Chapter 2

Algebra

2.1 Group Theory

Groups

Let G be a set :

(1) A semigroup is a set with associative : $a(bc) = (ab)c$ (an abelian semigroup if $ab = ba$) .

(2) A monoid is a semigroup with identity : $ae = ea = a$.

(3) A group is a monoid with inverse : $a^{-1}a = aa^{-1} = e$.

Subgroups

$H < G$. $\iff$ For any $a, b \in H$, one has $ab \in H$, $a^{-1} \in H$.

$\iff$ For any $a, b \in H$, one has $a^{-1}b \in H$.

If $H \neq \{e\}$ or G , then it is a proper subgroup.

Proposition

(1) For subgroups (or normal subgroups) $N_i < G$, $\bigcap\limits_{i \in I} N_i$ is a subgroup (or normal subgroup) of G .

(2) If H and K are subgroups of G , then $H \cup K$ is not subgroup generally.
The subgroup $< H \cup K >= H + K$ is called generated by subgroups H , K .

Lagrange Theorem

Let G be a finite group, $H < G$ be a subgroup of G , define $G/H = \{gH \mid g \in G\}$ (G/H is not a group generally) and $[G : H] = |G/H| = |G| \ / \ |H|$.

One has $|H| = |gH| = |g^2H| = \cdots = |g^mH|$ and $|G| = \sum\limits_{i=1}^{m} |g^iH| = m \cdot |H| = [G : H] \cdot |H|$.
($|gH| = |Hg|$ for any $g \in G$.)

Proposition

(1) If $K < H < G$ are three finite groups, then $[G : K] = [G : H] \cdot [H : K]$.

(2) For two subgroups $H < G$, $N < G$, one has : $HN = NH$. $\iff$ $HN < G$.
($HN = \{hn \mid h \in H, n \in N\}$ is not a group generally.)

(3) For two finite subgroups $H < G$, $N < G$, $H \cap N$ is a subgroup of H and N , by the Lagrange Theorem one has,

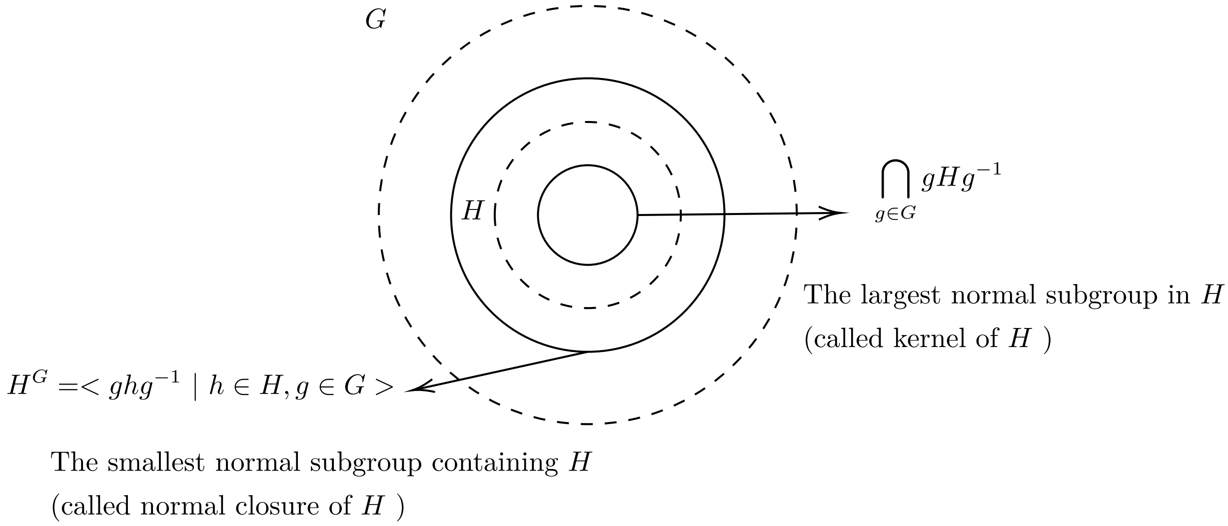
$$\frac{|H|}{|H \cap N|} = m = [H : H \cap N] \text{ with } H = \coprod_{i=1}^{m} a_i(H \cap N)$$

where either $a_iN = a_jN$ or $a_iN \cap a_jN = \emptyset$, then $\dfrac{|HN|}{|N|} = m$, $\dfrac{|HN|}{|N|} = \dfrac{|H|}{|H \cap N|}$.

Normal subgroups

N is a normal subgroup of G , $N \lhd G$. $\Longleftrightarrow \forall\, g \in G$, $gN = Ng$.

If N is a normal subgroup, G/N is not only a set but also a group, the identity is $eN = N$, the inverse of gN is $g^{-1}N$.



Proposition

For a normal subgroup $N \lhd G$ and a subgroup $K < G$:

(1) $N \lhd N + K$.

(2) $N \lhd KN = N + K = NK$.

(3) If $K \lhd G$ such that $N \cap K = \{e\}$, then $nk = kn$ for all $k \in K$, $n \in N$.

(4) If $N \subseteq K$, then $K/N < G/N$.

One has : K/N is normal. $\Longleftrightarrow$ K is normal.

The first isomorphism theorem for groups

Let $f : G \longrightarrow G'$ be a homomorphism, then one has

$$G/\mathcal{K}er(f) \cong \mathcal{I}m(f) \ , \ \mathcal{K}er(f) \lhd G \ , \ \mathcal{I}m(f) < G \ .$$

$\mathcal{I}m(f)$ is not a normal subgroup in general.

One has $|G| = |\mathcal{I}m(f)| \cdot |\mathcal{K}er(f)|$, $|\mathcal{I}m(f)| \mid |G'|$.

The second isomorphism theorem for groups

Let $N \lhd G$, $H < G$, then one has

$$H \cap N \lhd H \ , \ N \lhd HN \ , \ HN/N \cong H/(H \cap N) \ .$$

HN is a group because N is a normal subgroup.

The third isomorphism theorem for groups

Let M, N be normal subgroups of G with $N \subseteq M$, then one has

$$N \lhd M \ , \ M/N \lhd G/N \ , \ (G/N)/(M/N) \cong (G/M) \ .$$

Proposition

(1) $N \lhd G \ . \iff \forall \ g \in G \ , \ gN = Ng \ .$
$\iff \forall \ g \in G \ , \ gNg^{-1} = N \ .$
$\iff \forall \ g \in G \ , \ n \in N \ , \ gng^{-1} \in N \ .$

(2) For an abelian group G , the subgroup of G is always a normal subgroup.

(3) $\mathrm{SL}_n(\mathbb{R}) \lhd \mathrm{GL}_n(\mathbb{R})$, $\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R}) \cong (\mathbb{R}^\times, \cdot)$.

(4) For $n \in \mathbb{Z}$, one has $n\mathbb{Z} \lhd \mathbb{Z}$. The subgroup of a cyclic group is always a normal subgroup.
For a finite cyclic group $\mathbb{Z}_n$ and every $m|n$, one has a unique cyclic subgroup $< [\frac{n}{m}] >$ with order m .

(5) The automorphism group $\mathrm{Aut}(C)$ of a cyclic group C is an abelian group.
For an infinite cyclic group, $\mathrm{Aut}(C) \cong \mathbb{Z}_2$.
For a finite cyclic group, $\mathrm{Aut}(C_n) \cong \mathbb{Z}_n^\times \cong \mathbb{Z}_{\varphi(n)}$.
The order of the group $\mathbb{Z}_n^\times$ is $\varphi(n)$ (the Euler-φ function) .

(6) The squares of the elements of $\mathbb{Z}_4$ are just 0 and 1 , this concludes that the equation $a^2 + b^2 = 3c^2$ has no solution in $\mathbb{N}^+$.

(7) $G = \{z \in \mathbb{C} \mid z^n = 1, n \in \mathbb{Z}\}$ is a group under the multiplication but not a group under the addition.

Permutation groups

Define $S_\Omega = \mathrm{Perm}(\Omega) = \{\sigma \mid \sigma \colon \Omega \longrightarrow \Omega \text{ is a bijection}\}$, $(S_\Omega, \circ)$ is a permutation group.
Take $\Omega = \{1, 2, \cdots, n\}$, denote : $S_n = \mathrm{Perm}(\Omega) = \{\sigma \mid \sigma \colon \{1, 2, \cdots, n\} \longrightarrow \{1, 2, \cdots, n\} \text{ is a bijection}\}$.

Any permutation in S_n is a unique product of disjoint cycles.
The order of a permutation is the least common multiple of the orders of disjoint cycles.

Proposition

(1) For $n \geq 5$, A_n is a simple gruop.

(2) For $n \geq 3$, A_n is generated by 3-cycles $\{(abc) \mid c \neq a, b\}$ where distinct $a, b \in \{1, 2, \cdots, n\}$ have been given.

(3) For $n \geq 3$, if the normal subgroup $N \lhd A_n$ ($n \geq 3$) contains a 3-cycle, then $N = A_n$.

Direct products

For groups G_i , $i \in I$, define $\prod\limits_i G_i = \{(g_1, \cdots, g_n, \cdots) \mid g_i \in G_i\}$ ($\sum\limits_i G_i$ if the operation is additive) to be the direct product. Define the direct sum (or weak direct product) $\bigoplus\limits_i G_i$ to be a subgroup of $\prod\limits_i G_i$ where $\bigoplus\limits_i G_i = \{(g_1, \cdots, g_n, \cdots) \mid g_i \in G_i\ ,\ g_i = 0 \text{ almost everywhere}\}$.

Free groups

For a set X , the free group $F(X)$ is a free object in $(\mathbf{Gp})$ on the set X , then for any $f : X \longrightarrow G$ mapping to any group G , the unique induced morphism $\widetilde{f} : F(X) \longrightarrow G$ makes the diagram commutes.

There is an at-first-glance paradoxical fact : the infinitely generated free group can be a subgroup of the finitely generated free group.

$$
\begin{tikzcd}
F(X) \arrow[r, dashed, "\widetilde{f}"] & G \\
X \arrow[u, "\text{generated}"] \arrow[ur, "f"'] \arrow[ur, phantom, "\circlearrowleft", near start, shift left=3ex]
\end{tikzcd}
$$

Every group is the homomorphism image of a free group.

Free abelian groups

An abelian group (using the additive notation for abelian groups) F is a free abelian group if one of the following equivalent conditions holds :

(1) F has a nonempty basis X .

(2) $F \cong \bigoplus\limits_i \mathbb{Z}$ ($\prod\limits_{i=1}^{\infty} \mathbb{Z}$ is not free) .

(3) F is a free object in $(\mathbf{Ab})$.

For two bases X , X' of an abelian group, one has $|X| = |X'|$ (also if infinite) which is the rank of F .

Every abelian group $< X \mid R >$ is the homomorphism image of a free abelian group of rank $|X|$.

Proposition

For a free abelian group F with basis $\{x_1, \cdots, x_n\}$ and a nonzero subgroup $G < F$, there exist positive integrals $d_1 | d_2 | \cdots | d_r$ with $r \leq n$ such that G is free abelian with basis $\{d_1 x_1, \cdots, d_r x_r\}$.

Finitely generated abelian groups

Every finitely generated abelian group is isomorphic to a finite direct sum of cyclic groups in which the finite cyclic groups are with order $d_1, \cdots, d_r$ (called the invariant factors) such that $d_1|d_2|\cdots|d_r$ ($d_1 > 1$) .

Every finitely generated abelian group is isomorphic to a finite direct sum of cyclic groups of which is infinite or with order a power of a prime (called the elementary divisors) .

These two finite direct sum compatible since $\mathbb{Z}_{pq} \cong \mathbb{Z}_q \oplus \mathbb{Z}_p$ (also $\mathbb{Z}_{pq}^\times \cong \mathbb{Z}_q^\times \oplus \mathbb{Z}_p^\times$) if $(p, q) = 1$.

Proposition

(1) For a finitely generated abelian group with order n (or $p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$) , it has a subgroup with order m (or p_i^x) for every $m|n$ (or $x|k_i$) .

(2) For a finitely generated abelian group G , $G \cong \bigoplus_{i=1}^{r} \mathbb{Z}_{d_i} \oplus F$ where F is free abelian.

