$\mathbb{F}_{q^n}^{\phi_q=1} = \{x \mid x^q - x = 0\} = \mathbb{F}_{q^m}.$$

Definition 6.2.7 (Abelian extensions)**.** We say a finite extension K/F is **abelian** if K/F is Galois and $\mathrm{Gal}(K/F)$ is abelian.

Let $\mu_n := \langle \zeta_n \rangle \simeq \mathbb{Z}/n\mathbb{Z}$ be the group of n-th roots of unity.
A **primitive n-th root of unity** is a generator of μ_n, i.e. ζ_n^a for some $a \in (\mathbb{Z}/n\mathbb{Z})^\times$.
Define $\Phi_n(x) = \prod_{a \in (\mathbb{Z}/n\mathbb{Z})^\times} (x - \zeta_n^a)$, the n-th cyclotomic polynomial

$$x^n - 1 = \prod_{a \in \mathbb{Z}/n\mathbb{Z}} (x - \zeta_n^a) = \prod_{d \mid n} \Phi_d(x)$$

thus by induction $\Phi_n(x) \in \mathbb{Z}[x]$.

Theorem 6.2.8
$\Phi_n(x)$ is irreducible in $\mathbb{Z}[x]$ and in $\mathbb{Q}[x]$.

Proof. We only need to show $\Phi_n(x)$ is irreducible in $\mathbb{Z}[x]$. Let ζ be a primitive n-th root of unity in the splitting field of $\Phi_n(x)$.
Clearly $m_{\zeta,\mathbb{Q}} \mid \Phi_n(x)$. Let $f(x) := m_{\zeta,\mathbb{Q}}(x)$.

Claim 6.2.9. If p is a prime, $p \nmid n$, then ζ^p is a zero of $f(x)$.

Using this claim we know that every ζ^a is a zero of $f(x)$, $\forall a \in (\mathbb{Z}/n\mathbb{Z})^\times$, since $a = \prod_i p_i^{\alpha_i}$, where $p_i \nmid n$. Therefore the claim would imply the theorem.
Proof of the claim:
Suppose not, let $g(x) := m_{\zeta^p,\mathbb{Q}}(x)$, then $f(x) \neq g(x)$ and $(f, g) = (1)$, so $fg \mid \Phi_n(x)$.
But $g(\zeta^p) = 0 \implies g(x^p)$ has ζ as a zero, $f(x) \mid g(x^p)$. Write $g(x^p) = f(x)h(x)$ for some $h(x) \in \mathbb{Z}[x]$.
Consider this equality modulo p. Since $\overline{g}(x^p) = (\overline{g}(x))^p$ in $\mathbb{F}_p$,

$$(\overline{g}(x))^p = \overline{f}(x)\overline{h}(x).$$

Thus $\overline{f}$ and $\overline{g}$ have a common factor, which means $\overline{\Phi_n}$ has repeated zeros in its splitting field, and so does $x^n - 1$, contradiction! □

Corollary 6.2.10
$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg \Phi_n(x) = \varphi(n)$.

In fact $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$, by $a \mapsto (\varphi_a : \zeta_n \mapsto \zeta_n^a)$.

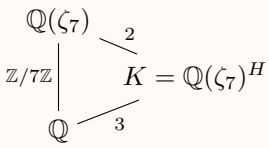
Corollary 6.2.11
For every finite abelian group G, there exists a finite Galois extension K of $\mathbb{Q}$ with Galois group G.

Proof. Write $G = \mathbb{Z}/n_1 \times \ldots \mathbb{Z}/n_r$.
The idea is to find $(\mathbb{Z}/p_i)^\times \twoheadrightarrow \mathbb{Z}/n_i$, (this can be done by choosing $p_i \equiv 1 (\mathrm{mod} n_i)$) then we can find an intermediate field K of $\mathbb{Q}(\zeta_{p_1 \cdots p_r})/\mathbb{Q}$, which corresponds to the kernel of the map $\mathbb{Z}/p_1 \cdots p_r \twoheadrightarrow G$.
Therefore we have $\mathrm{Gal}(K/\mathbb{Q}) = G$. □

Example 6.2.12

Find a cyclic extension of $\mathbb{Q}$ of degree 3. Since $7 \equiv 1 (\mathrm{mod} 3)$, consider $\mathbb{Q}(\zeta_7)$.

Note that the kernel of $(\mathbb{Z}/7)^\times \twoheadrightarrow \mathbb{Z}/3$ is the subgroup $H = \{\pm 1\}$, so $K = \mathbb{Q}(\zeta_7)^H$ is an extension of degree 3, namely $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$.



There is a large theorem related to the abelian extensions, which is the motivation of class field theory:

Theorem 6.2.13 (Kronecker-Weber)

Every finite abelian extension of $\mathbb{Q}$ is contained in some $\mathbb{Q}(\zeta_n)$.

§6.2.2 Proof of Galois Theory

Now we're goning to prove (1) of Theorem 6.2.1, the main result of Galois theory.

Lemma 6.2.14

For K/F finite Galois, we have $\#\operatorname{Gal}(K/F) = [K : F]$.

We'll use this result in the proof.

Since K/F finite normal, K is the splitting field of a separable polynomial $f(x) \in F[x]$, thus K/E is also Galois.

Now by $\operatorname{Gal}(K/E) = [K : E]$, we only need to show that $H \leq G$ implies $\operatorname{Gal}(K/K^H) = H$.

