Definitions and Theorems in Algebra

TRISCT

Contents

1 Groups

1.1 Groups and Elements

Basic properties of groups A group G has the following basic properties.

1. Uniqueness of the identity.
2. Uniqueness of inverses.
3. Possibility of left and right division.
4. Left and right cancellation laws.

Translation by group element Let G be a finite group, then

$$\forall a \in G,\, aG = G$$

Order of an element Let G be a group and $a, b, x \in G$, then

1. $\text{ord}(a) \mid n = |G|$ if G is finite.
2. $\text{ord}(x) = \text{ord}(a^{-1}xa)$, that is, order is an invariant under conjugation.

3. $\text{ord}(ab) = \text{ord}(ba)$
4. $\text{ord}(a) = st \implies \text{ord}(a^s) = t$
5. $\text{ord}(a^k) = \frac{\text{ord}(a)}{(k,\text{ord}(a))}$
6. $ab = ba \implies \text{ord}(ab) \big| [\text{ord}(a), \text{ord}(b)]$
7. $ab = ba \wedge (\text{ord}(a), \text{ord}(b)) = 1 \implies \text{ord}(ab) = \text{ord}(a) \cdot \text{ord}(b)$
8. A group of even order must contain an element of order 2.

Commutativity of elements

1. $ab = ba \iff b^{-1}ab = a \iff a^{-1}b^{-1}ab = 1$.
2. $\forall a \in G$, $a^2 = 1 \implies G$ is abelian.

1.2 Homomorphisms

Basic properties of group homomorphism Let $\varphi : G \to G'$ be a group homomorphism, then

1. $\varphi(1) = 1$
2. $\varphi(a^{-1}) = (\varphi(a))^{-1}$
3. $\varphi(a^k) = \varphi(a)^k$
4. $\text{ord}(\varphi(a)) \mid \text{ord}(a)$
5. $\ker \varphi < G$
6. $\text{im}\varphi < G'$
7. $H' < G' \implies \varphi^{-1}(H') < G$
8. φ is injective $\iff \ker \varphi = \{1\}$.

Basic properties of group isomorphism Let $\varphi : G \to G'$ be a group isomorphism, then

1. φ maps generators to generators.

Automorphisms

1. $G = Z_m \implies \text{Aut}(G) \cong (\mathbb{Z}/m\mathbb{Z})^*$
2. $G = Z_{p^n}$, p is prime and odd $\implies \text{Aut}(G) \cong (\mathbb{Z}/p^n\mathbb{Z})^* \cong Z_{\varphi(p^n)}$
3. $G = Z_{2^n}$, $n \geqslant 3 \implies \text{Aut}(G) \cong (\mathbb{Z}/2^n\mathbb{Z})^* \cong Z_2 \times Z_{2^{n-2}}$

1.3 Subgroups

Product of subsets $S, T, U < G$, $h \in G$. The following hold

1. $(ST)U = S(TU) = STU$
2. $T \subset U \implies ST \subset SU$
3. $T \supset U \implies ST \supset SU$
4. $h(T \cap U) = (hT) \cap (hU)$

Subgroup The following are equivalent.

1. $H < G$
2. H satisfies the group axioms.
3. H is closed under multiplication and taking inverses.
4. H is closed under division.
5. G is finite and H is closed under multiplication.

Properties of cosets $H < G$, then:

1. $HH = H$
2. $h \in H \implies hH = H$
3. $a' \in aH \iff a'H = aH$
4. $b \notin aH \implies aH \cap bH = \varnothing$
5. $aH \neq bH \implies aH \cap bH = \varnothing$
6. $\#H = \#(aH)$

Coset decomposition

$$H < G \implies G = \bigcup_{a_i \in G} a_i H, \qquad a_i H \cap a_j H = \varnothing$$

Lagrange's theorem $H < G$ and $|G| < \infty$, then:

1. $|H| \,\big|\, |G|$
2. $|G/H| = (G : H)$
3. $\mathrm{ord}(a) \big| \, |G|$
4. $G > H > K \implies (G : K) = (G : H)(H : K)$
5. $p = |G|$ is prime $\implies G = Z_p$

Twice decomposition $H, K < G$,then

$$(G : H) = m,\ (G : K) = n \text{ are finite } \implies [m, n] \leqslant (G : H \cap K) \leqslant mn$$

As a corollary,

$$(G : H) \text{ and } (G : K) \text{ are coprime } \implies (G : H \cap K) = (G : H)(G : K)$$

Normal subgroup The following are equivalent.

1. $H \lhd G$
2. $xH = Hx$
3. $xH \subset Hx$
4. $xH \supset Hx$
5. $\forall x \in G, h \in H, \exists h' \in H, xh = h'x$
6. $\forall \sigma \in \mathrm{Inn}(G),\ \sigma H = H$
7. $xHx^{-1} = H$
8. $xHx^{-1} \subset H$
9. $\forall x \in G, h \in H, \exists h' \in H, xhx^{-1} = h'$
10. $(aH)(bH) = (ab)H$ holds regardless of the choice of representatives.
11. $H = \ker \varphi$ for some homomorphism φ.

Sufficient conditions for a subgroup to be normal

1. $H < G$, $(G : H)$ is the minimum prime factor of $|G| \implies H \lhd G$.
2. $Z(G) \lhd G$
3. $\varphi \in \mathrm{Hom}(G, G'),\ H' \lhd G' \implies \varphi^{-1}(H') \lhd G$

Characteristic subgroup The following are true:

1. $H \operatorname{char} G \implies H \lhd G$
2. $H < G$ is the only one of its order $\implies H \operatorname{char} G$.
3. $K \operatorname{char} H \wedge H \lhd G \implies K \lhd G$.

Sylow subgroup Let group G be such that $|G| = p^n m$ (p is prime, $p \nmid m$, $n \geqslant 1$), then any subgroup of order p^n is called a Sylow p-subgroup of G. See the section on Sylow subgroups for more.

Note 1.1. *In other words, the subgroups of order of primary factors.*

Cardinality of a product of subsets

$$H,\, K < G \implies |HK| = \frac{|H| \cdot |K|}{H \cap K}$$

Note 1.2. *$hk = hj \cdot j^{-1}k = h_1 k_1$*

Equivalent condition for a product to be a group $H,\, K < G$, then

$$HK \text{ is a group} \iff HK = KH$$

Sufficient condition for a product to be a group $H,\, K < G$, then

$$H \subset N_G(K) \implies HK \text{ is a group}$$

$$K \lhd G \implies HK \text{ is a group}$$

Direct product (of normal subgroups) Let $H,\, K \lhd G$ and $H \cap K = \{1\}$, then the following is an isomorphism

$$\begin{array}{rcl} H \times_{\text{ext}} K & \xrightarrow{\cong} & HK \\ (h, k) & \mapsto & hk \end{array}$$

and HK is called the internal direct product $HK = H \times_{\text{in}} K$. The elements of H and K are mutually commutable.