$\mathrm{T}(G) = \bigoplus_{i=1}^{r} \mathbb{Z}_{d_i}$ is the torsion subgroup of G . If $\mathrm{T}(G) = G$, then G is a torsion group. If $\mathrm{T}(G) = 0$ (the additive notation) , then G is torsion-free.

(3) Finitely generated abelian groups $H \cong G$. $\Longleftrightarrow$ $G/\mathrm{T}(G)$ has the same rank with $H/\mathrm{T}(H)$.

Indecomposable groups

An indecomposable group G is not $\{e\}$ or the direct product of two proper subgroups (a simple group is indecomposable but indecomposable group not must be simple) .

Ascending chain condition

A group G is said to satisfy the ascending condition on subgorups (or normal subgroups) if for every chain of subgroups (or normal subgroups) $G_1 < G_2 < \cdots$, there is a k such that $G_k = G_{k+1} = \cdots$.

Descending chain condition

A group G is said to satisfy the descending condition on subgorups (or normal subgroups) if for every chain of subgroups (or normal subgroups) $G_1 > G_2 > \cdots$, there is a k such that $G_k = G_{k+1} = \cdots$.

Proposition

(1) Every finite group satisfies both the ascending chain condition and the descending chain condition.

(2) If a group G satisfies the ascending chain condition or the descending chain condition on normal subgroups, then G is the direct product of a finite number of indecomposable subgroups.

Normal endomorphisms

A endmorphism f of a group is called a normal endomorphism if $af(b)a^{-1} = f(aba^{-1})$ ($\mathcal{I}m(f)$ is a normal subgroup of G) .

Proposition

(1) Group G satisfies the ascending chain condition on normal subgroups and f is an endomorphism, then one has : $f \in \mathrm{Aut}(G)$. $\Longleftrightarrow f$ is an epimorphism.

(2) Group G satisfies the descending chain condition on normal subgroups and f is a normal endomorphism, then one has : $f \in \mathrm{Aut}(G)$. $\Longleftrightarrow f$ is a monomorphism.

Fitting Theorem

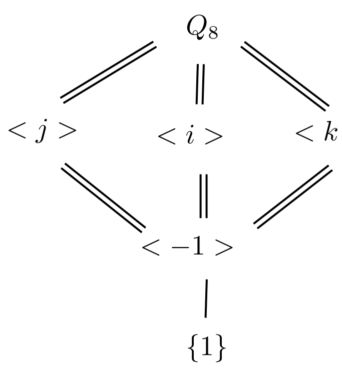
Let G be a group satisfying both the ascending and descending chain conditions on normal subgroups, for the normal endomorphism f , there exists a k such that $G = \mathcal{I}m(f^k) \times \mathcal{K}er(f^k)$.

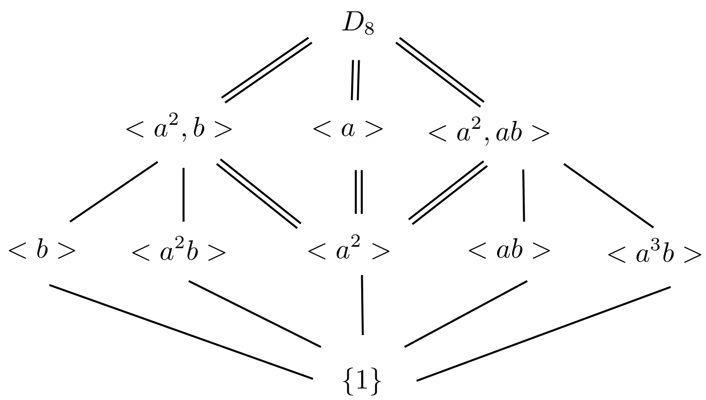
If G is indecomposable, then one has $\mathcal{K}er(f^k) = \{e\}$ or $\mathcal{I}m(f^k) = \{e\}$. Thus $\mathcal{I}m(f^k) = \{e\}$, f is nilpotent or $\mathcal{K}er(f^k) = \{e\} \Longleftrightarrow f \in \mathrm{Aut}(G)$.

Krull-Schmidt Theorem

Let G be a group satisfying both the ascending and descending chain conditions on normal subgroups, if $G = G_1 \times G_2 \times \cdots \times G_s$ and $G = H_1 \times H_2 \times \cdots \times H_t$ with each indecomposable G_i , H_i , then one has :
$s = t$, $G_i \cong H_i$ after reindexing.

Lattice





One has $Q_8 / < -1 > \cong D_8 / < a^2 >$ (the double line component) , even through $< a^2 > \cong < -1 >$, Q_8 and D_8 are not isomorphic.

Group action

A group action of G on X is a function $\phi : G \times X \longrightarrow X$ such that $e \cdot x = x$, $(ab) \cdot x = a \cdot (bx)$.
The kernel of this action is $\mathcal{K}er(\phi) = \{g \mid g \cdot x = x \text{ for all } x \in X\}$ (it is not normal in general.)

Orbit of x : $\mathrm{Orb}(x) = \{x' \in X \mid x' = g \cdot x \ , \ g \in G\}$.
Stabilizer of x : $G_x = \{g \mid g \cdot x = x\}$, also called isotropy group, subgroup fixing x .

$$\text{Translation} : \begin{cases} \text{a subgroup } H < G \text{ acts on } G \text{ by } h \cdot g = hg \ . \\ \text{a subgroup } H < G \text{ acts on the set of cosets } \{g_i K\} \text{ by } h \cdot g_i K = hg_i K \ . \end{cases}$$

$$\text{Conjugation} : \begin{cases} \text{a subgroup } H < G \text{ acts on } G \text{ by } h \cdot g = hgh^{-1} \ . \\ \text{a subgroup } H < G \text{ acts on the set of subgroups } \{K_i \mid K_i < G\} \text{ by } h \cdot K_i = hK_i h^{-1} \ . \end{cases}$$

Proposition

(1) If for all $x \in X$, the stabilizer $G_x = \{e\}$, then this group action is free.
If there is an $x \in X$ such that the stabilizer $G_x \neq \{e\}$, then this group action is not free.

(2) If $\mathcal{K}er(\phi) = \{e\}$, then this group action is faithful.

(3) If $\mathcal{K}er(\phi) = G$, then this group action is trivial.

(4) If there is only one orbit of X then this group action is transitive.

(5) Either $\mathrm{Orb}(x) = \mathrm{Orb}(x')$ or $\mathrm{Orb}(x) \cap \mathrm{Orb}(x') = \emptyset$.

Conjugation on elements

For conjugation

$$G \times G \longrightarrow G \ , \ h \cdot g = hgh^{-1} \ ,$$

the orbit $\mathrm{Orb}(x)$ of x is called the conjugate class of x ,
the stabilizer G_x of x is called the centralizer of x denoted by $C_G(x)$,
the kernel of group action is called the center of G denoted by $C_G(X)$ and it is normal and abelian.

For conjugation

$$H \times G \longrightarrow G \ , \ h \cdot g = hgh^{-1} \ ,$$

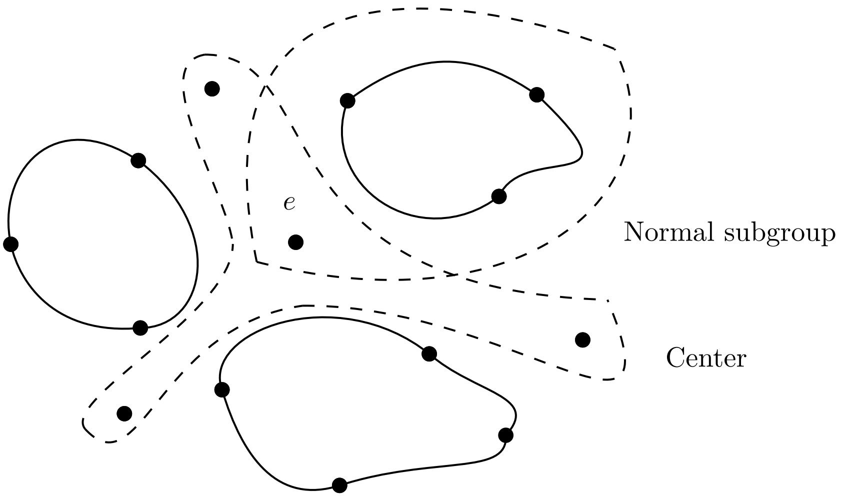
the stabilizer H_x of x is called the centralizer of x in H denoted by $C_H(x)$,
the kernel of group action is called the centralizer of G in H denoted by $C_H(G)$ and it is normal and abelian.

One has

$$C_H(x) = C_G(x) \cap H \ , \ C_H(X) = C_G(X) \cap H \ .$$

Structure of group

Consider the conjugation on elements :



Conjugacy classes in S_5

Partition of 5	Representative of conjugacy class
$1,1,1,1,1$	$\mathbb{1} = (1)(2)(3)(4)(5)$
$1,1,1,2$	$(45) = (1)(2)(3)(45)$
$1,1,3$	$(345) = (1)(2)(345)$
$1,4$	$(2345) = (1)(2345)$
5	(12345)
$1,2,2$	$(23)(45) = (1)(23)(45)$
$2,3$	$(12)(345) = (12(345)$

The elements with same (disjoint) cycle type are conjugate.

Conjugations on subgroups

For conjugation

$$G \times \{\text{subgroups of } G\} \longrightarrow \{\text{subgroups of } G\}\ ,\ h \cdot K = hKh^{-1}\ ,$$

the stabilizer of K is called the normalizer of K denoted by $N_G(K)$ (one has $N_G(G) = G$) .

For conjugation

$$H \times \{\text{subgroups of } G\} \longrightarrow \{\text{subgroups of } G\}\ ,\ h \cdot K = hKh^{-1}\ ,$$

the stabilizer of K is called the normalizer of K in H denoted by $N_H(K)$.

Proposition

(1) The subgroup K is normal in subgroup $N_G(K)$.

(2) The subgroup K is normal in G . $\Longleftrightarrow N_G(K) = G$.

Orbit-stabilizer Theorem

For a group action of G on X , take $x \in X$, then there is a bijection from G/G_x (not a group generally) to $\text{Orb}(x)$, thus we have $|G| = |G_x| \cdot |\text{Orb}(x)|$ if G is finite.

Proposition

(1) The number of the conjugacy classes (as a orbit of conjugation) of x is $[G : G_x] = [G : C_G(x)]$.

(2) If $\text{Orb}(x_1), \cdots, \text{Orb}(x_n)$ are distinct conjugacy classes of G , then $|G| = \sum\limits_n [G : G_{x_i}] = \sum\limits_n [G : C_G(x_i)]$.

(3) The number of subgroups conjugate to K is $[G : N_G(K)]$.

Proposition

(1) Every group action of G on X induces a homomorphism $G \longrightarrow S_X$ where S_X is the permutation group.

(2) The conjugation on G for each g induces an automorphism $G \longrightarrow S_G$ called inner automorphism. And $\text{Inn}(G) \cong G/C_G(G)$.

Cayley Theorem

For a group G , there is a monomorphism $G \longrightarrow S_G$.
Hence every group is isomorphic to a permutation group.
If $|G| = n$, then G is isomorphic to a subgroup of S_n .

Transitive permutation representations

For a subgroup $H < G$, take $\Omega = G/H = \{H, g_1H, \cdots, g_nH\}$, the group action $g \cdot g_iH = gg_iH$ of G on G/H is transitive and it is called the permutation representation of G on the subgroup H and $\mathcal{K}er(\phi) = \bigcap\limits_{g \in G} gHg^{-1}$.

Poincaré Argument

For a finite G , $H < G$ and $[G : H] = n$, then $|G/\mathcal{K}er(\phi)| = |G/(\bigcap\limits_{g \in G} gHg^{-1})|$ is a factor of $(n!, |G|)$.
One has $G/\mathcal{K}er(\phi) \cong \mathcal{I}m(\phi) < S_n$ by the Cayley Theorem.
If p is the smallest prime factor of $|G|$, then for subgroup $H < G$ satisfying $[G : H] = p$, then $H \lhd G$.

Frattini Argument

For a group action G on X , if the subgroup $N < G$ acts transitively on X , then one has $G = G_x N = \{gn \mid g \cdot x = x, n \in N\}$ for all $x \in X$.