Since $\forall h \in H$, h fixes K^H, $H \leq \operatorname{Gal}(K/K^H)$. It suffices to show

$$\#H \geq \#\operatorname{Gal}(K/K^H) = [K : K^H].$$

(Indeed, if this holds then $H = \operatorname{Gal}(K/K^H)$, conversely given $K/E/F$, $[K : E] = \#\operatorname{Gal}(K/E) = [K : K^{\operatorname{Gal}(E)}]$ and $E \subset K^{\operatorname{Gal}(K/E)}$, so $E = K^{\operatorname{Gal}(K/E)}$.)

There are two proofs of this equation.

Proof 1. By primitive element theorem, $K = K^H(\alpha)$ for some $\alpha \in K$ (K/K^H is finite separable).

Consider the polynomial

$$f(x) = \prod_{h \in H} (x - h(\alpha)).$$

Since every element of $f(x)$ is fixed by H, so $f \in K^H[x]$. Clearly $f(\alpha) = 0$, $m_{\alpha, K^H} \mid f$, so $[K : K^H] \leq \#H$. □

Proof 2. This proof uses Artin's lemma.

Let $H = \{\sigma_1, \ldots, \sigma_n\}$. Let $u_1, \ldots, u_{n+1} \in K$, we want to show they are K^H-linealy dependent.

Consider $(\sigma_i(u_j))_{ij}$, which is a $n \times (n+1)$ matrix in K. The columns $v_1, \ldots, v_{n+1}$ of the matrix are K-linealy dependent.

So there exists r s.t. $v_1, \ldots, v_r$ are K-linearly independent, and $v_1, \ldots, v_{r+1}$ are K-linearly dependent. Say $v_{r+1} = \alpha_1 v_1 + \cdots + \alpha_r v_r$.

Claim. $\alpha_1, \dots, \alpha_r \in K^H$.

Proof of the claim. $\forall \sigma \in H$,

$$\sigma(v_{r+1}) = \sigma(\alpha_1)\sigma(v_1) + \cdots + \sigma(\alpha_r)\sigma(v_r).$$

But note that $\sigma(v_i) = \begin{pmatrix} \sigma\sigma_1(v_i) \\ \vdots \\ \sigma\sigma_n(v_i) \end{pmatrix}$ is a permutation of v_i.

Thus we have

$$v_{r+1} = \sigma(\alpha_1)v_1 + \cdots + \sigma(\alpha_r)v_r.$$

Which implies that $\alpha_j = \sigma(\alpha_j)$, so $\alpha_j \in K^H$. □

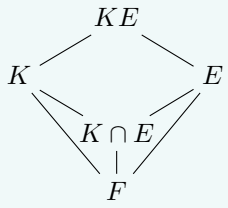
Therefore K as a K^H-vector space is at most n dimensional, which means $[K : K^H] \leq \#H$. □

§6.2.3 Galois theory for composite field

Proposition 6.2.15

Assume K/F is Galois, E/F is any field extension, then KE is a Galois extension of E, and

$$\mathrm{Gal}(KE/E) \cong \mathrm{Gal}(K/K \cap E).$$



Corollary 6.2.16

If K/F finite Galois and E/F finite, then

$$[KE : K \cap E] = [K : K \cap E][E : K \cap E].$$

Remark 6.2.17 — Caveat: K/F Galois is essential to this proposition, since $\mathbb{Q}(\sqrt[3]{2}, \zeta_3) = \mathbb{Q}(\sqrt[3]{2})\mathbb{Q}(\sqrt[3]{2}\zeta_3)$ is an extension of $\mathbb{Q}$ with degree 6, not $3 \times 3 = 9$.

Proof of Proposition 6.2.15. Since K/F finite Galois, K is a splitting field over F of some separable polynomial, so KE is a splitting field over E of the same polynomial, i,e, KE/E is Galois and finite.

Consider $\Psi : \mathrm{Gal}(KE/E) \to \mathrm{Gal}(K/K \cap E)$ by $\sigma \mapsto \sigma|_K$. (Since $K/K \cap E$ is normal, so K is stable under σ-action)

If $\sigma|_K = \mathrm{id}$ and $\sigma|_E = \mathrm{id}$, then $\sigma = \mathrm{id}$, so $\ker \Psi = \{\mathrm{id}_{KE}\}$.

For surjective part, let $H = \mathrm{Im}\, \Psi \subset \mathrm{Gal}(K/K \cap E)$. Consider $K \cap E \subset K^H \subset K$.

Claim. $K^H \subset E$, hence $K^H = K \cap E$.

Note that $\forall \sigma \in \mathrm{Gal}(KE/E)$, $\sigma|_E = \mathrm{id}$, and by definition $\sigma|_{K^H} = \mathrm{id} \implies \sigma|_{K^H E} = \mathrm{id}$.
By Galois theory, EK^H is fixed by entire $\mathrm{Gal}(KE/E)$, thus $EK^H = E \implies K^H \subset E$. □

Proposition 6.2.18

Assume $K_1/F, K_2/F$ are both finite Galois. Then K_1K_2, $K_1 \cap K_2$ are both Galois over F, and

$$\mathrm{Gal}(K_1K_2/F) \cong \{(g_1, g_2) \in \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F) \mid g_1|_{K_1\cap K_2} = g_2|_{K_1\cap K_2}\}$$

In particular, if $K_1 \cap K_2 = F$, $\mathrm{Gal}(K_1K_2/F) \cong \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)$.

The proof is nearly the same as above, i.e. construct a map, check it's injective and calculate the number of elements of both sides.

§6.3 Galois groups of polynomials

We need some preparations before we discuss polynomials.

Definition 6.3.1 (Character)**.** Let H be an abelian group and L be a field. A **character** χ of H with values in L is a group homomorphism $\chi : H \to L^\times$. (In fact this is a 1d representation of H, but this is not helpful)

The main application of characters is when $H = L^\times$, and $\chi = \sigma_i : L \xrightarrow{\sim} L$.