Note 1.3. *Mutual commutativity of elements of H and K comes from the fact that $H \cap K = \{1\}$.*

Semidirect product If $H \lhd G$, $K < G\, (K \not\lhd G)$ and $H \cap K = \{1\}$, then HK is a group and is called the semidirect product.

Direct sum (of additive groups) Let A be an additive group and B, C subgroups of it. The following are equivalent conditions for $B + C$ to be an internal direct sum.

1. $x \in B + C$ has a unique expression $x = b + c$, $b \in B$, $c \in C$.
2. $0 \in B + C$ has a unique expression $0 = 0 + 0$.
3. $B \cap C = \{0\}$
4. $B \oplus_{\text{ext}} C \cong B + C$ under the mapping $(b, c) \mapsto b + c$.

1.4 Quotient Groups

Sufficient condition for a quotient group to be commutative $H \triangleleft G$, then

$$G/H \text{ is abelian } \iff H \subset G^c$$

1.5 Isomorphism Theorems

Exact sequence For an exact sequence $0 \to G' \xrightarrow{f} G \xrightarrow{g} G'' \to 0$, there exists a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & G' & \xrightarrow{f} & G & \xrightarrow{g} & G'' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \mathrm{FIT}} & & \\ 0 & \longrightarrow & \ker g & \xrightarrow{j} & G & \xrightarrow{\mathrm{can}} & \frac{G}{\ker g} & \longrightarrow & 0 \end{array}$$

where the rows are exact and the columns are isomorphisms.

Fundamental homomorphism theorem

1. If $f \in \mathrm{Hom}(G, G')$, then

$$\exists\, ! \, f_* : \frac{G}{\ker f} \to G',\ f = f_* \circ \varphi$$

   where f_* is injective and $\varphi : G \to \frac{G}{\ker f}$ is the canonical map.

2. If $f \in \mathrm{Hom}(G, G')$, then

$$\exists\, ! \, f_* : \frac{G}{\ker f} \to G'$$

   where f_* is injective and $\varphi : G \to \frac{G}{\ker f}$ is the canonical map, such that the following diagram commutes

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ {\scriptstyle \varphi}\downarrow & \nearrow_{f_*} & \\ \frac{G}{\ker f} & & \end{array}$$

3. If $f \in \mathrm{Hom}(G, G')$, $\ker f \supset H < G$, $\ker f \supset N = \bigcap\limits_{\substack{K \triangleleft G \\ H \subset K}} K$, then

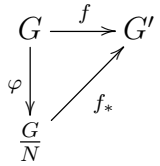
$$\exists\, ! \, f_* : \frac{G}{N} \to G',\ f = f_* \circ \varphi$$

   where f_* is injective and $\varphi : G \to \frac{G}{N}$ is the canonical map.

4. If $f \in \mathrm{Hom}(G, G')$, $\ker f \supset H < G$, $\ker f \supset N = \bigcap_{\substack{K \lhd G \\ H \subset K}} K$, then

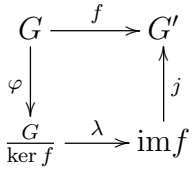
$$\exists\, !\, f_* : \frac{G}{N} \to G'$$

where f_* is injective and $\varphi : G \to \frac{G}{\ker f}$ is the canonical map, such that the following diagram commutes



5. The canonical projection φ is universal among homomorphisms on G that map N to the identity element.
6. Each homomorphism that maps N to identity can be factored through the canonical map φ.

First isomorphism theorem For $f \in \mathrm{Hom}(G, G')$, there exists a commutative diagram



where $\varphi : a \mapsto \bar{a}$ is the canonical map, $\lambda : \bar{a} \mapsto f(a)$ is the canonical isomorphism, and $j : b \mapsto b$ is the inclusion.

Second isomorphism theorem If $N, H < G$, $H \subset N_G(K)$, then

$$\begin{array}{rccc} \psi & : & \frac{HN}{N} & \xrightarrow{\cong} & \frac{H}{N \cap H} \\ & & \overline{hn} = \overline{h} & \mapsto & \overline{h} \end{array}$$

Third isomorphism theorem If $K < H < G$, $K \lhd G$, $H \lhd G$, then the following mapping is an isomorphism

$$\begin{array}{rccc} \tau & : & \frac{G/K}{H/K} & \xrightarrow{\cong} & \frac{G}{H} \\ & & \overline{gK} & \mapsto & \overline{g} \end{array}$$

Fourth isomorphism theorem If $\varphi : G \to G'$ is a surjective homomorphism, then the following hold.

1. The preimage $H = \varphi^{-1}(H')$ of each normal subgroup H' of G' is a normal subgroup of G.
2. The correspondence between normal subgroups of G' and normal subgroups of G containing H is a one-to-one correspondence.
3. For all $H' \lhd G'$ and $H = \varphi^{-1}(H')$, the following mapping is an isomorphism.

$$\begin{array}{rccc} \varphi_H & : & G/H & \xrightarrow{\cong} & G'/H' \\ & & \overline{x} & \mapsto & \overline{\varphi(x)} \end{array}$$

Corollary of the fourth theorem Assume $K \lhd G$, then the canonical surjective homomorphism

$$\begin{array}{rccccc} \varphi & : & G & \to & \overline{G} = G/K \\ & & x & \mapsto & \overline{x} \end{array}$$

induces a one-to-one correspondence between normal subgroups $\{\overline{H} : \overline{H} \lhd \overline{G}\}$ and normal subgroups $\{H : \ker\varphi \lhd H \lhd G\}$ by setting $H = \varphi^{-1}(H')$. and the correspondence

$$H = \varphi^{-1}(H') \leftrightarrow H'$$

satisfies

1. $H_1 \subset H_2 \iff \overline{H}_1 \subset \overline{H}_2$
2. $H_1 \subset H_2 \implies (H_2 : H_1) = (\overline{H}_2 : \overline{H}_1)$
3. $\overline{\langle H_1 \cup H_2 \rangle} = \langle \overline{H}_1 \cup \overline{H}_2 \rangle$
4. $H \lhd G \iff \overline{H} \lhd \overline{G}$

1.6 Decompositions of additive abelian groups

The following hold for all abelian groups. Stating them in terms of additive groups is simply for the consistency of notations.