Sylow Theorem

For a finite group G , if $|G| = p^n$ where p is prime, then G is a p-group.
If $|G| = p_1^{n_1} \cdot p_2^{n_2} \cdots p_k^{n_k}$ and $H < G$, $|H| \; |p_i^{n_i}$, then H is a p_i-subgroup.

(1) The Sylow p_i-subgroup (the p_i-subgroup with order $p_i^{n_i}$) of G always exists.
(2) Any two Sylow p_i-subgroups $P_1, P_2 \in \mathrm{Syl}_p(G)$ are conjugate.
(3) There are n_{p_i} Sylow p_i-subgroups in G and $n_{p_i} | \; |G|$, $n_{p_i} \equiv 1 (mod \; p_i)$.
(4) There are $n(p_i^{k_i})$ subgroups which are p_i-subgroup in G and $n(p_i^{k_i}) \equiv 1 (mod \; p_i)$.

Proposition

(1) B is a p-subgroup of finite group G , for a Sylow p-subgroup P , if $BP = PB$, then $B < P$.

(2) For the intersection of all the Sylow p-subgroups P_i of finite group G , denote $O_p(G) = \bigcap_i P_i$. $O_p(G)$ is the largest normal p-subgroup of G which means any normal p-subgroup is in $O_p(G)$. Moreover, $O_p(G)$ char G .

(3) If P is the only one subgroup with order n , then $P \lhd G$.
If $P \in \mathrm{Syl}_p(G)$ and $P \lhd G$, then $n_p = 1$ and P char G .

(4) For a finite p-group G , M is the largest subgroup of G , then $[G : M] = p$ and $M \lhd G$.

(5) For a finite p-group G with $|G| > 1$, the order of centre $|C_G(G)| > 1$.

(6) The subgroups, quotient groups and diret products of solvable groups are still solvable.
The finite p-group is solvable.

(7) For the prime p, q , the group G with order pq or $p^2 q$ is solvable.

Characteristic subgroups

For any automorphism $\alpha \in \mathrm{Aut}(G)$, if for a subgroup H , one has $\alpha(H) \subseteq H$, then H is a characteristic subgroup of G , denoted by H char G . In particular, for every $\alpha \in \mathrm{Inn}(G)$, if $\alpha(H) \subseteq H$, then $H \lhd G$.

If H char K , K char G , then H char G . If H char K , $K \lhd G$, then $H \lhd G$. But $H \lhd K$, $K \lhd G$ do not imply $H \lhd G$.

Trivially $\{e\}$, G and $C_G(G)$ are characteristic subgroups of G , if the only characteristic subgroups of G are $\{e\}$ and G , then G is a characteristic simple group.

N/C Theorem

Let $K < G$, then $N_G(K)/C_G(K)$ is isomorphic to a subgroup of $\mathrm{Aut}(K)$.

Composition series

$\{e\} = G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_{r-1} \lhd G_r = G$ is called a composition series of G where G_i/G_{i+1} is simple called the composition factor of G .

Jordan-Hölder Theorem

Suppose there are two composition series of G , $\{e\} = G_0 \lhd G_1 \lhd \cdots \lhd G_r = G$ and $\{e\} = H_0 \lhd H_1 \lhd \cdots \lhd H_s = G$, then $r = s$ and the composition factors are isomorphic with the other.

Proposition

Let G be a finite group, then :

G is solvable.

$\Longleftrightarrow$ The composition factors are all cyclic group with prime order.

$\Longleftrightarrow$ The composition factors are all Abelian.

Semi-products

For a normal subgroup N and a subgroup K of G , if $N \cap K = \{e\}$, then one can construct a semi-product $N \rtimes_f K$ with $|G| = |N \rtimes_f K|$ by :

considering the conjugation of K on the set N , $f : K \times N \longrightarrow N$ induces an automorphism $f : K \longrightarrow \mathrm{Aut}(N)$ given by $k \cdot h = khk^{-1} = f(k)(h)$,

the multiplication is $(h_1, k_1)(h_2, k_2) = (h_1(k_1 \cdot h_2), k_1k_2) = (h_1(k_1h_2k_1^{-1}), k_1k_2)$.

Hölder Theorem

Let $n, m \geq 2$, G is the extension of $N \cong \mathbb{Z}_n$ by $K \cong \mathbb{Z}_m$.

$\Longleftrightarrow G =< a, b \mid a^n = 1, b^m = a^t, ba^r = ab >$ where $r^m \equiv 1(mod\ n)$, $t(r-1) \equiv 0(mod\ n)$.

Groups with order 30

$|G| = 30 = 2 \cdot 3 \cdot 5$. If G is Abelian, then $G \cong \mathbb{Z}_{30}$.

By the Sylow theorem :

The number of Sylow 2-subgroups in G is $1, 3, 5, 15$. The number of Sylow 3-subgroups in G is $1, 10$. The number of Sylow 5-subgroups in G is $1, 6$.

For $P \in \mathrm{Syl}_3(G)$, $Q \in \mathrm{Syl}_5(G)$, if they are neither normal, then there are 20 nonidentity elements with order 3 and 24 nonidentity elements with order 5 , this makes a contradiction.

Then one of P , Q must be normal.

One has P char PQ and Q char PQ , since $PQ \lhd G$, then $P \lhd G$ and $Q \lhd G$.

One has $P \times Q \cong \mathbb{Z}_{15}$ is normal in G .

$G \cong \mathbb{Z}_{15} \rtimes_f \mathbb{Z}_2$ where $f : \mathbb{Z}_2 \longrightarrow \mathrm{Aut}(\mathbb{Z}_{15}) \cong \mathrm{Aut}(\mathbb{Z}_5) \times \mathrm{Aut}(\mathbb{Z}_3)$.

Considering the element with order 2 in $\mathrm{Aut}(\mathbb{Z}_5) \times \mathrm{Aut}(\mathbb{Z}_3)$, there are three elements :

$$\begin{cases} a \longmapsto a^{-1} \\ b \longmapsto b \end{cases} , \begin{cases} a \longmapsto a \\ b \longmapsto b^{-1} \end{cases} , \begin{cases} a \longmapsto a^{-1} \\ b \longmapsto b^{-1} \end{cases} \quad \text{described as three automorphisms on } \mathbb{Z}_{15} \text{ .}$$

(1) For $k \in \mathbb{Z}_2$, $kak^{-1} = k \cdot a = a^{-1} = a^4$, $G = < a, k \mid a^5 = 1, k^2 = 1, ak = ka^4 > \times \mathbb{Z}_3 = D_{10} \times \mathbb{Z}_3$.

(2) For $k \in \mathbb{Z}_2$, $kbk^{-1} = k \cdot b = b^{-1} = b^2$, $G = < b, k \mid b^3 = 1, k^2 = 1, bk = kb^2 > \times \mathbb{Z}_5 = D_6 \times \mathbb{Z}_5$.

(3) For $k \in \mathbb{Z}_2$, $n \in \mathbb{Z}_{15}$, $knk^{-1} = n^{-1} = n^{14}$, $G = < n, k \mid n^{15} = 1, k^2 = 1, nk = kn^{14} >= D_{30}$.

2.2 Rings and Ideals

Rings

$$(R,+,\cdot) \text{ is a ring} \Longleftrightarrow \begin{cases} (a+b)+c=a+(b+c) \\ a+0=0+a=a \\ a+(-a)=(-a)+a=0 \\ a+b=b+a \end{cases} \quad \text{and} \begin{cases} (ab)c=a(bc) \\ (a+b)\cdot c=ac+bc \\ a\cdot(b+c)=ab+ac \end{cases} .$$

Suppose $(I,+)$ is a subgroup of $(R,+)$, $(I,+)<(R,+)$,
if $\forall\ a\in I$, $r\in R$, one has $ar\in I$, $ra\in I$, then I is a ideal of ring $(R,+,\cdot)$, denoted by $I\lhd R$.

$\forall\ x\in(R,+,\cdot)$, $xR=\{xr \mid r\in R\}$ is a ideal of R , called principal ideal, denote $xR=<x>$.
If every ideal of ring R is a principal ideal, then R is a PIR (principal ideal ring) .

Ring homomorphisms

$$f:R\longrightarrow S \text{ is a ring homomorphism.} \Longleftrightarrow \begin{cases} \text{As Abelian group}:\ f(r_1+r_2)=f(r_1)+f(r_2)\ ,\ f(0_r)=0_s \\ \text{With multiplication}:\ f(r_1\cdot r_2)=f(r_1)\cdot f(r_2) \\ \text{If } R \text{ has identity } \mathbb{1}_r : f(\mathbb{1}_r)=\mathbb{1}_s \end{cases}$$

If S is a subring of R , then for $s_1,s_2\in S$, $s_1\cdot s_2$, s_1+s_2 , $s_1-s_2\in S$.
If R has identity $\mathbb{1}$, then for the subring S , $\mathbb{1}\in S$.

Proposition

(1) The polynomial ring $\mathbb{F}[x]$ is a domain and also a principal ideal domain.

(2) For any $p_1(x),\cdots,p_n(x)\in\mathbb{F}[x]$,
the ideal $<p_1(x),\cdots,p_n(x)>=\{r_1\cdot p_1+\cdots+r_n\cdot p_n \mid r_i\in R\}=<\gcd(p_1(x),\cdots,p_n(x))>$.

(3) $u\in R$ is a unit. $\Longleftrightarrow$ exist $u^{-1}\in R$ such that $u\cdot u^{-1}=\mathbb{1}$. $\Longleftrightarrow$ $<u>=R$.

(4) a and b are associate. $\Longleftrightarrow$ exist a unit $u\in R$, such that $a=ub$. $\Longleftrightarrow$ $<a>=<b>$.

(5) r divides s . $\Longleftrightarrow$ $s=xr$. $\Longleftrightarrow$ $r\mid s$. $\Longleftrightarrow$ $<s>\subseteq<r>$.

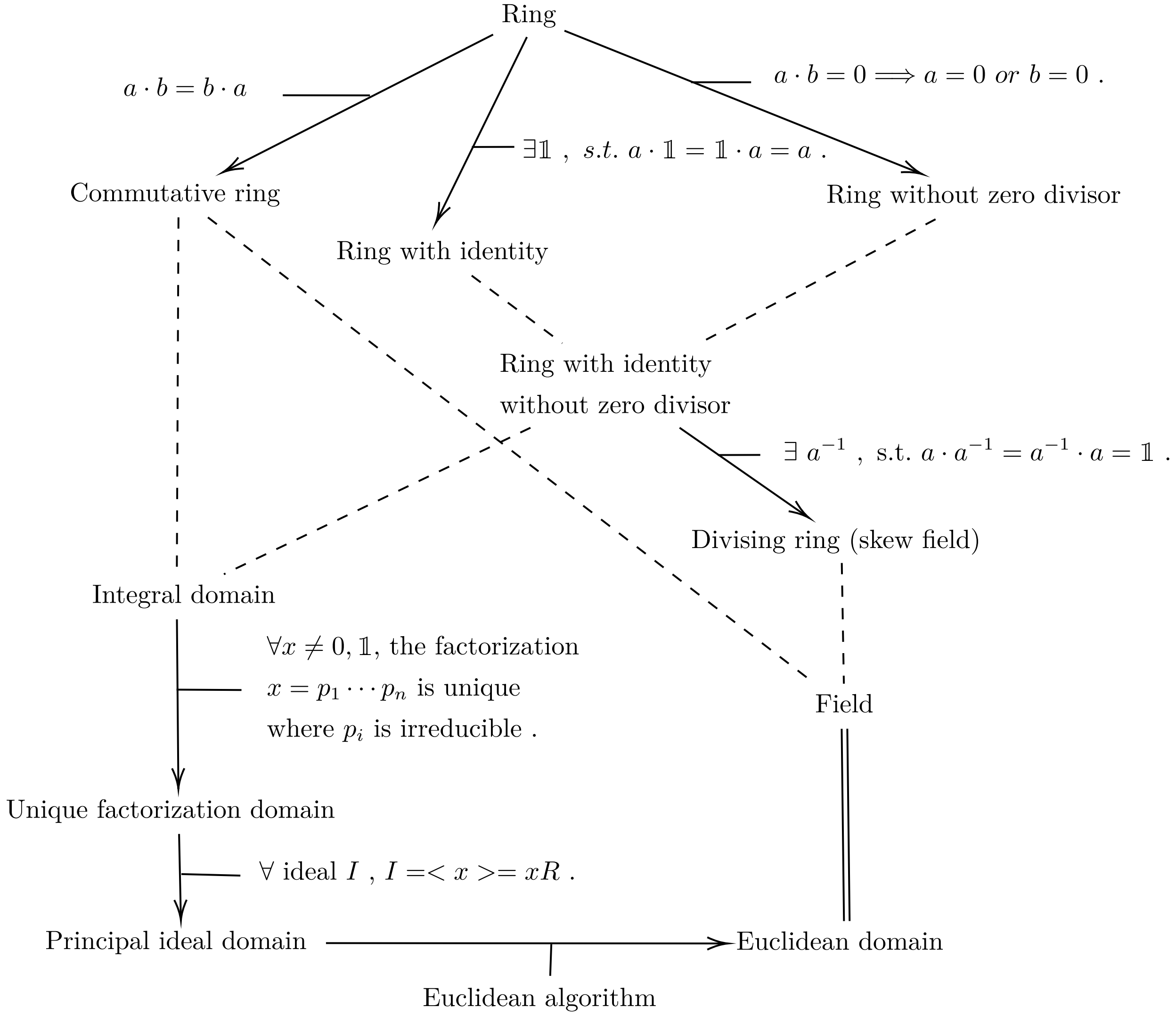
If x is not a unit , then $<s>\subsetneqq<r>$.