Theorem 6.3.2 (Artin's linear independence of character)

If $\chi_1, \ldots, \chi_n$ are distinct characters of an abelian group H with values in L. Then they are L-linearly independent as functions on H.

Proof. Suppose that they are linearly dependent. Then among all linear relations, there exists one with minimum number of nonzero coefficients, WLOG

$$a_1\chi_1 + a_2\chi_2 + \cdots + a_r\chi_r = 0.$$

Since $\chi_1 \neq \chi_r$, $\exists h_0$ s.t. $\chi_1(h_0) \neq \chi_r(h_0)$.

$$a_1\chi_1(hh_0) + \cdots + a_r\chi_r(hh_0) = a_1\chi_1(h_0)\chi_1(h) + \cdots + a_r\chi_r(h_0)\chi_r(h) = 0$$

Now by looking at the differece we get

$$a_1(\chi_1(h_0) - \chi_r(h_0))\chi_1(h) + \cdots + a_{r-1}(\chi_{r-1}(h_0) - \chi_r(h_0))\chi_{r-1}(h) = 0.$$

Which is a relation with fewer nonzero coefficients, contradiction! □

§6.3.1 Cyclic extensions

Definition 6.3.3 (Cyclic extensions)**.** An extension K/F is called a **cyclic extension** if K/F is Galois and $\mathrm{Gal}(K/F)$ is cyclic.

Proposition 6.3.4

Assume F is a field with

- $\operatorname{char} F \nmid n$.
- F contains all n-th root of unity.

Then $K = F(\sqrt[n]{a})$ for any $a \in F$ is a cyclic extension of degree dividing n.

Proof. Since

$$x^n - a = \prod_{i=1}^{n} (x - \zeta_n^i \sqrt[n]{a})$$

splits completely in K, thus K/F is normal and separable.

Let

$$\lambda : \operatorname{Gal}(K/F) \hookrightarrow \{1, \dots, \zeta_n^{n-1}\} = \mu_n, \quad \sigma \mapsto \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}} = \zeta_n^?$$

Clearly λ is a homomorphism, so $\operatorname{Gal}(K/F)$ is a subgroup of $\mu_n \cong \mathbb{Z}/n\mathbb{Z}$, which must be cyclic. □

Theorem 6.3.5 (Kummer)

If F is a field, such that $\operatorname{char} F \nmid n$, and F contains all n-th roots of unity. Then any cyclic field extension K/F of degree n is of the form $K = F(\sqrt[n]{a})$ for some $a \in F^\times$.

Proof. Let $\operatorname{Gal}(K/F) \simeq \mathbb{Z}/n\mathbb{Z} = \langle \sigma \rangle$.

For $\alpha \in K$, let

$$b := \alpha + \zeta_n \sigma(\alpha) + \cdots + \zeta_n^{n-1} \sigma^{n-1}(\alpha).$$

be the *Lagrange resolvent*.

By linear independence of characters, $1, \sigma, \dots, \sigma^{n-1}$ are characters $K^\times \to K^\times$, so they're independent, i.e. exists α s.t. $b \neq 0$.

Take $a = b^n$, note that $\sigma(b) = \zeta_n^{-1} b$, thus $\sigma(a) = a \implies a \in F$, and b is not contained in any intermediate fields in K/F, which means $K = F(b) = F(\sqrt[n]{a})$. □

Remark 6.3.6 — We can solve any element in K by taking radicals.

§6.3.2 Insolvability of equations of degree 5

Definition 6.3.7. An element $\alpha \in K$ algebraic over F can be **expressed by radicals** or **solved in terms of radicals**, if α belongs to a successive simple extensions

$$F = K_0 \subset K_1 \subset \cdots \subset K_s = K \quad (*)$$

where $K_{i+1} = K_i(\sqrt[n_i]{a_i})$.

Proposition 6.3.8

If an element $\alpha \in K$ can be expressed by radicals, then α is contained in a Galois extension L of F satisfying (*).

Proof. Let L be a Galois closure of K/F. Suppose $\mathrm{Gal}(L/F) = \{1, \sigma_1, \dots, \sigma_r\}$, $L = K_s\sigma_1(K_s)\cdots\sigma_r(K_s)$ satisfies (*). □

Definition 6.3.9. For an irreducible polynomial $f(x) \in F[x]$, its **Galois group** is the Galois group of its splitting field over F.

Theorem 6.3.10

An irreducible polynomial $f(x) \in F[x]$ can be solved by radicals if and only if its Galois group is a solvable group.

Proof. If $f(x)$ can be solved by radicals, then $\exists L/F$ Galois satisfies (*).

Let $F' = F(\zeta_{n_1}, \dots, \zeta_{n_s})$, by Kummer's theory, each $K_{i+i}F'$ is a cyclic extension K_iF', so $G_{i+1} \lhd G_i$ and G_i/G_{i+1} cyclic. Here $G_i = \mathrm{Gal}(L/K_iF')$ and $G = \mathrm{Gal}(L/F)$.

Also $G_0 \lhd G$ and G/G_0 abelian, which means G is solvable.

On the other hand, let K be the splitting field of $f(x)$ over F, $\mathrm{Gal}(K/F)$ solvable. Let

$$\{1\} = H_s \lhd H_{s-1} \lhd H_0 = G$$

such that H_i/H_{i+1} is cyclic.

Let $K_i = K^{H_i}$, $F' = F(\zeta_{\#G})$ is a radical extension.

Now since K'_{i+1}/K'_i is Galois, and $\mathrm{Gal}(K'_{i+1}/K'_i) \hookrightarrow \mathrm{Gal}(K_{i+1}/K_i)$ is cyclic, by Kummer theory, $K'_{i+1} = K'_i(\sqrt[n_i]{a_i})$ is a radical extension for each i, hence $f(x)$ can be solved by radicals. □

Corollary 6.3.11

If an equation has Galois group isomorphic to A_n or S_n with $n \geq 5$, it is not solvable by radicals.