Chinese remainder theorem (decomposition of a cyclic group) Suppose $m = p_1^{a_1} \cdots p_s^{a_s}$ where p_i are distinct prime numbers, then

$$\mathbb{Z}/m\mathbb{Z} = \langle \overline{e_1} \rangle \oplus_{\text{in}} \cdots \oplus_{\text{in}} \langle \overline{e_s} \rangle \cong \mathbb{Z}/p_1^{a_1}\mathbb{Z} \oplus_{\text{ext}} \cdots \oplus_{\text{ext}} \mathbb{Z}/p_s^{a_s}\mathbb{Z}$$

Lemmas for primary decomposition Let G be an additive abelian group. For a positive integer k, let $\ker k = \{x \in G : kx = 0\}$, then the following hold:

1. $k \big| l \implies \ker k \subset \ker l$
2. $\ker(k, l) = \ker k \cap \ker l$

3. $\ker[k,l] = \ker k + \ker l$
4. $(k,l) = 1 \implies \ker kl = \ker k \oplus \ker l$
5. G is of exponent $m \implies \ker k = \ker(k,m)$
6. G is of exponent mm', $(m,m') = 1$, then

$$A = \ker m \oplus \ker m'$$

Primary decomposition Let A be an additive abelian group of exponent $n = p_1^{e_1} \cdots p_s^{e_s}$ ($p_1, \cdots, p_s$ are distinct prime numbers), then

$$\begin{aligned} A &= A(p_1) \oplus \cdots \oplus A(p_s) \\ &= \ker p_1^{e_1} \oplus \cdots \oplus \ker p_s^{e_s} \end{aligned}$$

where $A(p_i) = \ker p_i^{e_i} = \{x \in A : p_i^k x = 0,\ 1 \leqslant k \in \mathbb{Z}\}$ is a p_i-group, called the p_i part of A. The numbers $\{p_1^{e_1}, \cdots, p_s^{e_s}\}$ are called its primary divisors.

Cyclic decomposition Let $A(p)$ be a finite additive abelian p-group (p is a prime number), then $A(p)$ can be decomposed into the direct sum of cyclic subgroups.

$$A(p) = \langle a_1 \rangle \oplus \cdots \oplus \langle a_t \rangle$$

where each $\langle a_i \rangle$ has power p^{r_i}. The sequence $\{r_i\}_{i=1}^t$ can be arranged in decreasing order $r_1 \geqslant \cdots \geqslant r_s \geqslant 1$ such that it is unique.

Note 1.4. *$A(p)$ is said to be of the type $(p^{r_1}, p^{r_2}, \cdots, p^{r_t})$.*

Basic theorem for finite abelian groups A finite additive abelian group A can be decomposed into

$$\begin{aligned} A &= \langle b_1 \rangle \oplus \cdots \oplus \langle b_u \rangle \\ &\cong (\mathbb{Z}/p_1^{r_{11}}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_1^{r_{1t_1}}\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/p_s^{r_{s1}}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_s^{r_{st_s}}\mathbb{Z}) \end{aligned}$$

The numbers $\{p_k^{r_{kj}} : 1 \leqslant k \leqslant s, 1 \leqslant j \leqslant t_k\}$ are called the elementary divisors of A.

Basic theorem for finitely generated additive abelian group A finitely generated additive abelian group A can be decomposed into

$$\begin{aligned} A &= \langle b_1 \rangle \oplus \cdots \oplus \langle b_u \rangle \oplus \langle c_1 \rangle \oplus \cdots \oplus \langle c_v \rangle \\ &\cong (\mathbb{Z}/p_1^{r_{11}}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_s^{r_{st_s}}\mathbb{Z}) \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z} \end{aligned}$$

The torsion part of A is $A_{\text{tors}} = \langle b_1 \rangle \oplus \cdots \oplus \langle b_u \rangle$, and the free part of A is $A_{\text{free}} = \langle c_1 \rangle \oplus \cdots \oplus \langle c_v \rangle$.

1.7 Group Action

Orbits and elements Let a group G act on a set S, then

1. Any element on a orbit is a generator of this orbit.
$$t \in G(s) \iff G(t) = G(s)$$
2. Different orbits do not intersect.
$$G(s) \cap G(t) \neq \varnothing \iff G(s) = G(t)$$
3. S is decomposed into the union of nonintersecting orbits.
$$S = G(s_1) \cup G(s_2) \cup \cdots \cup G(s_r) \quad (r \text{ may be } \infty)$$
4. The number of elements of S is the sum of the numbers of elements in each orbit.
$$|S| = \sum_{i=1}^{r} |G(s_i)|$$
5. The relation of "being on the same orbit" is an equivalence relation, which may be denoted by $s \sim t$.

Action and isotropy group Let a group G act on a set S, then for all $s \in S$ and $a \in G$:
$$\pi_x s = \pi_a s \iff x \equiv a \pmod{G_s}$$

Length of orbit Let a group G act on a set S, and $s \in S$. The following are true:

1. The following mapping that maps a coset to a point on the orbit
$$G/G_s \to G, \quad aG_s \mapsto as$$
is a bijection.

   Note 1.5. *G/G_s is the set of cosets, not necessarily a quotient group.*
2. Index of isotropy group=$(G : G_s) = |G/G_s| = |G(s)|$ = length of orbit

Orbit decomposition formula Let a group G act on a set S, then S is decomposed into the union of nonintersecting orbits.
$$S = G(s_1) \cup G(s_2) \cup \cdots \cup G(s_r) \quad (r \text{ may be } \infty)$$
The number of elements of S is the sum of the lengths of the orbits.
$$|S| = \sum_{i=1}^{r} |G(s_i)| = \sum_{i=r}^{r} (G : G_{s_i})$$

Transitivity on an orbit $\forall s_1, s_2 \in G(s)$, $\exists g \in G$, $gs_1 = s_2$.

Transitivity on the set Let a group G act on a set S, then

$$\text{The group action is transitive on } S \iff S = G(s)$$

Translation on a group itself Let G act on itself by translation:

$$\begin{array}{rccc} T & : & G & \to & \mathrm{Perm}(G) \\ & & g & \mapsto & T_g(\cdot) = g(\cdot) \end{array}$$

This group action is faithful. Each T_g is a bijection but not a homomorphism. T itself is a homomorphism.

Translation on the set of subsets Let G act on the set $2^G = \{H : H \subset G\}$ of its subsets:

$$\begin{array}{rccc} T & : & G & \to & \mathrm{Perm}(2^G) \\ & & g & \mapsto & T_g(\cdot) = g(\cdot) \end{array}$$

Translation on the set of cosets Let G act on the set G/H of its cosets:

$$\begin{array}{rccc} T & : & G & \to & \mathrm{Perm}(G/H) \\ & & g & \mapsto & T_g(\cdot) = g(\cdot) \end{array}$$

T satisfies the following properties:

1. The isotropy group of $\overline{1} = H$ is $G_{\overline{1}} = G_{\overline{H}} = H$.
2. It is transitive on G/H, that is, there is only one orbit.
3. $\ker T = \bigcap\limits_{x \in G} xHx^{-1}$ is the maximal normal subgroup of G contained in H in the sense that any $N \lhd G$, $N \subset H$ belongs to $\ker T$ as well.