Characteristic of ring

For a ring R with $\mathbb{1}$, if c is the minimum positive integer (or $c=0$)such that $c\cdot\mathbb{1}=0$, then c is the characteristic of R . If F is a field, then the characteristic c is either 0 or a prime p .

From rings to fields

In a commutative ring with identity,
if $p \neq 0, \mathbb{1}$ is a prime element, then $p \mid a \cdot b \Longrightarrow p \mid a$ or $p \mid b$.
if $c = ab$ is an irreducible element, then $a = \mathbb{1}$ *or* $b = \mathbb{1}$.



Ring with zero divisor : the matrices ring $M_n(\mathbb{R})$.

Division ring : the quaternions ring $\mathbb{H}$ where
$\mathbb{H} = \{a + bi + cj + dk \mid i^2 = j^2 = k^2 = -1, ij = k, jk = i, ki = j, ji = -k, kj = -i, ik = -j\}$.

Integral domain : $\mathbb{Z}[\sqrt{-3}]$ where $4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$ and $2, 1 + \sqrt{-3}, 1 - \sqrt{-3}$ are irreducible.

UFD : the polonomial ring on integrals $\mathbb{Z}[x]$, it is not a PID .

Proposition

(1) For ideals $I \lhd R$ and $J \lhd R$, $I + J = \{i + j \mid i \in I \ , \ j \in J\}$ is an ideal and $I + J =< I \cup J >$.

(2) For ideals $I \lhd R$ and $J \lhd R$, $I \cap J$ is also an ideal, but IJ is not an ideal in general.

(3) For ideals $I \lhd R$ and $J \lhd R$, if $I \subseteq J$, then $I/J = \{i \mid iJ \subseteq I\}$ is an ideal.

Radicals of ideals

For an ideal $J \lhd R$, the radical of J is :

$$\sqrt{J} = \{f \mid f \in R \ , \ f^k \in J \text{ for some } k \in \mathbb{N}\} \ ,$$

and it is also an ideal.

For an ideal J , if $\sqrt{J} = J$, then J is a radical ideal. Trivially, the radical of an ideal is a redical ideal.

Reduced rings

The ideal $\sqrt{0} = \{a \mid a^k = 0 \text{ for some } k\}$ is called nilradical of R , the element in $\sqrt{0}$ is called nilpotent. If $\sqrt{0} = 0$ (the zero ideal is radical) , then R is a reduced ring.

Proposition

(1) The ideal $I \lhd R$ is radical. $\Longleftrightarrow$ R/I is reduced.

(2) For two ideals I and J , one has $IJ \subseteq I \cap J$ and $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

(3) Two ideals $I \lhd R$, $J \lhd R$ are called coprime if $I + J = R$, then one has $IJ = I \cap J$.

(4) If $I_1, \cdots, I_n$ are pairwise coprime, then one has $I_1 \cdots I_n = I_1 \cap \cdots \cap I_n$.

The Chinese Remainder Theorem

For ideals $I_1, \cdots, I_n$ of R , there is a homomorphism $f : R \longrightarrow R/I_1 \times \cdots \times R/I_n$, $a \longmapsto (a_1, \cdots, a_n)$, then one has :

(1) f is injective. $\Longleftrightarrow$ $I_1 \cap \cdots \cap I_n = 0$.

(2) f is surjective. $\Longleftrightarrow$ $I_1, \cdots, I_n$ are pairwise coprime which means $I_i + I_j = R$ for $i \neq j$.

Prime ideals

$P \lhd R$ is an ideal with $P \neq R$, for any $a, b \in R$, if $ab \in P$ implies $a \in P$ or $b \in P$, then P is called a prime ideal.

The set of all the prime ideals of R is called the prime spectrum of R , denoted by $\mathrm{Spec}(R)$.

Maximal ideals

If the only one ideal containing M is R itself where $M \lhd R$ and $M \neq R$, then M is called a maximal ideal.

The set of all the maximal ideals of R is called the maximal spectrum of R , denoted by $\mathrm{MaxSpec}(R)$.

Proposition

(1) For a ring R with identity, one has : R/M is a field. $\Longleftrightarrow$ M is a maximal ideal.

(2) For a ring R with identity, one has : R/I is an integral domain. $\Longleftrightarrow$ I is a prime ideal.

(3) For a commutative ring R with identity, every maximal ideal of R is a prime ideal, every prime ideal of R is a radical ideal.

(4) For a PID (principal ideal domain) R , the nonzero prime ideal is a maximal ideal.

(5) For ideals $I \subseteq J$ of a ring R , one has :
J is radical, prime or radical in R . $\Longleftrightarrow$ J/I is radical, prime or radical in R/I .

Contractions and extensions of rings

Let $f : R \longrightarrow R'$ be a ring homomorphism.

(1) For $I \lhd R'$, the inverse image $f^{-1}(I)$ is an ideal of R called the inverse image ideal of I or the contraction of I by f .

(2) For $I \lhd R$, the ideal $< f(I) >$ generated by $f(I)$ is an ideal of R' called the image ideal of I or the extension of I of f , also written as $f(I) \cdot R'$.

Localizations of rings

A set $S \subseteq R$ is called multiplicatively closed if $\mathbb{1} \in S$ and $ab \in S$ for all $a, b \in S$.

For a a multiplicatively closed set S , define an equivalent relation on $R \times S$ by $(r, s) \sim (r', s')$ if there is a $u \in S$ such that $u(rs' - r's) = 0$. Denote this class by $(r, s) = \frac{r}{s}$, $S^{-1}R = \{\frac{r}{s} \mid r \in R \ , \ s \in S\}$ is called the localization of R at S .

Hilbert's Basis Theorem

If R is a Noeitherian ring, then so is the polynomial ring $R[x]$.

2.3 Galois Theory

Proposition

(1) For the finite field $\mathbb{F}_p = \mathbb{Z}_p$, the characteristic of $\mathbb{F}_p$ is p .

(2) The integral domain $\mathbb{F}_p[x]$ of polynomials with coefficient $\mathbb{F}_p$ has characteristic p .

(3) For a field F , the polynomial ring $F[x]$ is an integral domain, the field

$$F(x) = \{\frac{f(x)}{g(x)} \mid f(x), g(x) \in F[x], g(x) \neq 0\}$$

is called the field of rational functions.
Trivially, $F \subseteq F(x)$ is a subfield of $F(x)$.

(4) For a field homomorphism $f : F \longrightarrow F'$, if f is not injective, then it must be 0 .

Pime subfields

The subfield generated by $\mathbb{1}$ is the smallest subfield of F containing $\mathbb{1}$.
The prime subfield of field F is the subfield generated by $\mathbb{1}$.
If char $F = 0$, then it is $\mathbb{Q}$. If char $F = p$, then it is (isomorphic to) $\mathbb{F}_p$.

Extension fields

If F is a subfield of K , then K is an extension field of F (F is called the base field) , this extension is denoted by K/F . Trivailly, every field F is an extension field of its prime subfield.

For extension K/F , K is a vector space over field F , the dimension is denoted by $[K : F]$. The extension is finite if and only if $[K : F]$ is finite. For K/E and E/F one has $[K : F] = [K : E][E : F]$.

Simple extensions

For extension K/F , for $\alpha, \beta, \cdots \in K$, the smallest field containing both F and $\alpha, \beta, \cdots \in K$ is denoted by $F(\alpha, \beta, \cdots)$.

For a single element $\alpha \in K$, $F(\alpha)$ is celled a simple extension (field) of F (also can think of $F[\alpha]$ a simple extension of F as a domain) . α is celled a primitive element for this extension.

Eisenstien Argument

For $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Q}(x)$:
if there is a prime p such that $p \nmid a_n$, $p | a_{n-1}, \cdots , a_1$, $p^2 \nmid a_0$, then $f(x)$ is irreducible in $\mathbb{Q}(x)$.

Algebraic and transcendental elements

Suppose there is an extension K/F . If $u \in K$ could be a root of some nonzero $p(x) \in F[x]$, then u is an algebraic element over F . Otherwise, u is a transcendental element over F .

Proposition

Suppose there is an extension K/F :

If $u \in K$ is a transcendental element over F , then one has $K(u) \cong K(x)$.

If $u \in K$ is an algebraic element over F , then :

(1) $F(u) = F[u]$.

(2) $\{\mathbb{1}, u, \cdots, u^{n-1}\}$ is a basis of the vector space $F(u)$ over field F .

(3) $[F(u) : F] = n$.

(4) $F(u) \cong F[x]/ < p(x) >$ where $p(x) \in F[x]$ is an irreducible monic polynomial of degree n , which is uniquely determined by $p(u) = 0$ and $f(u) = 0$ for all $p(x)|f(x)$ in $F[x]$.

The irreducible monic polynomial in (4) is called the minimum polynomial of u , its degree deg $p(x) = [F(u) : F] = n$.

Isomorphisms between simple extensions

For a field isomorphism $f : F \longrightarrow F'$, u is an element of an extension of F , v is an element of an extension of F' .

(1) u is transcendental over F , v is transcendental over F' .

(2) u is a root of an irreducible polynomial $p(x) \in F[x]$, $f : p(x) \longmapsto p'(x)$, v is a root of an irreducible polynomial $p(x) \in F[x]$.

(u is algebraic over F , v is algebraic over F' .)

Then one has : either (1) or (2) implies $F(u) \cong F'(v)$ given by $u \longmapsto v$.

Proposition

If F is a field and $p(x) \in F[x]$ a polynomial of degree n . Then there is a simple extension $F(u)$ of F such that :

(1) u is a root of $p(x)$.

(2) $[F(u) : F] \leq n$.

(3) $p(x)$ is irreducible. $\Longrightarrow$ $F(u)$ is unique up to an isomorphism which is identity on F .

(4) $p(x)$ is irreducible. $\Longleftrightarrow$ $[F(u) : F] = n$.

Algebraic extensions

If K/F is a finite extension, then K is finitely generated and algebraic (all elements are algebraic) over F . For $\alpha, \beta, \cdots \in K$, $F(\alpha, \beta, \cdots)$ is an algebraic extension of F if $\alpha, \beta, \cdots$ are all algebraic over F .

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

If $\alpha, \beta, \cdots \in K$ are exactly all the algebraic elements over F in K , then the set $\{\alpha, \beta, \cdots\}$ is the subfield of K (this subfield is algebraic over F) .

F-homomorphism

For a field homomorphism $f : K \longrightarrow E$ between two extensions K/F , E/F of F , if f is not 0 , it must be injective, then $f : \mathbb{1}_K \longmapsto \mathbb{1}_E$ (they are both $\mathbb{1}_F$) .

If $f : K \longrightarrow E$ is a field homomorphism, then one has :

$f : K \longrightarrow E$ is a F-module homomorphism. $\Longleftrightarrow f|_F = \mathbb{1}_F$.