§6.4 Inverse limits

Definition 6.4.1 (Inverse limits (easy version))**.** Consider a sequence of surjective maps of finite sets

$$A_1 \twoheadleftarrow A_2 \twoheadleftarrow A_3 \dots$$

Define

$$\varprojlim_n A_n := \left\{ (a_1, a_2, \dots) \in \prod_n A_n \mid f_n(a_{n+1}) = a_n \right\}.$$

This is called the **inverse limit / projective limit** of the A_i's.

When each A_n has a structure of a group / ring / field, and each f_i is a homomorphism, the inverse limit is a group / ring / field.

Example 6.4.2

Let p be a prime,

$$\mathbb{Z}/p\mathbb{Z} \twoheadleftarrow \mathbb{Z}/p^2\mathbb{Z} \dots$$

where each map is modulo p^n, the inverse limit

$$\varprojlim_n \mathbb{Z}/p^n\mathbb{Z} =: \mathbb{Z}_p$$

the ring of **p-adic numbers**.

For example, $\mathbb{Z}$ can be embedded into $\mathbb{Z}_p$ by $a \mapsto (a \bmod p, a \bmod p^2, \dots)$. When $p = 7$, the number $a = 2$ is invertible in $\mathbb{Z}_7$, since we can solve $2x_n \equiv 1 (\mathrm{mod} p^n)$ for each n.

In fact we have $\mathbb{Z}_p^\times = \{(x_0, x_1, \dots) \mid x_0 \neq 0\}$.

An alternative way to write $x \in \mathbb{Z}_p$ is the infinite sum

$$x = a_0 + a_1 p + a_2 p^2 + \cdots = (a_0, a_0 + a_1 p, a_0 + a_1 p + a_2 p^2, \dots)$$

so x is indeed looks like an integer with base p.

More generally, if $R = \varprojlim_n R_n$, then $R^\times = \varprojlim_n R_n^\times$.

Proof. Let $f_n : R_{n+1} \to R_n$, then $f_n(R_{n+1}^\times) \subset R_n^\times$.

Given $a \in R^\times$, $b = a^{-1} \in R$. Then for all n, $a_n b_n = 1 \in R_n \implies a_n \in R_n^\times$, so $a \in \varprojlim_n R_n^\times$.

Conversely, given $a = (a_n) \in \varprojlim_n R_n^\times$, put $b_n := a_n^{-1} \in R_n$, we need to check $f_n(b_{n+1}) = b_n$.

$$1 = f_n(a_{n+1} b_{n+1}) = a_n f_n(b_{n+1}),$$

by uniqueness of inverses, we know that $f_n(b_{n+1}) = b_n$. □

Example 6.4.3

The formal power series

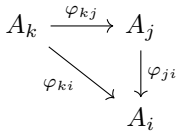
$$\mathbb{C}[[x]] = \varprojlim_n \mathbb{C}[x]/(x^n)$$

can be viewed as "Taylor expansion of a function at $x = 0$", that's why it's called a limit.

More generally, we can define the inverse limit as

Definition 6.4.4. Let I be a poset (partially ordered set), we say that I is **filtered** if $\forall i, j \in I$, $\exists k \in I$ s.t. $k > i$ and $k > j$. (We always assume that I is filtered below)

Suppose that for each $i \in I$, we are given a set/group/ring A_i, and if $j > i$, we have a homomorphism $\varphi_{ji} : A_j \to A_i$ such that if $k > j > i$, the maps are compatible:



We call this an **inverse system**.

Define the **inverse limit**

$$\varprojlim_{i \in I} A_i = \{(a_i)_{i \in I} \mid \varphi_{ji}(a_j) = a_i\} \subset \prod_{i \in I} A_i.$$

If B is a set/group/ring with homomorphisms $\lambda_i : B \to A_i$ such that $\forall j > i$,

$$\begin{array}{ccc} B & \xrightarrow{\lambda_j} & A_j \\ & \searrow^{\lambda_i} & \downarrow{\scriptstyle \varphi_{ji}} \\ & & A_i \end{array}$$

Then there exists a homomorphism $B \to \varprojlim_{i\in I} A_i$, by sending b to $(\lambda_i(b))_{i\in I}$.

Example 6.4.5

Let $\varprojlim_n \mathbb{Z}/n\mathbb{Z} =: \widehat{\mathbb{Z}}$, where the inverse limit is by divisibility, i.e. if $m \mid n$, we have the modulo map $\mathbb{Z}/n\mathbb{Z} \twoheadrightarrow \mathbb{Z}/m\mathbb{Z}$.

In fact we have

$$\widehat{\mathbb{Z}} \simeq \prod_p \mathbb{Z}_p.$$

Let $\varphi_p : \widehat{\mathbb{Z}} \to \mathbb{Z}_p$ by $(a_n) \mapsto (a_{p^r})$, this clearly induces a map $\varphi : \widehat{\mathbb{Z}} \to \prod_p \mathbb{Z}_p$.

Conversely, to construct the map we need compactible family of $\prod_p \mathbb{Z}_p \to \mathbb{Z}/n\mathbb{Z}$ for all n, and this is done by Chinese Remainder Theorem.

Another example is $\mathrm{GL}_N(\widehat{\mathbb{Z}}) = \prod_p \mathrm{GL}_N(\mathbb{Z}_p)$.

Next we can define the topology of inverse limits. Let the topology on A_i be the discrete topology.