Conjugation on a group itself Let G act on itself by conjugation:

$$\begin{array}{rccc} C & : & G & \to & \mathrm{Aut}(G) \\ & & g & \mapsto & C_g(\cdot) = g(\cdot)g^{-1} = (\cdot)^g \end{array}$$

This action satisfies the following:

1. $\ker C = Z(G)$, that is, C is faithful $\iff Z(G) = \{1\}$.
2. $\mathrm{im}C$ is the collection of all conjugations, and is called the inner automorphism group $\mathrm{Inn}(G)$ of G.
3. The isotropy subgroup of $a \in G$ is $G_a = \mathrm{Centr}(a)$

4. The orbit of a is called the conjugacy class of a and is denoted by $G(a) = a^G$. The length of the orbit is

$$\left|a^G\right| = (G : G_a) = (G : \mathrm{Centr}(a))$$

Moreover, a^G is of length 1 $\iff$ $a \in Z(G)$, that is, a is invariant under all inner automorphisms.

5. (Class formula)

$$|G| = |Z(G)| + \sum_{\substack{i=1 \\ (G:G_{y_i})\geqslant 2}}^{m} (G : G_{y_i})$$

Note 1.6. *This formula is so important that I will say it again.*

(Conjugacy) class formula Let G be a finite group, then

$$\begin{aligned} |G| &= |Z(G)| + \sum_{\substack{i=1 \\ (G:G_{y_i})\geqslant 2}}^{m} (G : G_{y_i}) \\ &= |Z(G)| + \sum_{\substack{i=1 \\ (G:G_{y_i})\geqslant 2}}^{m} |G(y_i)| \end{aligned}$$

where $G_{y_i} = \mathrm{Centr}(y_i)$ is the isotropy subgroup/centralizer of y_i. In the summation y_i goes through the representatives of all conjugacy classes.

Conjugation on a normal subgroup Let G act on one of its normal subgroup $H \lhd G$ by conjugation:

$$\begin{array}{rccc} C & : & G & \to & \mathrm{Aut}(H) \\ & & g & \mapsto & C_g(\cdot) = g(\cdot)g^{-1} = (\cdot)^g \end{array}$$

This action satisfies the following:

1. The kernel of C is

$$\begin{aligned} \ker C &= \{g \in G : ghg^{-1} = h, \forall h \in H\} \\ &= \{g \in G : gh = hg, \forall h \in H\} \\ &= \mathrm{Centr}_G(H) \end{aligned}$$

The latter is called the centralizer of H in G, that is, the elements that commutes with each element of H.

Note 1.7. *Not the elements that commutes with H, but with elements of H.*

Conjugation on the set of all subgroups Let G act on the set $S = \{H : H < G\}$ of its subgroups by conjugation:

$$\begin{array}{rccc} C & : & G & \to & \mathrm{Perm}(S) \\ & & g & \mapsto & C_g(\cdot) = g(\cdot)g^{-1} = (\cdot)^g \end{array}$$

This action satisfies the following:

1. The isotropy subgroup of a subgroup $H < G$ is

$$\begin{aligned} G_H &= \{g \in G : gHg^{-1} = H\} \\ &= \{g \in G : gH = Hg\} \\ &= N_G(H) \end{aligned}$$

   The latter is called the normalizer of H in G, and it the maximal subgroup of G that contains H as a normal subgroup.

2. An orbit H^G is called a conjugacy class

3. The length of an orbit is

$$\left|H^G\right| = (G : N_G(H))$$

Cayley's theorem Each group of order n is isomorphic to some subgroup of S_n.

1.8 p-groups and Sylow subgroups

Lemmas for p-groups

1. The center of a p-group G is not trivial ($Z(G) \neq \{1\}$), and $Z(G)$ contains a subgroup of order p.

   Proof 1.1. Use the class formula.

2. p-groups are solvable.

   Proof 1.2. Prove $G/Z(G)$ is solvable first and use induction.

3. A group of order p^2 is abelian, and is either of the type (p^2) or (p, p).

   Proof 1.3. Construct an isomorphism from $\langle x\rangle \times_{\text{ext}} \langle y\rangle$ if there is no element of order p^2.

4. If G is abelian and $p \big| |G|$ (p is prime), then G has a subgroup of order p.

5. The center of a nonabelian group G of order p^3 is a subgroup of order p and $Z = G^C$.
6. A group G of order p^n has normal subgroups of order $p^0, p^1, p^2, \cdots, p^n$.
7. The normalizer N_H of a proper subgroup $H \lneqq G$ of a p-group G contains H properly, that is,
$$H \lneqq N_H \leqslant G$$
8. Any normal subgroup $N \lhd G$ of a p-group G intersects nontrivially with the center $Z(G)$ of G, that is,
$$N \cap Z(G) \neq \{1\}$$

Sylow subgroup Let group G be such that $|G| = p^n m$ (p is prime, $p \nmid m$, $n \geqslant 1$), then any subgroup of order p^n is called a Sylow p-subgroup of G.

Note 1.8. *In other words, the subgroups of order of primary factors.*

Sylow theorems Let group G be such that $|G| = p^n m$ (p is prime, $p \nmid m$, $n \geqslant 1$). The following theorems hold.

1. (Existence)G has at least one Sylow p-subgroup, and hence has all subgroups of order $p, p^2, \cdots, p^n$.
2. (Maximal)Any p-subgroup of G is contained in some Sylow p-subgroup.
3. (Conjugate)Sylow p-subgroups of G are conjugate in G.
4. (Number)The number n_p of Sylow p-subgroup of G satisfies
$$n_p \equiv 1 \pmod{p}, \quad n_p | m$$
5. (Uniqueness and Normality)Sylow subgroup is unique $\iff$ Sylow subgroup is normal

   Note 1.9. *The last one was not listed on the lecture note.*

1.9 Structures of groups

Group of order pq The following about a group G of order pq ($p < q$ are prime) are true:

1. The Sylow q-subgroup of G is unique and normal.
2. G is solvable.
3. $G = PQ$ is a semidirect/direct product, where Q is the unique Sylow q-subgroup and P is an arbitrary Sylow p-subgroup.

4. If $G = PQ$ is a direct product, then it is cyclic, otherwise it is non-abelian.
5. If $p \nmid q - 1$, then G is cyclic. If $p \mid q - 1$, then it can be both.