If a field homomorphism $f : K \longrightarrow E$ is also a F-module homomorphism (it satisfies $f|_F = \mathbb{1}_F$) , then $f : K \longrightarrow E$ is called a F-homomorphism. If $K = E$, f is an field automorphism, then $f : K \longrightarrow E$ is called a F-automorphism. All the F-automorphism of K form the Galois group of K over F , denoted by $\mathrm{Aut}_F(K)$.

Proposition

(1) For an extension K/F and a polynomial $p(x) \in F[x]$, if $u \in K$ is a root of $p(x)$ and $f : K \longrightarrow K$ is a K-homomorphism, then $f(u)$ is also a root of $p(x)$.

(2) For an extension K/F , E is an intermediate field, $F \subseteq E \subseteq K$, $H < \mathrm{Aut}_F(K)$ is a subgroup, one has :
the fixed field $H' = \{k \mid f(k) = k, f \in H, k \in K\}$ of H is an intermediate field, $F \subseteq H' \subseteq K$,
$E' = \mathrm{Aut}_E(K) = \{f \mid f \in \mathrm{Aut}_F(K), f|_E = \mathbb{1}_E\}$ is a subgroup of Galois group $\mathrm{Aut}_F(K)$.

(3) If the fixed field of $\mathrm{Aut}_F(K)$ is F and $F \subseteq K$, then K/F is celled a Galois extension of F , K is Galois over F .

(4) $\mathbb{C}$ is Galois over $\mathbb{R}$, $\mathbb{Q}(\sqrt{3})$ is Galois over $\mathbb{Q}$.
If F is an infinite field, then the simple extension $F(x)$ is Galois over F .

Fundamental Theorem of Galois Theory

For a finite Galois extension K/F , there is an one-to-one correspondence between all intermediate fields of this extension and all subgroups of Galois group $\mathrm{Aut}_F(K)$ such that :

(1) $[\mathrm{Aut}_E(K) : \mathrm{Aut}_{E'}(K)] = [E' : E]$.

(2) E' is Galois over E . $\Longleftrightarrow$ $\mathrm{Aut}_E(K) \lhd \mathrm{Aut}_{E'}(K)$.

(Thus K is Galois over every E .)

$$\begin{array}{rcl} \{e\} = \mathrm{Aut}_K(K) & \longleftrightarrow & K \\ \mathrm{Aut}_{E'}(K) & \longleftrightarrow & E' \\ \mathrm{Aut}_E(K) & \longleftrightarrow & E \\ \mathrm{Aut}_F(K) & \longleftrightarrow & F \end{array}$$

Splitting fields

For a field F , $f(x) = u_0(u_1 - x) \cdots (u_n - x)$ is called a splitting polynomial in $F[x]$ where $u_i \in F$.

$K = F(u_1, \cdots, u_n)$ where $u_i \in F$ are all roots of $f(x)$ in K is called a splitting field of the splitting polynomial $f(x) \in F[x]$.

Algebraic closures

A field K is algebraically closed.

$\Longleftrightarrow$ There is no algebraic extension of K except itself.

$\Longleftrightarrow$ Every nonconstant polynomial in $K[x]$ has a root in K .

$\Longleftrightarrow$ Every nonconstant polynomial in $K[x]$ is splitting over K .

$\Longleftrightarrow$ Every nonconstant irreducible polynomial in $K[x]$ has degree 1 .

$\Longleftrightarrow$ There is a subfield $F \subseteq K$ such that K is algebraic over F and every polynomial $f(x) \in F[x]$ is splitting in $K[x]$.

Proposition

(1) The splitting fields of same polynomials over F are F-isomorphism.

Thus every field F has a unique algebraic closure up to F-isomorphism.

(2) For a field isomorphism $\sigma : F \longrightarrow F'$, $S = \{f_i\}$ are polynomials in $F[x]$, $S' = \{\sigma(f_i)\}$ are polynomials in $F'[x]$:

if K is a splitting field over F of S , K' is a splitting field over F' of S' , then one has $K \cong K'$.

Separable and normal extensions

For an irreducible polynomial $f(x) \in F[x]$, in a splitting field of F if every root of $f(x)$ is a simple root, then $f(x)$ is separable.

For an algebraic extension K/F , the element $u \in K$ is separable if its minimum polynomial is separable, if all the elements in K are separable, then K/F is a separable extension.

For an algebraic extension K/F , if every irreducible polynomial $f(x) \in F[x]$ that has a root in K is splitting in $K[x]$, then K/F is a normal extension.

Proposition

(1) Every algebraic extension of an infinite field F is separable.

(2) The algebraic extension K/F is Galois over F .
$\Longleftrightarrow$ K/F is separable and K is a splitting field over F of some polynomials in $F[x]$.
$\Longleftrightarrow$ K is a splitting field over F of some separable polynomials in $F[x]$.

(3) The algebraic extension K/F is normal over F .
$\Longleftrightarrow$ K is a splitting field over F of some polynomials in $F[x]$.
$\Longleftrightarrow$ If $\overline{F}$ is an algebraic closure of F and $F \subseteq K \subseteq \overline{F}$, then for F-homomorphism $f : K \longrightarrow \overline{F}$, one has $\mathcal{I}m(f) = K$.

(4) For the algebraic extension K/F :
K/F is Galois. $\Longleftrightarrow$ K/F is separable and normal.
K is infinite :
K/F is Galois. $\Longleftrightarrow$ K/F is normal.

Normal closures

For an algebraic extension K/F , N is a normal closure of K , then :
(1) N is normal over F .
(2) No proper subfield of N containing K is normal over F .
(3) If K/F is separable, then N/F is Galois.
(4) $[N : F]$ is finite. $\Longleftrightarrow$ $[K : F]$ is finite.
(5) N is unique up to K-isomorphism.

Galois groups of polynomials

For a field F and a splitting polynomial $f(x) \in F[x]$ with splitting field K , the group $\mathrm{Aut}_F(K)$ is the Galois group of $f(x)$.

Proposition

For a Galois group $\mathrm{Aut}_F(K)$ of irreducible polynomial $f(x) \in F[x]$, one has :

(1) $\mathrm{Aut}_F(K)$ is isomorphic to a subgroup of S_n .

(2) If $f(x)$ is separable of degree n , then $n|\ |\mathrm{Aut}_F(K)|$ and $\mathrm{Aut}_F(K)$ is isomorphic to a transitive subgroup of S_n .

Discriminants of polynomials

For a field with char $F \neq 2$, a polynomial $f(x) \in F[x]$ of degree n with n distinct roots $u_1, \cdots, u_n$ in a splitting field, the discriminant of $f(x)$ is $D = \Delta^2 = (\prod\limits_{i<j}(u_i - u_j))^2$.

Both Δ and D are in this splitting field.

For each $\sigma \in \mathrm{Aut}_F(K) < S_n$:

σ is even. $\Longleftrightarrow \sigma(\Delta) = \Delta$.

σ is odd. $\Longleftrightarrow \sigma(\Delta) = -\Delta$.

Proposition

(1) $f(x) \in F[x]$ is an irreducible polynomial of degree 2 with Galois group $\mathrm{Aut}_F(K)$. If $f(x)$ is separable, then $\mathrm{Aut}_F(K) \cong \mathbb{Z}_2$. otherwise, $\mathrm{Aut}_F(K) = \{e\}$.

(2) $f(x) \in F[x]$ is an irreducible and separable polynomial of degree 3 with Galois group $\mathrm{Aut}_F(K)$. $\mathrm{Aut}_F(K)$ is either A_3 or S_3 .
If char $F \neq 2$, then : $\mathrm{Aut}_F(K) \cong A_3$. $\Longleftrightarrow D(f)$ is the square of an element in F .

(3) For a field F with char $F \neq 2, 3$, if $f(x) = x^3 + bx^2 + cx + d \in F[x]$ has three distinct roots in slitting field, then $g(x) = f(x - \frac{1}{3}b)$ has the form $x^3 + px + q$ and $D(f) = -4p^3 - 27q^2$.

(4) For an $f(x) \in \mathbb{Q}[x]$ of degree prime p , if $f(x)$ has precisely two roots in $\mathbb{C}$, then the Galois group $\mathrm{Aut}_{\mathbb{Q}}(K)$ of $f(x)$ is isomorphic to S_p .

(5) $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta))$ is the Galois group of $x^n - 1$. Then $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$ and $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta)) \cong \mathbb{Z}_n^{\times}$.

Galois Theorem

Char $F = 0$, K is the splitting field of $f(x) \in F[x]$, then : $f(x)$ is solvable. $\Longleftrightarrow \mathrm{Aut}_F(K)$ is solvable.

2.4 Homological Algebra

Modules over ring R

An Abelian group $(M,+)$ is a left R-module over a ring R , then $\forall\ (r,m)\in R\times M$, $rm\in M$.
An Abelian group $(M,+)$ is a right R-module over a ring R , then $\forall\ (m,r)\in M\times R$, $mr\in M$.
M satisfies the module distributivity and the module associativity,
$\forall\ r,s\in R,\ m,n\in M$:

Module distributivity : $\begin{cases} (r+s)m = rm+sm \\ r(m+n) = rm+rn \end{cases}$

Module associativity : $\begin{cases} r(sm) = (rs)m \\ \mathbb{1}m = m \end{cases}$

$f: M\longrightarrow N$ is an R-module homomorphism, if for any $r\in R$, $m_1,m_2\in M$ one has :

$$f(r\cdot m) = r\cdot f(m)\ ,\ f(m_1+m_2) = f(m_1)+f(m_2)\ .$$

Proposition

(1) A module over a field $\mathbb{F}$ is a vector space, a vector space is an $\mathbb{F}$-module.
A module over $\mathbb{Z}$ is an Abelian group, an Abelian group is a $\mathbb{Z}$-module.

(2) Let R , S be rings, suppose M is an S-module, $\psi: R\longrightarrow S$ is a ring homomorphism.
If $\forall\ m\in M$, $r\in R$, one has $rm=\psi(r)m$, then M is also an R-module.

(3) Let M be an R-module, as groups N is a subgroup of M .
If $\forall\ r\in R$, $n\in N$,one has $rn\in N$, then N is a submodule of M , denoted by $N<M$.

(4) For module homomorphism $f: M\longrightarrow M'$, one has $\mathcal{K}er(f)<M$, $\mathcal{I}m(f)<M'$.

(5) The annihilator of element $r\in R$ is $\mathrm{Ann}_R(r)=\{a\mid a\in R\ ,\ ar=0\}$, it is an ideal of ring R .

(6) $RX=\{r_1x_1+\cdots+r_nx_n\mid r_i\in R\ ,\ x_i\in X\}$ is a submodule generated by X , denoted by $(X)=RX$.
It is the minimal submodule containing the set X .

(7) If $\mathrm{Ann}_R(r)\neq 0$, then r is a torsion element of ring R .
If R is an integral domain, then all the torsion elements $T(M)$ is a submodule of M , called the torsion submodule.
If $T(M)=M$, then M is a torsion module.
If $T(M)=0$, then M is a torsion-free module.
If $M=(x)$, then M is a cyclic module.
If N is a submodule of an R-module M , then $M/N=\{m+N\mid m\in M\}$ is a quotient module.

(9) For an Abelian group A , let $\mathrm{End}(A) = \{f : A \longrightarrow A\}$ be the homomorphism ring of A , then A is an $\mathrm{End}(A)$-module.

(10) For an R-module M , there is a natural module homomorphism $\varphi_r : M \longrightarrow M$, $m \longmapsto rm$ which induces a ring homomorphism $\psi : R \longrightarrow \mathrm{End}(M)$, $r \longmapsto \varphi_r$.
Thus M is also an $\mathrm{End}(M)$-module.

Direct sums of modules

M_1 and M_2 are R-module, the direct sum $M_1 \oplus M_2 = \{(m_1, m_2) \mid m_1 \in M_1, m_2 \in M_2\}$ is an R-module,

which induces a canonical map $\begin{cases} \tau_1 : M_1 \longrightarrow M_1 \oplus M_2, m_1 \mapsto (m_1, 0) \\ \tau_2 : M_2 \longrightarrow M_1 \oplus M_2, m_2 \mapsto (0, m_2) \\ \pi_1 : M_1 \oplus M_2 \longrightarrow M_1, (m_1, m_2) \mapsto m_1 \\ \pi_2 : M_1 \oplus M_2 \longrightarrow M_2, (m_1, m_2) \mapsto m_2 \end{cases}$

and an exact (also split) sequence $0 \longrightarrow M_1 \xrightarrow{\tau_1} M_1 \oplus M_2 \xrightarrow{\pi_2} M_2 \longrightarrow 0$.