- An open subset of A is a union of **basic opens**.

$$\forall i \in I, a_i \in A, \quad \pi^{-1}(a_i) \subset A \text{ is a basic open.}$$

- The inverse limits can be embedded into product space $\prod_{i\in I} A_i$, so the topology can be induced by the product topology.

Above two definitions induces the same topology (not proved here).

Theorem 6.4.6

If each A_i is compact Hausdorff, then $\varprojlim_{i\in I} A_i$ is also compact Hausdorff.

Proof. Since $\prod_{i\in I} A_i$ is compact and Hausdorff by Tychonoff theorem, but $\varprojlim A_i$ is closed ("cut out" by conditions $\varphi_{ji}(a_j) = a_i$), thus it's compact and Hausdorff. □

Definition 6.4.7. A **topological group** is a group G with a topology on the underlying subset, such that $\iota : g \mapsto g^{-1}$ and $m : (g, h) \mapsto gh$ are continuous maps.

Let $U \subset G$ be an open set, then $\forall g, h \in G$, gUh is still open.
If $H \leq G$ is an open subgroup, then H is also closed.

Proof. Let $G = \sqcup g_i H$ be the cosets, since each coset is open, their union $G \setminus H$ is open, thus H is closed. □

If G is a compact group, an open subgroup H is of finite index. (Since the open cover by cosets is disjoint union, the only subcover is itself)

Example 6.4.8

The p-adic numbers has open subgroup $p\mathbb{Z}_p = \pi_1^{-1}(0)$.

$$\mathbb{Z}_p = p\mathbb{Z}_p \sqcup (1 + p\mathbb{Z}_p) \sqcup \cdots \sqcup (p - 1 + p\mathbb{Z}_p)$$

where each component is disconnected with the others, and can be divided into smaller components. Hence $\mathbb{Z}_p$ is a "totally disconnected" space.

If G is a compact group, a closed subgroup of finite index is open. (Again this follows by considering the cosets)

Definition 6.4.9. A **profinite group** is a filtered inverse limit of finite groups, with inverse topology.

Lemma 6.4.10

If G is a profinite group,

$$G \simeq \varprojlim_{H \lhd G \text{ open}} G/H$$

Note that such H forms an inverse system, $H_1, H_2 \lhd G$ implies $H_1 \cap H_2 \lhd G$.

Proof. Obviously $G \to \varprojlim G/H$ is the projection on each component.

Conversely, write $G = \varprojlim_{i \in I} G_i$ with G_i finite, consider $\pi_i : G \to G_i$, $\ker \pi_i \lhd G$ is open (since it's finite). The map

$$\varprojlim_{H \lhd G \text{ open}} G/H \to G/\ker \pi_i \to G_i$$

is compactible as i varies. Hence this induces the desired map.

(Here we didn't check they are inverse maps for simplicity) □

§6.5 Infinite Galois theory

Recall that if K/F is a Galois extension, then

$$K = \bigcup_{E/F \text{ finite Galois}} E.$$

Now we define

$$\mathrm{Gal}(K/F) := \varprojlim_{E/F \text{ finite Galois}} \mathrm{Gal}(E/F).$$

The connecting homomorphism is the natural projection (i.e. the quotient map)

$$\mathrm{Gal}(E_1/F) \twoheadrightarrow \mathrm{Gal}(E_2/F), \quad E_2 \subset E_1.$$

Example 6.5.1

Let $\mathbb{Q}(\mu_{p^\infty}) := \mathbb{Q}(\zeta_{p^r}, r \in \mathbb{N})$. Then

$$\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) = \varprojlim_n \mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}) = \mathbb{Z}_p^\times.$$

Let $\mathbb{Q}(\mu_\infty) := \mathbb{Q}(\mu_n, n \in \mathbb{N})$,

$$\mathrm{Gal}(\mathbb{Q}(\mu_\infty)/\mathbb{Q}) = \varprojlim_n \mathrm{Gal}(\mathbb{Q}(\zeta)n)/\mathbb{Q}) = \widehat{\mathbb{Z}}^\times \simeq \prod_p \mathbb{Z}_p^\times.$$

Lemma 6.5.2

The Galois group is

$$\mathrm{Gal}(K/F) = \{\sigma : K \xrightarrow{\sim} K \mid \sigma|_F = \mathrm{id}_F\}.$$

Proof. Note that for each σ, it induces a compatible family σ_E for each E/F finite Galois.

By definition this is precisely $\varprojlim \mathrm{Gal}(E/F)$.

(There's a topology issue, i.e. $\mathrm{Gal}(K/F)$ acts on K continuously, which is not checked in this course) □

Theorem 6.5.3 (Galois theory for infinite extensions)

Let K/F be a Galois extension. Then there's a 1-to-1 correspondece

$$\{\text{closed subgroups } H \leq \mathrm{Gal}(K/F)\} \longleftrightarrow \{\text{intermediate fields } E \text{ of } K/F\}$$

$$\text{open} \longleftrightarrow E/F \text{ finite}$$

$$\text{normal} \longleftrightarrow E/F \text{ Galois}$$

When H is normal, $\mathrm{Gal}(E/F) \simeq \mathrm{Gal}(K/F)/\mathrm{Gal}(K/E)$.

Remark 6.5.4 — This way we have

$$G = \mathrm{Gal}(K/F) = \varprojlim_{E/F \text{ fin Galois}} \mathrm{Gal}(E/F) = \varprojlim_{H \lhd G \text{ open}} G/H$$

where H can be think of $\mathrm{Gal}(K/E)$.

Lemma 6.5.5

Let G be a profinite group, $H \leq G$ a closed subgroup. For each open $N \lhd G$, put $H_N := \mathrm{Im}(H \to G/N)$. Then

$$H \cong \varprojlim_{N \lhd G \text{ open}} H_N = G \cap \bigcap_{N \lhd G \text{ open}} \pi_N^{-1}(H_N).$$

Note that there's a natural $H_{N'} \to H_N$ if $N' < N$, so H_N forms an inverse system.