Examples

1. A group of order 35 is cyclic.
2. A group of order 6 is cyclic or isomorphic to S_3.

Group of order p^q The following about a group of order p^q (p, q are distinct prime numbers) are true:

1. The Sylow p or q-subgroups are normal

Example

1. A group G of order 12 has either a unique Sylow 3-subgroup or a unique Sylow 2-subgroup. In the second case, $G \cong A_4$.

Example

1. The Sylow 3-subgroup P and Sylow 5-subgroup Q of a group G of order 30 are normal in G, and $P \times Q$ is a normal cyclic subgroup of order 15.

2 Rings

2.1 Definitions

The following are from GTM158.

Ring A **ring** is a nonempty set R, together two binary operations addition and multiplication that satisfy:

1. R is an abelian group under addition.
2. R is a semigroup under multiplication.
3. Left and right distributivity holds.

Ring with identity A ring R is called a **ring with identity** if there exists a multiplicative element.

Unit An element in a ring is a **unit** if there exists an inverse of it.

Commutative ring A ring that is commutative in multiplication.

Zero divisor A **zero divisor** is a nonzero element such that for some other nonzero element their product equals 0.

Integral domain An **integral domain** is a commutative ring with identity and no zero divisors.

Field A **field** is a commutative ring with identity such that $1 \neq 0$ and that every nonzero element has an inverse.

Subring Omitted.

Subfield Omitted.

Ring homomorphism A mapping from a ring to another that preserves addition and multiplication.

Monomorphism An injective homomorphism.

Embedding Monomorphism.

Epimorphism A surjective homomorphism.

Isomorphism A bijective homomorphism.

Endomorphism A homomorphism from a ring into itself.

Automorphism An isomorphism from a ring onto itself.

Ideal An **ideal** is a nonempty subset of a ring that is closed under subtraction and absorbs the ring into itself through left and right multiplication.

> **Note 2.1.** *Roman's defining ideal using closedness under subtraction may have something to do with the fact that an identity is not yet required.*

Generated ideal The **ideal generated** by a nonempty subset of a ring is the smallest ideal containing that set.

Principal ideal An ideal generated by a single element.

Factor ring The ring of cosets of an ideal.

Maximal ideal Omitted.

Characteristic The **characteristic** of a ring is the smallest positive integer such that this number of $1's$ added equals 0, should it exist. If it does not, the ring has characteristic 0.

Prime subfield The smallest subfield, or the intersection of all subfield.

The following are defined for only integral domains.

Divides In an integral domain, a **divides** b if $b = \rho a$ for some ρ.

Properly divides In an integral domain, if $b = \rho a$ and a, b are nonunits, then a **properly divides** b.

Associates In an integral domain, if $a = ub$ for some unit u, then a, b are associates.

Irreducible A nonzero nonunit element is **irreducible** if it has no proper divisors.

Prime A nonzero nonunit element is **prime** if it dividing a product always implies it dividing a factor of that product.

Greatest common divisor A **greatest common divisor** is a common divisor such that any other common divisor is a factor of it.

Relatively prime Two elements are **relatively prime** if their greatest common divisor is a unit.

2.2 Ideals

Proposition A commutative ring A contains no proper ideal $\iff$ A is a field.

Kernel of a homomorphism The kernel of a ring homomorphism is a two-sided ideal.

Sum of ideals The sum of the ideals $\mathfrak{a}$, $\mathfrak{b}$:

$$\mathfrak{a} + \mathfrak{b} \triangleq \{x + y : x \in \mathfrak{a},\, y \in \mathfrak{b}\}$$

is an ideal.

Product of ideals The product of the ideals $\mathfrak{a}$, $\mathfrak{b}$:

$$\mathfrak{a}\mathfrak{b} \triangleq \{x_1 y_1 + \cdots + x_n y_n,\, x_i \in \mathfrak{a},\, y_i \in \mathfrak{b}\}$$

is an ideal.

Intersection of ideals The intersection of any family of ideals $\{\mathfrak{a}_i\}_{i \in I}$

$$\bigcap_{i \in I} \mathfrak{a}_i$$

is an ideal.

The set of ideals

1. The set of ideals form a additive monoid, with (0) as the zero element.
2. The set of ideals form a multiplicative monoid, with (1) as the identity.
3. Distributivity holds for ideal addition and multiplication.
4. The set of ideals **does not** form a ring.

Proposition $\mathfrak{a}$, $\mathfrak{b}$ are ideals of a commutative ring A, then

$$(\mathfrak{a}+\mathfrak{b})(\mathfrak{a}\cap\mathfrak{b})\subset\mathfrak{a}\mathfrak{b}\subset\mathfrak{a}\cap\mathfrak{b}$$

Coprime ideals The following are true for a commutative ring A and its coprime ideals $\mathfrak{a}$, $\mathfrak{b}$.

1. $\mathfrak{a}+\mathfrak{b}=A \implies \mathfrak{a}\mathfrak{b}=\mathfrak{a}\cap\mathfrak{b}$
2. $\mathfrak{a}+\mathfrak{b}=A \implies \mathfrak{a}^m+\mathfrak{b}^n=A,\ \forall m,n\in\mathbb{N}$

Prime ideal The following are equivalent.

1. $\mathfrak{p}\subset A$ is a **prime ideal**.
2. $\mathfrak{p}\neq A,\ xy\in\mathfrak{p} \implies (x\in\mathfrak{p})\vee(y\in\mathfrak{p})$
3. $\mathfrak{p}\neq A$, $A/\mathfrak{p}$ is an integral domain.

Maximal ideal The following are equivalent.

1. $\mathfrak{m}\subset A$ is a **maximal ideal**.
2. $\mathfrak{m}\subset\mathfrak{a}\subset A \implies (\mathfrak{m}=\mathfrak{a})\vee(\mathfrak{m}=A)$
3. $A/\mathfrak{m}$ is a field.

Suff. cond. for the existence of a maximal ideal Any nonzero commutative ring R with identity contains a maximal ideal.

Proof 2.1. Use Zorn's lemma on the set of all proper ideals.

About maximal and prime The following are true.

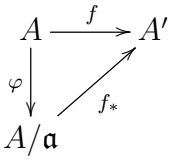
1. Every maximal ideal is prime.
2. Every nonunit ideal is contained in some maximal ideal.
3. $\{0\}\subset A$ is prime $\iff$ A is entire.
4. $f\in\mathrm{Hom}(A,A')$, $\mathfrak{p}'\subset A$ is prime $\implies$ $f^{-1}(\mathfrak{p}')$ is prime.
5. $f\in\mathrm{Hom}(A,A')$, f is surjective, $\mathfrak{m}'\subset A'$ is maximal $\implies$ $f^{-1}(\mathfrak{m}')$ is maximal.