Proposition

(1) Let $f : N \longrightarrow M$, $\widetilde{f} : M \longrightarrow N$ be R-module homomorphisms,
if $\widetilde{f} \circ f = \mathbb{1}_N$, then f is injective called split monomorphism, $\widetilde{f}$ is surjective called split epimorphism, and one has $M = \mathcal{I}m(f) \oplus \mathcal{K}er(\widetilde{f})$.

(2) An exact sequence $0 \longrightarrow M_1 \xrightarrow{f} M \xrightarrow{g} M_2 \longrightarrow 0$ is split.
$\Longleftrightarrow$ The monomorphism f is a split monomorphism.
$\Longleftrightarrow$ Exist an epimorphism $\widetilde{f} : M \longrightarrow M_1$,such that $\widetilde{f} \circ f = \mathbb{1}_{M_1}$.
$\Longleftrightarrow$ The epimorphism g is a split epimorphism.
$\Longleftrightarrow$ Exist a monomorphism $\widetilde{g} : M_2 \longrightarrow M$,such that $g \circ \widetilde{g} = \mathbb{1}_{M_2}$.
$\Longleftrightarrow$ $\mathcal{I}m(f) = \mathcal{K}er(g)$ is a direct summand of M (M_1 is not the direct summand generally) .
$\Longleftrightarrow$ Every homomorphism $h : M_1 \longrightarrow N$ factors through f .
$\Longleftrightarrow$ Every homomorphism $h : N \longrightarrow M_2$ factors through g .

$$\begin{tikzcd}
 & & N & N \arrow[d, dashed, "\widetilde{h}"'] \arrow[dr, "h"] \arrow[d, phantom, shift left=4ex, "\circlearrowright"] & & \\
0 \arrow[r] & M_1 \arrow[ur, "h"] \arrow[r, "f"'] & M \arrow[u, dashed, "\widetilde{h}"'] \arrow[u, phantom, shift right=4ex, "\circlearrowright"] & M \arrow[r, "g"'] & M_2 \arrow[r] & 0
\end{tikzcd}$$

$\Longrightarrow M \cong M_1 \oplus M_2$.

(3) An exact sequence $0 \longrightarrow M_1 \xrightarrow{f} M \xrightarrow{g} M_2 \longrightarrow 0$ is split.
$\Longrightarrow$ If $\mathcal{T}$ is an additive functor, then

$$0 \longrightarrow \mathcal{T}(M_1) \xrightarrow{\mathcal{T}(f)} \mathcal{T}(M) \xrightarrow{\mathcal{T}(g)} \mathcal{T}(M_2) \longrightarrow 0 \text{ is also exact and split.}$$

Projective modules and injective modules

$$\begin{tikzcd}
 & & N & N \arrow[d, dashed, "\tilde{h}"'] \arrow[dr, "h"] & & \\
0 \arrow[r] & M_1 \arrow[ur, "h"] \arrow[r, "f"'] \arrow[ur, phantom, shift right=4, "\circlearrowright"] & M \arrow[u, dashed, "\tilde{h}"'] & M \arrow[r, "g"'] \arrow[ur, phantom, shift left=4, "\circlearrowright"] & M_2 \arrow[r] & 0
\end{tikzcd}$$

For any monomorphism $f : M_1 \longrightarrow M$ and any homomorphism $h : M_1 \longrightarrow N$, if there exists $\widetilde{h} : M \longrightarrow N$ such that $h = \widetilde{h} \circ f$, then N is an injective module.

For any epimorphism $g : M \longrightarrow M_2$ and any homomorphism $h : N \longrightarrow M_2$, if there exists $\widetilde{h} : N \longrightarrow M$ such that $h = g \circ \widetilde{h}$, then N is a projective module.

Proposition

(1) If a co-cone $(N, h, \widetilde{h})$ of monomorphism $f : M_1 \longrightarrow M$ satisfies the universal property, then N is a colimit and an injective module.
If a cone $(N, h, \widetilde{h})$ of epimorphism $g : M \longrightarrow M_2$ satisfies the universal property, then N is a limit and a projective module.

(2) An R-module J is an injective module.
$\Longleftrightarrow$ The contravariant functor $\mathrm{Hom}_R(-, J)$ is exact.
$\Longleftrightarrow$ If J is a submodule of M , then there is a $K \subseteq M$ such that $J \oplus K = M$.

(3) An R-module P is a projective module.
$\Longleftrightarrow$ The covariant functor $\mathrm{Hom}_R(P, -)$ is exact.
$\Longleftrightarrow$ If there is another module K such that $P \oplus K$ is a free module, then P is a projective module.

(4)

$$\begin{tikzcd}[column sep=large]
\text{free} \arrow[r, Rightarrow] & \text{projective} \arrow[r, Rightarrow] \arrow[l, Rightarrow, dashed, bend left=80, "\text{local ring or } PID"] & \text{flat} \arrow[r, Rightarrow] \arrow[l, Rightarrow, dashed, bend left=80, "\text{perfect ring}"] & \text{torsion-free} \arrow[l, Rightarrow, dashed, bend left=80, "\text{Dedekind ring}"]
\end{tikzcd}$$

Flat modules

Flat modules include free modules, projective modules and torsion-free modules over a PID .

An R-module F is flat. $\Longleftrightarrow$ The covariant functor $\otimes_R F$ or $F \otimes_R$ is exact.

Resolutions of modules

To be continuous...

Module homomorphisms

For module homomorphisms $f : M \longrightarrow M'$, $g, h : K \longrightarrow M$, $g', h' : M' \longrightarrow K'$,
we have

$$K \xrightarrow{g,h} M \xrightarrow{f} M' \xrightarrow{g',h'} K' \ ,$$

and an exact sequence

$$0 \longrightarrow \mathcal{K}er(f) \xrightarrow{i} M \xrightarrow{f} M' \xrightarrow{j} \mathcal{C}oker(f) \longrightarrow 0 \ .$$

f is injective.
$\Longleftrightarrow \mathcal{K}er(f) = 0$.
$\Longleftrightarrow 0 \longrightarrow M \xrightarrow{f} M' \xrightarrow{j} \mathcal{C}oker(f) \longrightarrow 0$ is exact.
$\Longleftrightarrow$ If $f \circ g = f \circ h$, then $g = h$ (left cancellation) .
$\Longleftrightarrow$ If $f \circ g = 0$, then $g = 0$.

f is surjective.
$\Longleftrightarrow \mathcal{I}m(f) = M'$
$\Longleftrightarrow 0 \longrightarrow \mathcal{K}er(f) \xrightarrow{i} M \xrightarrow{f} M' \longrightarrow 0$ is exact.
$\Longleftrightarrow$ If $g' \circ f = h' \circ f$, then $g' = h'$ (right cancellation) .
$\Longleftrightarrow$ If $g' \circ f = 0$, then $g' = 0$.

Decomposition Theorem

Let $f : M \longrightarrow M'$ and $g : M \longrightarrow N$ be R-module homomorphisms.

If $g : M \longrightarrow N$ is surjective and $\mathcal{K}er(g) \subseteq \mathcal{K}er(f)$,
then one has a unique $h : N \longrightarrow M'$ such that $f = h \circ g$ and $\mathcal{K}er(h) = g(\mathcal{K}er(f))$, $\mathcal{I}m(h) = \mathcal{I}m(f)$.

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[dr, "g"'] & M' \\ \arrow[ur, phantom, "\circlearrowleft"] & N \arrow[u, dashed, "h"'] \end{tikzcd}$$

thus we have :
(1) h is injective. $\Longleftrightarrow \mathcal{K}er(g) = \mathcal{K}er(f)$
(2) h is surjective. $\Longleftrightarrow f$ is surjective.

That means any R-module homomorphism f factors through a epimorphism $g : M \longrightarrow N$
which satisfies $\mathcal{K}er(g) \subseteq \mathcal{K}er(f)$.

If $h : N \longrightarrow M'$ is injective and $\mathcal{I}m(f) \subseteq \mathcal{I}m(h)$,
then one has a unique $g : M \longrightarrow N$ such that $f = h \circ h$ and $\mathcal{K}er(f) = \mathcal{K}er(g)$, $(\mathcal{I}m(g)) = h^{-1}(\mathcal{I}m(f))$.

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[dr, dashed, "g"'] & M' \\ \arrow[ur, phantom, "\circlearrowleft"] & N \arrow[u, "h"'] \end{tikzcd}$$

thus we have :
(1) g is injective. $\Longleftrightarrow f$ is injective.
(2) g is surjective. $\Longleftrightarrow \mathcal{I}m(f) = \mathcal{I}m(h)$

That means any R-module homomorphism f factors through a monomorphism $h : N \longrightarrow M'$
which satisfies $\mathcal{I}m(f) \subseteq \mathcal{I}m(h)$.

Fundamental Theorem of Module Homomorphisms

(1) $f : M \longrightarrow M'$ is an epimorphism, then $M/\mathcal{K}er(f) \cong M'$.
Let N be a submodule of M , and $\mathcal{K}er(f) \subseteq N$, then $M/N \cong M'/f(N)$.

(2) K, N are submodules of M , $K \subseteq N$, then $M/N \cong (M/K)/(N/K)$.

(3) K, N are submodules of M , then $(N+K)/K \cong ((N+K) \cap N)/(K \cap N) = N/(K \cap N)$.

Proposition

Let $M_1, M_2, \cdots, M_n$ are submodules of M , $M = \sum_n M_i$, then these following are equivalent:
(1) $M_1 \oplus \cdots \oplus M_n \cong M$, $(m_1, \cdots, m_n) \longmapsto m_1 + \cdots + m_n$.
(2) The representation of the 0 in M is unique.
(3) The representation of any elements in M is unique.
(4) For any i , $M_i \cap (M_1 + \cdots + \hat{M}_i + \cdots + M_n) = 0$.

Free modules

Let M be an R-module, for a linearly independent set $B \subseteq M$,
if every $m \in M$ is the unique linear combination of the elements $b_i \in B$, then M is free R-module (with the basis B) .

Proposition

(1) If R is a field, then all R-modules (linear space) are free modules.

(2) Free $\mathbb{Z}$-module is precisely the free Abelian group.

(3) M is free R-module.
$\Longleftrightarrow M = \bigoplus_{i \in I} M_i = \bigoplus_{i \in I} (b_i)$, where $M_i = (b_i)$ is the cyclic submodule of M and for every i , $M_i \cong R$.

(4) If R is a commutative ring with $\mathbb{1}$, M is a finitely generated free R-module, then any basis of M has the same number of elements.

Noetherian rings

Let R be a ring, if all the ideals are finitely generated, then R is a Noetherian ring.

Let R-module M be finitely generated , but generally its submodule is not finitely generated necessarily.
If R is a Noetherian ring, then its submodule is finitely generated definitely.

Finitely generated modules on a PID (principal ideal domain)

(1) The submodule of a finitely generated PID-module M is also finitely generated.

(2) The submodule of a finitely generated free PID-module M is also free and their rank are not bigger than $r(M)$.

(3) If M is a finitely generated PID-module, then one has: M is free. $\Longleftrightarrow M$ is torsion-free.

(4) If $T(M)$ is the torsion submodule of a finitely generated PID-module M , then the quotient module $M/T(M)$ is a free module.

(5) For a finitely generated PID-module there is always a decomposition

$$M = T(M) \oplus F \cong T(M) \oplus M/T(M) \ .$$

Exact sequences

There is a sequence of Abelian groups (modules) $A_1 \xrightarrow{f_1} A_2 \xrightarrow{f_2} A_3$.

$A_1 \xrightarrow{f_1} A_2 \xrightarrow{f_2} A_3$ is an exact sequence. $\Longleftrightarrow \mathcal{K}er(f_2) = \mathcal{I}m(f_1) \Longrightarrow f_2 \circ f_1 = 0$

$\cdots \longrightarrow A_1 \xrightarrow{f_1} A_2 \xrightarrow{f_2} A_3 \longrightarrow \cdots$ is a complex. $\Longleftrightarrow f_2 \circ f_1 = 0$.