Proof. TODO: diagram

We have

$$H \subset \varprojlim_{N \lhd G \text{ open}} H_N \subset G.$$

Suppose this inclusion is strict,

$$H^c \cap \varprojlim H_N \neq \emptyset.$$

Since H^c is open, there exists a basic open $gN' \subset G$, $N' \lhd G$ open such that

$$gN' \cap H = \emptyset, \quad gN' \cap \varprojlim H_N \neq \emptyset.$$

This means that

$$gN' \notin \mathrm{Im}(H \to G/N') = H_{N'}, \quad gn' \in H_{N'},$$

contradiction! □

Proof of Galois theory, part 1. First we check $\mathrm{Gal}(K/K^H) = H$ for each closed subgroup H.

$$\begin{aligned}
\mathrm{Gal}(K/K^H) &= \{\sigma : K \xrightarrow{\sim} K \mid \sigma|_{K^H} = \mathrm{id}\} \\
&= \varprojlim_{E/F \text{ fin Gal}} \mathrm{Gal}(E/E \cap K^H) \\
&= \varprojlim_{E/F \text{ fin Gal}} \mathrm{Gal}(E/E^{\psi_E(H)}) \\
&= \varprojlim_{E/F \text{ fin Gal}} \psi_E(H) = H.
\end{aligned}$$

where $\psi_E : G \to \mathrm{Gal}(E/F)$ by $g \mapsto g|_E$.

Let $N = \ker \psi_E$, then $\psi_E(H) = H_N$, the last equality follows from the lemma. □

Recall that $\mathrm{Gal}(K/F) := \varprojlim_{E/F \text{ fin Gal}} \mathrm{Gal}(E/F)$. We want to compute $\mathrm{Gal}(K/L)$ for an intermediate field L.

$$\begin{aligned}
\mathrm{Gal}(K/L) &= \varprojlim_{L'/L \text{ fin Gal}} \mathrm{Gal}(L'/L) \\
&= \varprojlim_{E/F \text{ fin Gal}} \mathrm{Gal}(LE/L),
\end{aligned}$$

since $\forall L'/L$ finite Galois, there exists E/F finite Galois, such that $L' \subset EL$.

Note that

$$\mathrm{Gal}(LE/L) = \mathrm{Gal}(E/E \cap L) \leq \mathrm{Gal}(E/F).$$

hence $\mathrm{Gal}(K/L) \leq \mathrm{Gal}(K/F)$ as desired.

Proof of Galois theory, part 2. We'll check $L = K^{\mathrm{Gal}(K/L)}$ in this part.

It suffices to check, for finite Galois extension E/F, $L \cap E = K^{\mathrm{Gal}(K/L)} \cap E$.

In fact,

$$K^{\mathrm{Gal}(K/L)} \cap E = E^{\mathrm{Im}(\mathrm{Gal}(K/L) \to \mathrm{Gal}(E/F))} = E^{\mathrm{Gal}(E/E\cap L)} = E \cap L,$$

where the last equality follows from finite Galois theory. □

§6.6 Algebraic closures

Definition 6.6.1. A field extension K/F is called an **algebraic closure** (resp. **separable closure**) if

- K/F is an algebraic (resp. separable) extension.
- Every polynomial (resp. separable polynomial) $f(x) \in F[x]$ splits completely over K.

Denote them by F^{alg} and F^{sep} respectively.

Remark 6.6.2 — F^{alg} contains all splitting fields of F.

Definition 6.6.3. A field K is called **algebraically closed** if all polynomials in $K[x]$ splits completely. (i.e. all irreducible polynomials in $K[x]$ has degree $\leq 1 \iff K$ has no nontrivial algebraic closures)

A field K is called **separably closed** if all nontrivial algebraic extensions of K are inseparable.

Proposition 6.6.4

Let K be a field.

(1) An algebraic (separable) closure of an algebraically (separably) closed field K is just K.

(2) If K is an alg (separable) closure of F, then K is algebraically (separably) closed.

Proof. For (2), suppose α is algebraic over K, consider

$$m_{\alpha,K}(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0, \quad a_i \in K.$$

Since $F(a_0, \ldots, a_{n-1}, \alpha)$ is a finite extension over F, hence algebraic, which implies $\alpha \in K$. □

Theorem 6.6.5 (1) Any field F is contained in an algebraically closed field.

(2) If $F \subset K$ with K algebraically closed,

$$F^{alg} := \{x \in K : x \text{ algebraic over } F\}$$

$$F^{sep} := \{x \in K : x \text{ algebraic and separable over } F\}$$

(3) Algebraic closure is unique up to isomorphisms, but not a canonical isomorphism.

Proof. We skip the proof of (1) since it's too difficult.

(2): Every $f(x) \in F[x]$ splits completely in $K[x]$, and zeros of f is in F^{alg}, thus f splits in $F^{alg}[x]$ i.e. F^{alg} is an algebraic closure of F.

(3): Let F^{alg}, $F^{alg'}$ be two algebraic closures of F. By the fact

$$F^{alg} = \bigcup_{E/F \text{ finte normal}} E,$$

we can extend

$$\eta : F^{alg} \to F^{alg'},$$

but $\eta(F^{alg})$ is algebraically closed, $F^{alg'}/\eta(F^{alg})$ is algebraic, η must be an isomorphism. □

The main object in number theory is to study $\overline{\mathbb{Q}}$, the algebraic closure of $\mathbb{Q}$. We can do this by looking at

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(K/\mathbb{Q})$$

like when $K = \mathbb{Q}(\mu_\infty)$.