2.3 Isomorphism Theorems

Fundamental homomorphism theorem If $f \in \mathrm{Hom}(A, A')$, $\mathfrak{a} \subset A$ is an ideal, $\ker f \supset \mathfrak{a}$, then there exists a unique $f_* : A/\mathfrak{a} \to A'$ such that

$$g = g_* \circ \varphi$$

where $\varphi : A \to A/\mathfrak{a}$ is the canonical mapping. In other words, the following diagram commutes:



2.4 Characteristic

Characteristic The characteristic of an integral domain is either 0 or a prime p.

Prime subfield Let F be a field, then

1. $\mathrm{char}\, F = 0 \implies$ the prime subfield of $F \cong \mathbb{Q}$
2. $\mathrm{char}\, F = p \implies$ the prime subfield of $F \cong \mathbb{Z}_p$

Power of sum In a commutative ring with identity of prime characteristic p,

$$(a + b)^p = a^p + b^p$$

Field of quotients Let R' be the field of quotients of an integral domain R, then any monomorphism σ from R into a field F has a unique extension to a monomorphism $\bar{\sigma} : R' \to F$.

2.5 Integral Domains

The following are considered within an integral domain R.

Note 2.2. *Prime ideal is a concept defined for all commutative rings; irreducible element and prime element are concepts defined for only integral domains, hence here I shall discuss only propositions concerning irreducible and prime elements and others that only hold in integral domains.*

Dividing The following are true in R.

1. $u \in R^* \implies u \big| a, \forall a \in R$

2. $a \big| b \iff (b) \subset (a)$
3. $a \big| b$ properly $\iff (b) \subsetneqq (a) \subsetneqq R$

Associates The following are equivalent.

1. $a \sim b$
2. $u \in R^*$, $a = bu$
3. $a \big| b$, $b \big| a$
4. $(a) = (b)$

Proposition $(a) \neq (0)$ is prime $\iff$ a is prime .

Proposition A prime element is irreducible.

Proposition The greatest common divisor is unique up to associate.

UFD The following are equivalent for an integral domain R with the **factorization property**.

1. R is UFD.
2. Factorization is essentially unique.
3. Irreducible implies prime.
4. Nonzero elements have a gcd.

Proposition In a UFD, prime $\iff$ irreducible.

PID The following are equivalent in a PID R.

1. $R/(a)$ is a field.
2. $R/(a)$ is an integral domain.
3. a is irreducible.
4. a is prime.

Proposition In a PID A, $a, b \neq 0$, then

$$(a) + (b) = (c) \implies c = \gcd(a, b)$$

Proposition In a PID, prime $\iff$ irreducible.

Theorem ED is PID.

Theorem PID is UFD.

Theorem PID is BézoutD

3 Polynomials

3.1 Definitions

Split If a polynomial $f(x) \in F[x]$ factors into linear factors

$$f(x) = a(x - \alpha_1) \cdots (x - \alpha_n)$$

in an extension field E, we say that $f(x)$ **splits** in E.

Separable An irreducible polynomial $f(x) \in F[x]$ is **separable** if it has no multiple roots in any extension of F.

3.2 Polynomials over a Ring

Polynomials as a ring The polynomials $R[x]$ over a ring x is a ring.

Units Units of R are exactly units of $R[x]$.

Extension of a ring homomorphism If there is a ring homomorphism $\sigma : R \to S$, then it has an extension $\sigma^* : R[x] \to S[x]$, $f \to f^\sigma$.

Properties of the original ring carried over to polynomials The following are true.

1. R is an integral domain $\implies$ $R[x]$ is an integral domain.
2. R is a UFD $\implies$ $R[x]$ is a UFD.
3. R is a PID $\not\implies$ $R[x]$ is a PID.
4. F is a field $\implies$ $F[x]$ is an ED.

Degree formula Let R be an integral domain, then in $R[x]$,

$$\deg(fg) = \deg f + \deg g$$

Division algorithm Let R be a commutative ring with identity. If $g(x)$ has an invertible leading coefficient, then $g(x)$ can be used as a divisor, that is, for all $f(x) \in R[x]$, there exists unique $q(x)$, $r(x) \in R[x]$ such that

$$f(x) = q(x)g(x) + r(x)$$

where $\deg r < \deg g$.

Divisor theorem Let R be a commutative ring with identity. Let $f(x) \in R[x]$ and $a \in R$, then

$$f(a) = 0 \iff (x - a) \big| f(x)$$

Number of roots Let R be an integral domain, then $0 \neq f \in R[x]$ has at most $\deg f$ distinct roots in R.

Finite multiplicative subgroup of a field is cyclic Let F be a field, then any finite multiplicative subgroup of F^* is cyclic.

3.3 Polynomials over a Field

Polynomials as a domain The polynomials $F[x]$ over a field F is an ED.

Units Units of $F[x]$ are exactly units of F.

Degree formula In $F[x]$,

$$\deg(fg) = \deg f + \deg g$$

Division algorithm Omitted.

Divisor theorem Let $f(x) \in F[x]$ and $a \in F$, then

$$f(a) = 0 \iff (x-a) \big| f(x)$$

Number of roots $0 \neq f \in F[x]$ has at most $\deg f$ distinct roots in F.

Finite multiplicative subgroup of a field is cyclic Let F be a field, then any finite multiplicative subgroup of F^* is cyclic.

Field independence of gcd (1) Let $f(x)$, $g(x) \in F[x]$. Let $K \subset F$ be the smallest field containing the coefficient of $f(x)$ and $g(x)$.

1. The gcd of f, g does not depend on F.
2. $d = (f, g)$ has coefficients in K.
3. The Bézout equality holds in $K[x]$.

Field independence of gcd (2) Let $f(x)$, $g(x) \in F[x]$. If E is any extension of F, then f, g have a nonconstant common factor over $E \iff f$, g have a nonconstant common factor over F.

Existence of root in an extension Let $f(x) \in F[x]$ be a nonconstant polynomial. Then there exists an extension E of F and an $a \in E$ such that $f(a) = 0$.

Existence of a splitting field Let $f(x) \in F[x]$. There exists an extension of F over which $f(x)$ **splits**.

Common roots Let $f(x)$, $g(x) \in F[x]$, then

1. f, g have a nonconstant common factor over some extension of $F \iff$ f, g have a common root over some extension of F
2. f, g are relatively prime $\iff$ f, g have no common roots in any extension of F

Separability The following are true.