The sequence $0 \longrightarrow A_1 \xrightarrow{f_1} A_2 \xrightarrow{f_2} A_3 \longrightarrow 0 \begin{cases} \text{is exact at } A_1 \text{ .} \Longleftrightarrow f_1 \text{ is injective.} \\ \text{is exact at } A_2 \text{ .} \Longleftrightarrow \mathcal{K}er(f_2) = \mathcal{I}m(f_1) \Longrightarrow f_2 \circ f_1 = 0 \\ \text{is exact at } A_3 \text{ .} \Longleftrightarrow f_2 \text{ is surjective.} \end{cases}$

then this sequence is exact at A_1 , A_2 , A_3 .

$0 \longrightarrow \mathrm{Hom}(B, A_1) \xrightarrow{\mathrm{Hom}(B,f_1)} \mathrm{Hom}(B, A_2) \xrightarrow{\mathrm{Hom}(B,f_2)} \mathrm{Hom}(B, A_3) \longrightarrow 0$ is also a sequence of Abelian groups, where $\mathrm{Hom}(B, A_i) = \{\varphi_i \mid \varphi_i : B \longrightarrow A_i\}$

and $\mathrm{Hom}(B, f_1) = f_1\circ$, $\mathrm{Hom}(B, f_1)(\varphi_1) = f_1 \circ \varphi_1 \in \mathrm{Hom}(B, A_2)$,

which is $0 \longrightarrow \varphi_1 \xrightarrow{f_1\circ} \varphi_2 \xrightarrow{f_2\circ} \varphi_3 \longrightarrow 0$.

$0 \longleftarrow \mathrm{Hom}(A_1, B) \xleftarrow{\mathrm{Hom}(f_1,B)} \mathrm{Hom}(A_2, B) \xleftarrow{\mathrm{Hom}(f_2,B)} \mathrm{Hom}(A_3, B) \longleftarrow 0$ is also a sequence of Abelian groups, where $\mathrm{Hom}(A_i, B) = \{\psi_i \mid \psi_i : B \longleftarrow A_i\}$

and $\mathrm{Hom}(f_1, B) = \circ f_1$, $\mathrm{Hom}(f_1, B)(\psi_2) = \psi_2 \circ f_1 \in \mathrm{Hom}(A_1, B)$,

which is $0 \longleftarrow \psi_1 \xleftarrow{\circ f_1} \psi_2 \xleftarrow{\circ f_2} \psi_3 \longleftarrow 0$.

Proposition

(1) For $f \in \mathrm{Hom}(M, N)$, these sequences are exact:

$$0 \longrightarrow \mathcal{K}er(f) \xrightarrow{i} M \xrightarrow{j} \mathcal{C}oker(f) \longrightarrow 0$$

$$0 \longrightarrow \mathcal{K}er(f) \xrightarrow{i} M \xrightarrow{f} N \xrightarrow{j} \mathcal{C}oker(f) \longrightarrow 0$$

(2) For an exact sequence of Abelian groups(modules) $A_1 \xrightarrow{f} A_2 \xrightarrow{g} A_3$,
$\mathcal{K}er(f)$ and $\mathcal{I}m(g)$ are submodules of A_1 and A_3 respectively, then :

$$\begin{tikzcd}
 & & 0 \arrow[dr] & & 0 \\
 & & & \mathcal{I}m(g) \arrow[ur] \arrow[dr, "i"] \arrow[d, phantom, "\circlearrowright"] & \\
A_1 \arrow[rr, "f"] \arrow[dr, "j"'] & & A_2 \arrow[ur] \arrow[rr, "g"'] & & A_3 \\
 & \mathcal{K}er(f) \arrow[ur] \arrow[dr] \arrow[u, phantom, "\circlearrowright"] & & & \\
0 \arrow[ur] & & 0 & &
\end{tikzcd}$$

This diagram commutes.

$\Longleftrightarrow$ these sequences are also exact:

$A_1 \xrightarrow{j} \mathcal{K}er(f) \longrightarrow 0$, $0 \longrightarrow \mathcal{I}m(g) \xrightarrow{i} A_3$, $0 \longrightarrow \mathcal{K}er(f) \longrightarrow A_2 \longrightarrow \mathcal{I}m(g) \longrightarrow 0$.

(3) $0 \longrightarrow A \longrightarrow B \longrightarrow 0$ is exact. $\Longrightarrow A \cong B$
$0 \longrightarrow A \longrightarrow 0$ is exact. $\Longrightarrow A = 0$

(4) If $A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$ is exact, then f is surjective $\Longleftrightarrow$ h is injective.

(5) If $\cdots \longrightarrow A_n \xrightarrow{f_n} B_n \longrightarrow C_n \longrightarrow A_{n-1} \xrightarrow{f_{n-1}} B_{n-1} \longrightarrow \cdots$ is exact, then $A_n \cong B_n \Longrightarrow C_n = 0$.

Short free resolutions

A is an Abelian group, then there exists a short free resolution of this free module A which is a short exact sequence $0 \longrightarrow K \longrightarrow F \longrightarrow A \longrightarrow 0$ and K , F are free Abelian groups.

For an Abelian group A , let F be the free Abelian group with the basis A (F is generated by A) , and K is the kernel of map $F \longrightarrow A$.

Thus the short free resolution of A is $0 \longrightarrow K \xrightarrow{i} F \longrightarrow A \longrightarrow 0$

Proposition

If $0 \longrightarrow A_1 \xrightarrow{f_1} A_2 \xrightarrow{f_2} A_3 \longrightarrow 0$ is exact, then

$$0 \longrightarrow \mathrm{Hom}(B, A_1) \xrightarrow{\mathrm{Hom}(f_1)} \mathrm{Hom}(B, A_2) \xrightarrow{\mathrm{Hom}(f_2)} \mathrm{Hom}(B, A_3) \longrightarrow 0$$

is exact at $\mathrm{Hom}(B, A_1)$ and $\mathrm{Hom}(B, A_2)$ for any Abelian group B ,

which means $\mathrm{Hom}(B, -)$ is a left exact functor,

$$0 \longrightarrow \mathrm{Hom}(B, A_1) \xrightarrow{\mathrm{Hom}(B,f_1)} \mathrm{Hom}(B, A_2) \xrightarrow{\mathrm{Hom}(B,f_2)} \mathrm{Hom}(B, A_3) \text{ is exact.}$$

proof:

(1) $\mathrm{Hom}(B, f_1)$ is injective:

For any $f_1 \circ \varphi_1 = f_1 \circ \psi_1 \in \mathcal{I}m(\mathrm{Hom}(B, f_1))$,one always has $\varphi_1 = \psi_1$ because f_1 is injective.
$\Longrightarrow \mathrm{Hom}(B, f_1)$ is injective.

(2) $\mathcal{K}er(\mathrm{Hom}(B, f_2)) = \mathcal{I}m(\mathrm{Hom}(B, f_1))$:

$\mathcal{K}er(\mathrm{Hom}(B, f_2)) \subseteq \mathcal{I}m(\mathrm{Hom}(B, f_1))$:
For $\varphi_2 \in \mathcal{K}er(\mathrm{Hom}(B, f_2))$, $f_2 \circ \varphi_2 = 0 \Longrightarrow \mathcal{I}m(\varphi_2) \subseteq \mathcal{K}er(f_2) = \mathcal{I}m(f_1)$
Because f_1 is injective, there exists $h : B \longrightarrow A_1$ such that $\varphi_2 = f_1 \circ h$,
then $\varphi_2 \in \mathcal{I}m(\mathrm{Hom}(B, f_1))$.

$\mathcal{I}m(\mathrm{Hom}(B, f_1)) \subseteq \mathcal{K}er(\mathrm{Hom}(B, f_2))$:
for $\varphi_2 \in \mathcal{I}m(\mathrm{Hom}(B, f_1))$, $\varphi_2 = f_1 \circ h$,
because $f_2 \circ f_1 = 0$, $g = 0$,
then $\varphi_2 \in \mathcal{K}er(\mathrm{Hom}(B, f_2))$.

$$\begin{tikzcd}
& B \arrow[dl, dashed, "h"'] \arrow[d, "\varphi_2"'] \arrow[dr, "0"] & \\
A_1 \arrow[r, "f_1"'] & A_2 \arrow[ur, phantom, "\circlearrowright"] \arrow[r, "f_2"'] & A_3
\end{tikzcd}
\qquad
\begin{tikzcd}
& B \arrow[dl, "h"'] \arrow[d, "\varphi_2"] \arrow[dr, dashed, "g=0"] & \\
A_1 \arrow[ur, phantom, "\circlearrowright"] \arrow[r, "f_1"'] & A_2 \arrow[r, "f_2"'] & A_3
\end{tikzcd}$$

$$f_2 \circ f_1 = 0$$

Proposition

If $0 \longrightarrow A_1 \xrightarrow{f_1} A_2 \xrightarrow{f_2} A_3 \longrightarrow 0$ is exact, then

$0 \longleftarrow \mathrm{Hom}(A_1, B) \xleftarrow{\mathrm{Hom}(f_1,B)} \mathrm{Hom}(A_2, B) \xleftarrow{\mathrm{Hom}(f_2,B)} \mathrm{Hom}(A_3, B) \longleftarrow 0$

is exact at $\mathrm{Hom}(A_2, B)$ and $\mathrm{Hom}(A_3, B)$ for any Abelian group B ,

which means $\mathrm{Hom}(-, B)$ (contravariant Hom functor) is also a left exact functor,

$\mathrm{Hom}(A_1, B) \xleftarrow{\mathrm{Hom}(f_1,B)} \mathrm{Hom}(A_2, B) \xleftarrow{\mathrm{Hom}(f_2,B)} \mathrm{Hom}(A_3, B) \longleftarrow 0$ is exact.

$0 \longrightarrow \mathrm{Hom}(A_3, B) \xrightarrow{\mathrm{Hom}(f_2,B)} \mathrm{Hom}(A_2, B) \xrightarrow{\mathrm{Hom}(f_1,B)} \mathrm{Hom}(A_1, B)$ is exact.

proof:

(1) $\mathrm{Hom}(f_2, B)$ is injective:

For any $\varphi_3 \circ f_2 = \psi_3 \circ f_2 \in \mathrm{Hom}(A_2, B)$, one always has $\varphi_3 = \psi_3$ because f_2 is surjective.
$\Longrightarrow \mathrm{Hom}(f_2, B)$ is injective.

(2) $\mathcal{K}er(\mathrm{Hom}(f_1, B)) = \mathcal{I}m(\mathrm{Hom}(f_2, B))$:

$\mathcal{K}er(\mathrm{Hom}(f_1, B)) \subseteq \mathcal{I}m(\mathrm{Hom}(f_2, B))$:
For $\psi_2 \in \mathcal{K}er(\mathrm{Hom}(f_1, B))$, $\psi_2 \circ f_1 = 0 \Longrightarrow \mathcal{K}er(f_2) = \mathcal{I}m(f_1) \subseteq \mathcal{K}er(\psi_2)$
Because f_2 is surjective, there exists $h : A_3 \longrightarrow B$ such that $\psi_2 = h \circ f_2$,
then $\psi_2 \in \mathcal{I}m(\mathrm{Hom}(f_2, B))$.

$\mathcal{I}m(\mathrm{Hom}(f_2, B)) \subseteq \mathcal{K}er(\mathrm{Hom}(f_1, B))$:
For $\psi_2 \in \mathcal{I}m(\mathrm{Hom}(f_2, B))$, $\psi_2 = h \circ f_2$,
because $f_2 \circ f_1 = 0$, $\psi_2 \circ f_1 = 0$,
then $\psi_2 \in \mathcal{K}er(\mathrm{Hom}(f_1, B))$.

$$\begin{tikzcd}
& B & \\
A_1 \arrow[ur, "0"] \arrow[r, "f_1"'] & A_2 \arrow[u, "\psi_2"] \arrow[r, "f_2"'] & A_3 \arrow[ul, dashed, "h"']
\end{tikzcd}
\qquad
\begin{tikzcd}
& B & \\
A_1 \arrow[ur, dashed, "0"] \arrow[r, "f_1"'] & A_2 \arrow[u, "\psi_2"] \arrow[r, "f_2"'] & A_3 \arrow[ul, "h"']
\end{tikzcd}$$

$f_2 \circ f_1 = 0$

Proposition

If $0 \longrightarrow A_1 \xrightarrow{f_1} A_2 \xrightarrow{f_2} A_3 \longrightarrow 0$ is exact, then

$A_1 \otimes B \xrightarrow{f_1 \otimes \mathbb{1}_B} A_2 \otimes B \xrightarrow{f_2 \otimes \mathbb{1}_B} A_3 \otimes B \longrightarrow 0$ is exact for any Abelian group B ,

which means $\otimes B$ (and $B \otimes$ as well) is a right exact functor,

proof:

(1) $f_2 \otimes \mathbb{1}_B$ is surjective:

f_2 is surjective.