§6.7 Transcendence extension

Definition 6.7.1. Let K/F be a field. A subset $\{\alpha_1, \dots, \alpha_n\} \subset K$ is **algebraiccally independent** over F, if there is no nonzero polynomial $f(x_1, \dots, x_n) \in F[x_1, \dots, x_n]$ s.t.

$$f(\alpha_1, \dots, \alpha_n) = 0.$$

This gives rise to an injection

$$\eta : F(x_1, \dots, x_n) \to K, \quad \frac{p(x)}{q(x)} \mapsto \frac{f(\alpha)}{g(\alpha)}.$$

An infinite subset $A \subset K$ is algebraically independent if and only if any finite subset is algebraically independent.

Definition 6.7.2. A **transcendence base** is a maximal algebraically independent subset of K over F. This is equivalent to $K/F(\alpha_1, \dots, \alpha_n)$ is algebraic.

Theorem 6.7.3

The extension K/F has a transcendence base, and any two transcendence bases for K/F have the same cardinality.

Proof. The proof is essentially same as bases in vector spaces.

Existence follows from Zorn's lemma.

Cardinality (finite version) can be proved by

$$\#\{\text{an alg indep set}\} \le \#\{\text{a "transcendent generating set"}\}$$

This is identical with the proof in vector spaces. Let $\{\alpha_i\}$ be an algebraically independent set, $\{\beta_j\}$ be a transcendent generating set (TGS). (Idea: swap the α_i's into $\{\beta_1, \dots, \beta_n\}$ one by one)

WLOG $\alpha_1 \notin \{\beta_j\}$, we need to find $\beta_j \notin \{\alpha_i\}$, such that $\{\alpha_1, \beta_1, \dots, \widehat{\beta_j}, \dots, \beta_n\}$ is a TGS.

Since $\exists f$ s.t. $f(\alpha_1, \beta_i, \dots, \beta_n) = 0$. Then $\exists j \in \{1, \dots, m\}$ s.t. β_j appears in f and $\beta_j \notin \{\alpha_i\}$.

Now $F(\alpha_1, \beta_1, \dots, \beta_n)/F(\alpha_1, \dots, \widehat{\beta_j})$ is an algebraic extension, $K/F(\alpha_1, \dots, \widehat{\beta_j})$ is also algebraic, giving the desired result. □

Definition 6.7.4. The cardinality of transcendence base is called **transcendence degree** of K/F.

Example 6.7.5
$\mathbb{Q}(\pi) \simeq \mathbb{Q}(x)$ has transcendence degree 1.

Remark 6.7.6 — If $\{\alpha_1, \dots, \alpha_n\}$ and $\{\alpha_1', \dots, \alpha_n'\}$ are transcendence bases, in general, $F(\alpha_1, \dots, \alpha_n) \neq F(\alpha_1', \dots, \alpha_n')$.
E.g. $\{x^2\}$ is also a base of $\mathbb{Q}(x)/\mathbb{Q}$.

Definition 6.7.7. An extension K/F is called **purely transcendent** if $K \simeq F(\alpha_1, \dots, \alpha_n)$.

Example 6.7.8 (How to describe transcendent extensions?)
For example $F(x)(\sqrt{x^3 - x})$.

This leads to the basics of *algebraic geometry*. The basic idea is

$$U \subset \mathbb{C}^n \text{ open} \longleftrightarrow \mathcal{O}(U) = \{\text{holomorphic functions on } U\}$$

$$x \in U \longleftrightarrow \mathfrak{m}_x = \{f \in \mathcal{O}(U), f(x) = 0\}.$$

Here $\mathfrak{m}_x = \ker(\mathcal{O}(U) \overset{\text{ev}_x}{\twoheadrightarrow} \mathbb{C})$. Since $\mathcal{O}(U)/\mathfrak{m}_x \simeq \mathbb{C}$, it is a maximal ideal.

Let k is an algebraically closed field, the same thing can be done in k^n and $k[x_1, \dots, k_n]$ replacing U and $\mathcal{O}(U)$.

Theorem 6.7.9 (Hilbert Nullstellensatz (weak form))
Every maximal ideal of $k[x_1, \dots, x_n]$ is of the form $(x_1 - a_1, \dots, x_n - a_n)$ for some $(a_1, \dots, a_n) \in k^n$.

It's tempating to state that there's a bijection between k^n and maximal ideals of $k[x_1, \dots, x_n]$, but there's some problems.

Given $f \in k[x_1, \dots, x_n]$, let

$$Z(f) := \{a \in k^n \mid f \in \mathfrak{m}_a\} = \{a \in k^n \mid f(a) = 0\}.$$

Similarly, let $I = (f_1, \dots, f_m) \subset k[x_1, \dots, x_n]$ be an ideal.

$$Z(I) = \{a \in k^n \mid \forall f \in I, f(a) = 0\} = Z(f_1) \cap \dots \cap Z(f_m).$$

Note that $Z(f^m) = Z(f)$, and $(f) \neq (f^m)$. So we need to use some commutative algebra to get rid of this problem.

§6.7.1 Some commutative algebra

Let R be a commutative ring, I is an ideal. Define its **radical** to be

$$\sqrt{I} = \{f \in R \mid f^n \in I \text{ for some } n \in \mathbb{N}^*\}.$$

Check $\sqrt{I}$ is an ideal:

$$f, g \in \sqrt{I} \implies f^m, g^n \in I \implies (f+g)^{m+n-1} = f^m A + g^n A \in I \implies f+g \in I.$$

$$f \in \sqrt{I}, a \in R \implies f^m \in I \implies a^m f^m \in I \implies af \in \sqrt{I}.$$

Definition 6.7.10. An ideal I is called **radical** if $I = \sqrt{I}$.