1. An irreducible polynomial is separable $\iff$ its derivative is nonzero.
2. All irreducible polynomials over a field of characteristic 0 are separable.
3. An irreducible polynomial $f(x)$ over a field of characteristic p is inseparable $\iff$ $f(x)$ has the form $f(x) = g(x^{p^d})$ where $d > 0$ and $g(x)$ is nonconstant.

4 Fields

4.1 Definitions

Conjugate Let $F < E$. Then $a, b \in E$ are said to be **conjugates** over F if $\min(a, F) = \min(b, F)$.

Algebraic element Let E/F. The following are equivalent.

1. $\alpha \in E$ is **algebraic** over F.
2. $\exists\, a_0, a_1, \cdots, a_n \in F\, (n \geqslant 1)$ not all equal to $0, a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$
3. $\exists\, f \in F[X],\ f(\alpha) = 0$
4. The homomorphism $F[X] \to E,\ f(X) \mapsto f(\alpha)$ has a nonzero kernel.

Primitive element In a simple extension $E = F(a)$, a is called a **primitive element** of E.

Separable element An algebraic element is called **separable** if its minimal polynomial is separable.

Tower A sequence of field extensions is referred to as a **tower** of fields.

Distinguished class of extensions A class $\mathcal{C}$ of field extensions is **distinguished** provided that it has the following properties.

1. (The tower property) For any 2-tower $F < K < E$,

$$(F < E) \in \mathcal{C} \iff (F < K) \in \mathcal{C},\ (K < E) \in \mathcal{C}$$

2. (The lifting property) The class $\mathcal{C}$ is closed under lifting by an arbitrary field, that is,

$$(F < E) \in \mathcal{C},\ F < K \implies (K < EK) \in \mathcal{C}$$

   The tower $K < EK$ is the **lifting** of $F < E$ by K.

3. (Closure under finite compositions) If EK is defined, then

$$(F < E) \in \mathcal{C},\ (F < K) \in \mathcal{C} \implies (F < EK) \in \mathcal{C}$$

Algebraic extension Let $F < E$. E is **algebraic** over F if every $a \in E$ is algebraic over F.

Transcendental extension E is **transcendental** over F if there exists a transcendental element in E over F.

Finitely generated extension Let $F < E$. If $E = F(S)$ where $S \subset E$ is a finite set, then we say E is **finitely generated** over F.

Separable extension An algebraic extension $F < E$ is **separable** if every element in E is separable over F.

Degreewise separable An algebraic extension $F < E$ is **degreewise separable** if $[E : F]_S = [E : F]$.

Degreewise separable An algebraic extension $F < E$ is **separably generated** if $E = F(S)$ where each $\alpha \in S$ is separable over F.

Simple extension E is a **simple** extension of F if $E = F(a)$ for some a.

Finite extension E is a finite extension of F if $[E : F]$ is finite.

Normal extension Let $F < E < \bar{F}$. The following are equivalent.

1. $F \lhd E$
2. E is a splitting field of a family $\mathcal{F}$ of polynomials over F.
3. E is invariant under every embedding $\sigma : E \hookrightarrow \bar{F}$ over F.
4. Every embedding of E into F is an automorphism of E.
5. Every irreducible polynomial over F that has one root in E splits in E.

Galois extension An extension that is both separable and normal is called a **Galois extension**.

4.2 Fields

Field The following are equivalent.

1. F is a field.
2. F is a commutative division ring.
3. F is a commutative ring with no proper ideal.

Sufficient condition for a field A finite integral domain is a field.

Wedderburn's theorem A finite division ring is a field.

Homomorphism Any nonzero field homomorphism is injective.

4.3 Extensions

Extension as vector space An extension field is a vector space over the original field.

Degree of extension Let $K \subset F \subset E$ be an extension tower, then

1. $[E : K] = [E : F][F : K]$
2. $\{x_i\}_{i \in I}$ is a basis for F over K, $\{y_i\}_{j \in J}$ is a basis for E over F, then $\{x_i y_j\}_{(i,j) \in I \times J}$ is a basis for E over K.

Distinguished classes of extensions The following are distinguished.

1. Algebraic extensions
2. Finite extensions
3. Finitely generated extensions
4. Separable extensions

Not distinguished extensions The following are not distinguished.

1. Transcendental extensions
2. Simple extensions (lifting property holds, upper and lower steps simple)
3. Normal extensions (lifting property holds, upper step normal)

Finitely generated extensions The following are true for finitely generated extensions.

1. $F(a_1, \cdots, a_n) = F(a_1, \cdots, a_k)(a_{k+1}, \cdots, a_n)$

2. $F(a_1, \cdots, a_n) = \left\{ \frac{f(a_1,\cdots,a_n)}{g(a_1,\cdots,a_n)} : f,\, g \in F[x_1, \cdots, x_n],\, g(a_1, \cdots, a_n) \neq 0 \right\}$
3. Finitely generated extensions are distinguished.

Simple extensions The following are true for simple extensions.

1. Simple extensions are not distinguished.
2. Full extension is simple implies upper step and lower step are simple.
3. Lifting property holds.

Finite and algebraic extensions The following are true.

1. A finite extension is algebraic.
2. An algebraic extension may not be finite.

Simple algebraic extensions Let $F < E$ and $a \in E$ be algebraic over F, then

1. The extension can be written as

$$\begin{aligned} F(a) &= \left\{ \frac{f(a)}{g(a)} : f,\, g \in F[x],\, g(a) \neq 0 \right\} \\ &= \left\{ f(a) : f \in F[x] \right\} \\ &= \left\{ f(a) : f \in F[x],\, \deg f < \deg \mathrm{Irr}(a, F, X) \right\} \end{aligned}$$

2. The extension is isomorphic to the exterior extension.

$$F(a) = F[x]/(p_a(x))$$

3. $F(a)$ is finite over F and $[F(a) : F] = \deg(p_a(x))$. The set $\mathcal{B} = \{1, a, \cdots, a^{d-1}$ is a vector space basis for E over F.
4. If a, $b \in E$ are conjugate over F then $F(a) = F(b)$.

Simple extensions and algebraic extensions The following are equivalent for a simple extension $F < F(a)$.

1. a is algebraic.
2. $F(a)$ is algebraic.
3. $F(a)$ is finite.

Finitely generated algebraic extensions Let $E = F(a_1, \cdots, a_n)$ be finitely generated over F by algebraic elements over F.

1. $E = F(a)$ for some algebraic element $a \in E \iff$ there is only a finite number of intermediate fields $F < K < E$.
2. In this case, if E is an infinite field, then $E = F(a)$ where a has the form
$$a = \lambda_1 a_1 + \cdots + \lambda_n a_n$$

Simple transcendent extension Let E/F and $\alpha \in E$ is transcendent over F, then $F(\alpha) \cong F(X)$.

Finite extensions The following are true.