$\Longrightarrow$ For any $a_3 \in A_2$, there is a $a_2 \in A_2$ such that $f_2(a_2) = a_3 \in A_3$.

$\Longrightarrow$ For any $a_3 \otimes b \in A_2 \otimes B$, there is a $a_2 \otimes b \in A_2 \otimes B$ such that $f_2 \otimes \mathbb{1}_B(a_2 \otimes b) = a_3 \otimes b \in A_3 \otimes B$.

$\Longrightarrow$ $f_2 \otimes \mathbb{1}_B$ is surjective.

(2) $\mathcal{K}er(f_2 \otimes \mathbb{1}_B) = \mathcal{I}m(f_1 \otimes \mathbb{1}_B)$:

$\mathcal{I}m(f_1 \otimes \mathbb{1}_B) \subseteq \mathcal{K}er(f_2 \otimes \mathbb{1}_B)$:

$(f_2 \otimes \mathbb{1}_B) \circ (f_1 \otimes \mathbb{1}_B) = (f_2 \circ f_1) \otimes \mathbb{1}_B = 0$

$\Longrightarrow \mathcal{I}m(f_1 \otimes \mathbb{1}_B) \subseteq \mathcal{K}er(f_2 \otimes \mathbb{1}_B)$

$\mathcal{K}er(f_2 \otimes \mathbb{1}_B) = \mathcal{I}m(f_1 \otimes \mathbb{1}_B)$:

Take $h : A_2 \otimes B/\mathcal{I}m(f_1 \otimes \mathbb{1}_B) \longrightarrow A_3 \otimes B$, $a_2 \otimes b + \mathcal{I}m(f_1 \otimes \mathbb{1}_B) \longmapsto f_2(a_2) \otimes b$ such that $f_2 \otimes \mathbb{1}_B = h \circ p$

For $a_3 \in A_3$ there are $a_2 \in A_2$ and $a_2' \in A_2$ such that $f_2(a_2) = f_2(a_2') = a_3$.

$\Longrightarrow a_2 - a_2' \in \mathcal{K}er(f_2) = \mathcal{I}m(f_1)$

$\Longrightarrow$ There is $a_1 \in A_1$ such that $f_1(a_1) = a_2 - a_2'$.

$\Longrightarrow$ For $b \in B$, $f_1 \otimes \mathbb{1}_B(a_1 \otimes b) = (a_2 - a_2') \otimes b = a_2 \otimes b - a_2' \otimes b \in \mathcal{I}m(f_1 \otimes \mathbb{1}_B)$.

$\Longrightarrow$ There is well defined bilinear map $\varphi : (a_3, b) \longmapsto a_2 \otimes b + \mathcal{I}m(f_1 \otimes \mathbb{1}_B)$ such that $f_2(a_2) = a_3$.

$$\begin{tikzcd}
A_3 \times B \arrow[r] \arrow[d, "\varphi"'] \arrow[dr, phantom, "\circlearrowright"] & A_3 \otimes B \arrow[dl, dashed, "j"] \arrow[dr, phantom, "\circlearrowright"] & A_2 \otimes B \arrow[l, "f_2 \otimes \mathbb{1}_B"'] \arrow[dll, bend left, "p"] \\
A_2 \otimes B/\mathcal{I}m(f_1 \otimes \mathbb{1}_B) \arrow[ur, bend right, "h"'] & &
\end{tikzcd}$$

By the universal property, there is:

$j : A_3 \otimes B \longrightarrow A_2 \otimes B/\mathcal{I}m(f_1 \otimes \mathbb{1}_B)$, $a_2 \otimes b + \mathcal{I}m(f_1 \otimes \mathbb{1}_B)$ such that $f_2(a_2) = a_3$.

Then $j = h^{-1}$, $A_3 \otimes B \cong A_2 \otimes B/\mathcal{I}m(f_1 \otimes \mathbb{1}_B)$.

$\Longrightarrow \mathcal{I}m(f_1 \otimes \mathbb{1}_B) = \mathcal{K}er(p) = \mathcal{K}er(h \circ p) = \mathcal{K}er(f_2 \otimes \mathbb{1}_B)$

2.5 Representation Theory

Representations of groups

Suppose V is a vector space over field F , a linear representation of G is a homomorphism $f : G \longrightarrow \mathrm{End}(V)$. For $n \in N^+$, a matrix representation of G is a homomorphism $f : G \longrightarrow \mathrm{GL}_n(F)$. By fixing a basis of V , one has $\mathrm{End}(V) \cong \mathrm{GL}_n(F)$.

A linear or matrix representation is faithful if it is injective.

Group rings

Given a group G , a group ring of G over F is a set of such element $\sum_{g \in G} \alpha_g g$ where $\alpha_g \in F$, denoted by FG . The operators are : $\alpha_g g + \beta_g g = (\alpha_g + \beta_g)g$, $(\alpha_g g)(\beta_h h) = (\alpha_g \beta_h)(gh)$.

FG is a commutative ring. $\Longleftrightarrow$ G is an Abelian gorup.
By identifying $F = F\{e\}$, $G = \{\mathbb{1}_F\}G$, FG is a vector space with elements in G as a basis.

FG-modules

For a linear reprsentation $f : G \longrightarrow \mathrm{End}(V)$, V can be an FG-module by :
$(\alpha g)v = \alpha f(g)v$, $(\alpha g)(\beta h)v = (\alpha\beta)(gh)v = (\alpha\beta)f(g)f(h)v$ where $f \in \mathrm{End}(V)$.
FG-submodules are precisely G-stable subspaces of V .

There is a bijective correspondence between FG-module V and representation $f : G \longrightarrow \mathrm{End}(V)$.
We say the module V affords the linear representation $f : G \longrightarrow \mathrm{End}(V)$.

Equivalent representations

Given two linear representation $f : G \longrightarrow \mathrm{End}(V)$, $f : G \longrightarrow \mathrm{End}(W)$, let $T : V \longrightarrow W$ be isomorphism of two vector spaces over F (also isomorphism as FG-modules) , then these two representations are equivalent.

Given two matrix representation $f : G \longrightarrow \mathrm{GL}_n(F)$, $g : G \longrightarrow \mathrm{GL}_n(F)$, if there is a fixed invertible matrix P such that $f(g) = P^{-1}g(g)P$ for all $g \in G$, then these two representations are equivalent.

Completely reducible modules

If module M has no proper submodule, then it is simple or irreducible.

For a decomposable module $M = M_1 \oplus M_2 \oplus \cdots$, if every M_i is simple, then M is a completely reducible module.

For a completely reducible module M one has : $M = M_1 \oplus M_2 \oplus \cdots . \Longleftrightarrow M = M_1 + M_2 + \cdots$.

A representation is irreducible, reducible, indecomposable, decomposable or completely reducible if the FG-module affording it is irreducible, reducible, indecomposable, decomposable or completely reducible.

Schur Lemma

For two irreducible modules V and W , every nonzero element in $\mathrm{Hom}(V, W)$ has inverse.

Maschke Thorem

Let G be a finite group, F be a field with char $F \nmid |G|$.

For any FG-module V and submodule $U \subseteq V$, one has submodule $W \subseteq V$ such that $V = U \oplus W$ (every submodule is a direct summand) .

Proposition

(1) An FG-module V is finitely generated. $\Longleftrightarrow$ V is finitely dimensional.

(2) Let G be a finite group, F be a field with char $F \nmid |G|$, then :

Every finitely generated FG-module is completely reducible.

$\Longleftrightarrow$ Every finitely dimensional FG-module is completely reducible.

(2) Let G be a finite group, F be a field with char $F \nmid |G|$, then one can fix a basis of V such that the matrix representation $f(g)$ has the form

$$\begin{pmatrix} f_1(g) & & & \\ & f_2(g) & & \\ & & \cdots & \\ & & & f_n(g) \end{pmatrix}$$

for every $g \in G$.

Wedderburn Theorem

For a nonzero ring R with $\mathbb{1}$ (not commutative necessarily) , then :

Every R-module is projective.

$\Longleftrightarrow$ Every R-module is injective.

$\Longleftrightarrow$ Every R-module is completely reducible.

$\Longleftrightarrow$ As a left R-module, $R = I_1 \oplus \cdots \oplus I_n$ where $I_i = Re_i$ is a left simple ideal.

And $e_i e_j = 0$ if $i \neq j$, $e_i^2 = e_i$, $\sum\limits_{i=1}^{n} e_i = \mathbb{1}$.

$\Longleftrightarrow$ As a ring, $R = R_1 \times \cdots \times R_n$ where R_i is a two-sided ideal of R and $R_i \cong M_{n_i}(F)$ with elements all have inverse.

Characters of representations

A function $f : G \longrightarrow F$ such that $f(g^{-1}hg) = f(h)$ for $g, h \in G$ is called a class function.

Suppose $f : G \longrightarrow \mathrm{End}(V) \cong \mathrm{GL}_n(\mathbb{C})$ is a representation of G afforded by the FG-module V , the function $\chi : G \longrightarrow F$, $g \longmapsto tr(f(g))$ is called the character of f . The character is irreducible or reducible according to the representation is irreducible or reducible.

Proposition

(1) Some representations are equivalent. $\Longleftrightarrow$ they have same character.

(2) The character χ of representation is a class function.

(3) $\chi(e)$ is the degree of representation f .

Hermitian inner products

For two class functions θ and ψ , define the Hermitian inner product $(\theta,\psi)=\frac{1}{|G|}\sum\limits_{g\in G}\theta(g)\overline{\psi(g)}$.

Then for $a,b\in\mathbb{C}$ one has : $(a\theta_1+b\theta_2,\psi)=a(\theta_1,\psi)+b(\theta_2,\psi)$, $(\theta,a\psi_1+b\psi_2)=\overline{a}(\theta,\psi_1)+\overline{b}(\theta,\psi_2)$, $(\theta,\psi)=\overline{(\psi,\theta)}$.

The First Orthogonality Relation of Group Characters

Let G be a finite group, $\chi_1,\cdots,\chi_r$ be the irreducible characters of G over $\mathbb{C}$, then one has $(\chi_i,\chi_j)=\delta_j^i$.

These irreducible characters are a basis of the class functions space, that is for any character θ , one has $\theta=\sum\limits_{i=1}^{r}(\theta,\chi_i)\chi_i$.

The Second Orthogonality Relation of Group Characters

For any $x,y\in G$, $\sum\limits_{i=1}^{r}\chi_i(x)\overline{\chi_i(y)}=\begin{cases}|C_G(x)| & \text{if } x \text{ and } y \text{ are conjugate in } G\\ 0 & \text{otherwise}\end{cases}$.

The norm of class functions

For any class function on G , denote $||\theta||=\sqrt{(\theta,\theta)}$ to be the norm of θ .

For $\theta=\sum\alpha_i\chi_i$, $||\theta||=\sqrt{\sum\alpha_i^2}$.

$||\theta||=1$. $\Longleftrightarrow$ The character is irreducible.

For conjugate classes $C_1,\cdots,C_r$ with lenth $d_1,\cdots,d_r$ and representation $f_1,\cdots,f_r$, the value $\theta(f_i)\overline{\psi(f_i)}$ appears d_i times in (θ,ψ) , thus

$$(\theta,\psi)=\frac{1}{|G|}\sum_{i=1}^{r}d_i\theta(f_i)\overline{\psi(f_i)} .$$

The norm is given by $||\theta||^2=(\theta,\theta)=\frac{1}{|G|}\sum\limits_{i=1}^{r}d_i|\theta(f_i)|^2$.