Fact: Let $I \subset k[x_1, \ldots, x_n]$ be an ideal, then $Z(I) = Z(\sqrt{I})$. (prove it yourself!)

Theorem 6.7.11 (Hilbert Nullstellensatz (strong form))

There is a bijection between algebraic subsets of k^n (i.e. of the form $Z(I)$) and radical ideals of $k[x_1, \ldots, x_n]$.

$Z \mapsto I(Z) := \{f \in k[x_1, \ldots, x_n] \mid f|_Z = 0\}$.

§6.8 Proof of Hilbert Nullstellensatz

All rings are commutative below.

Recall that for field extensions, finite $\iff$ algebraic and fin gen. We'll do similar things on rings.

Definition 6.8.1. Let $A \subset B$ be a subring, an element $x \in B$ is called **integral** over A if it satidfies an equation

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

for some $a_0, \ldots, a_{n-1} \in A$.

Proposition 6.8.2

The following are equivalent:

(1) x is integral over A.

(2) $A[x] \subset B$ is a finitely generated A-module.

(3) $A[x]$ is contained in a subring C of B s.t. C is a fin gen A-module.

Proof. (1) $\implies$ (2). Note that $x^{n+s} = -a_{n-1}x^{n+s-1} - \cdots - a_0 x^s$, so any element in $A[x]$ can be written as an A-linear combination of $1, x, \ldots, x^{n-1}$, hence $A[x]$ is generated by them.

(3) $\implies$ (1). Assume C is generated by $e_1, \ldots, e_n$ as an A-module.

Consider $xe_j \in C$, let $xe_j = \sum a_{ij}e_i$ (not uniquely, but fix one).

Let $f(x) := \det(xI_n - (a_{ij}))$. Since

$$(e_1, \ldots, e_n)(xI_n - (a_{ij})) = (0, \ldots, 0)$$

multiplying by the adjugate matrix of $xI_n - (a_{ij})$,

$$(e_1, \ldots, e_n)f(x) = (0, \ldots, 0).$$

Hence $e_i f(x) = 0$, but $e_1, \ldots, e_n$ generate C as an A-module, $1 = c_1e_1 + \cdots + c_ne_n \implies f(x) = 0$. □

Corollary 6.8.3

Let $x_1, \dots, x_n$ be elements of B, each integral over A. Then $A[x_1, \dots, x_n]$ is a fin gen A-module.

Corollary 6.8.4

The set C of elements of B integral over A is a subring of B. This C is called the **integral closure** of A in B.

Proof. Given $x, y \in C$, $A[x, y]$ is a fin gen A-module, and $x \pm y, xy \in A[x, y] \implies x \pm y, xy$ are integral over A. □

An example is $A = \mathbb{Z}$, $B = \mathbb{Q}(\sqrt{D})$, then $C = \mathbb{Z}[\sqrt{D}]$ or $\mathbb{Z}[\frac{1+\sqrt{D}}{2}]$, according to whether $D \equiv 1 (\mathrm{mod} 4)$ or not.

If $C = A$, we say A is **integrally closed** in B; If $C = B$, we say B is **integral** over A.

Corollary 6.8.5

If $A \subset B \subset C$ are rings and if B is integral over A, C is integral over B, then C is integral over A.

Proof. Identical with the proofs of algebraic field extensions. □

Corollary 6.8.6

Let $A \subset B$ be a subring, C is the integral closure of A in B, then C is integrally closed in B.

§6.8.1 Noether normalization

Let k be a field, and R is a finitely generated k-algebra, i.e. $R = k[x_1, \dots, x_n]/I$ for some ideal I.

E.g. $\mathbb{Q}[x, x^{-1}] = \mathbb{Q}[x, y]/(xy - 1)$ is a fin gen $\mathbb{Q}$-algebra, but $\mathbb{Q}(x)$ is not.

Theorem 6.8.7

Given a fin gen k-algebra R, there exists $r \leq n$ and an injective homomorphism

$$\varphi : k[y] = k[y_1, \dots, y_r] \hookrightarrow R$$

such that R is integral over $k[y]$.

Proof (Nagata). Induction on n. Suppose theorem proved for $n - 1$, Say $R = k[x_1, \dots, x_n]/I$.

If $I = (0)$, we're done. WLOG $I \neq (0)$, let $f(x) \in I$.

Take positive integers $r_2, \dots, r_n$ and put

$$z_2 = x_2 - x_1^{r_2}, \dots, z_n = x_n - x_1^{r_n}.$$

Then by this substitution, set $\widetilde{f} = f(x_1, x_1^{r_2} + z_2, \dots) \in k[x_1, z_2, \dots, z_n]$, Suppose $1 \ll r_2 \ll \cdots \ll r_n$.

Hence we have $\widetilde{f} = ax_1^N + (\text{terms of degree} < N)$, WLOG $a = 1$. So $k[x_1, z_2, \ldots, z_n]/(\widetilde{f})$ is integral over $k[z_2, \ldots, z_n]$, and it's generated by $1, x_1, \ldots, x_1^{N-1}$.

This implies every element of $k[x_1, z_2, \ldots, z_n]/I$ can be written as

$$h_0(z) + \cdots + h_{N-1}(z)x_1^{N-1}$$

So $k[x_1, z_2, \ldots, z_n]/I$ is a fin gen module over $k[z]/(I \cap k[z])$. Meaning that R is integral over $k[y]$ by induction hypo. □

§6.8.2 Weak form

Lemma 6.8.8

Let R be a field, $S \subset R$ be a subring s.t. R is integral over S. Then S is a field.

Proof. Trivial. □

TODO