1. An extension is finite $\iff$ it is finitely generated by algebraic elements.
2. A finite extension is algebraic.
3. Finite extensions are distinguished.
4. (The lifting degree) $[EK : K] \leqslant [E : F]$

Algebraic extensions The following are true.

1. The set of all algebraic elements over F is a field called the **algebraic closure** of F.
2. Algebraic extensions are distinguished.
3. Algebraic extensions are closed under taking arbitrary composites.

Finite extensions and algebraic extensions The following are equivalent for $F < E$.

1. $F < E$ is finite.
2. $F < E$ is finitely generated by algebraic elements.
3. $F < E$ is algebraic and finitely generated.

Existence of primitive elements Any extension of the form
$$F < F(\alpha_1, \cdots, \alpha_n, \beta)$$
where α_i is separable over F and β is algebraic over F is a simple extension. Moreover, if F is infinite, this extension has infinitely many primitive elements, of the form
$$a_1\alpha_1 + \cdots + a_n\alpha_n + b\beta$$
where $a_i, b \in F$.

Existence of primitive elements (for finite extensions) For any finite extension $F < E$, there exists $\beta \in E$ such that

$$F(\beta) : F] = [E : F]_s$$

If F is infinite, there exist infinitely many such elements β.

Theorem of the primitive element If $F < E$ is finite and separable, say

$$F < F(\alpha_1, \cdots, \alpha_n)$$

where α_i is separable over F then $F < E$ is simple. If F is infinite, there exists infinitely many primitive elements for E over F of the form

$$a_1\alpha_1 + \cdots + a_n\alpha_n$$

Normal extensions The following are true.

1. Normal extensions are not distinguished.
2. Full extension normal implies upper step normal.
3. Lifting of a normal extension is normal.
4. Arbitrary composites and intersections of normal are normal.

Galois extensions See the next section.

4.4 Embeddings

Ring homomorphism from a field Any ring homomorphism from a field into a ring is either the zero mapping or a monomorphism.

Embeddings preserve factorizations and roots If $\sigma : F \hookrightarrow L$ and $f(x) \in F[x]$, then

1. $f(x) = p(x)q(x) \iff f^\sigma(x) = p^\sigma(x)q^\sigma(x)$
2. $p(a) = 0$, $a \in F \iff p^\sigma(\sigma a) = 0$

Embeddings preserve the lattice structure If $\sigma : F \hookrightarrow L$ and $\{E_i : i \in I\}$ is a family of subfields of F, then

$$\sigma(\bigcap E_i) = \bigcap \sigma E_i, \quad \sigma(\bigvee E_i) = \bigvee \sigma E_i$$

Embeddings preserve adjoining If $\sigma : K \hookrightarrow L$ and $F < K$, $S \subset K$, then

$$\sigma(F(S)) = F^\sigma(\sigma S)$$

Embeddings preserve being algebraic Let $\sigma : F \hookrightarrow L$ and $F < E$. If $\bar{\sigma} : E \hookrightarrow L$ is an extension of σ, then

$$F < E \text{ is algebraic } \implies \sigma F < \bar{\sigma} E \text{ is algebraic}$$

Embeddings preserve the algebraic closures Omitted.

Embedding is automorphism

$$F < E \text{ is algebraic } \implies \mathrm{Hom}_F(E, E) = \mathrm{Aut}_F(E)$$

Simple algebraic extensions Let $F < E$ and $a \in E$ be algebraic over F, with $\min(a, F) = p_a(x)$. Let $\sigma : F \hookrightarrow L$, where L is algebraically closed.

1. $b \in L$, $p^\sigma(b) = 0 \implies \sigma$ can be extended to an embedding $\sigma_b : F(a) \hookrightarrow L$ for which $\sigma_b a = b$.
2. Any extension of σ to $F(a)$ can only have the form σ_b, $p^\sigma(b) = 0$.
3. The number of extensions of σ to $F(a)$ equals the number of distinct roots of $\min(a, F)$.

5 Galois Theory

5.1 Definitions

Galois connection Let P and Q be partially ordered sets. A **Galois connection** on the pair (P, Q) is a pair (Π, Ω) of maps $\Pi : P \to Q$ and $\Omega : Q \to P$, where we write $\Pi = p^*$ and $\Omega(q) = q'$, with the following properties:

1. (**Order-reversing** or **antitone**) For all $p, r \in P$ and $q, s \in Q$,

$$p \leqslant r \implies p^* \geqslant r^*$$

$$q \leqslant s \implies q' \geqslant s'$$

2. (**Extensive**) For all $p \in P$, $q \in Q$,

$$p \leqslant p^{*\prime} \text{ and } q \leqslant q'^*$$

Closure operation Let P be a partially ordered set. A map $p \mapsto \mathrm{cl}(p)$ on P is an (algebraic) **closure operation** if the following properties hold for all $p, q \in P$:

1. (**Extensive**)
$$p \leqslant \mathrm{cl}(p)$$
2. (**Idempotent**)
$$\mathrm{cl}(\mathrm{cl}(p)) = \mathrm{cl}(p)$$
3. (**Isotone**)
$$p \leqslant q \implies \mathrm{cl}(p) \leqslant \mathrm{cl}(q)$$

Closed element An element $p \in P$ is said to be **closed** if $\mathrm{cl}(p) = p$. The set of all closed elements in P is denoted by $\mathrm{Cl}(P)$.

Indexed Galois connection A Galois connection (Π, Ω) on (P, Q) is **indexed** if

1. For each $p, r \in P$ with $p \leqslant r$, there exists a number $(r : p)_P \in \mathbb{Z}^+ \cup \{\infty\}$, called the **degree**, or **index** of r over p.
2. For each $q, s \in P$ with $q \leqslant s$, there exists a number $(s : q)_Q \in \mathbb{Z}^+ \cup \{\infty\}$, called the **degree**, or **index** of s over q.
3. (**Degree is multiplicative**) Both in P and Q,
$$a \leqslant b \leqslant c \implies (c : a) = (c : b)(b : a)$$
4. (Π **and** Ω **are degree-nonincreasing**)
$$p, r \in P,\ p \leqslant r \implies (q^* : r^*) \leqslant (r : q)$$
$$q, s \in Q,\ q \leqslant s \implies (q' : s') \leqslant (s : q)$$
5. (**Equality by degree**) Both in P and Q,
$$(s : t) = 1 \iff s = t$$

Galois group The **Galois group** of a field extension $F < E$, denoted by $G_F(E)$ or $G(E/F)$, is the group $\mathrm{Aut}_F(E)$ of all automorphisms of E over F. The group $G_F(E)$ is also called the **Galois group of** E **over** F.

Fixed field Let $G_F(E)$ be the Galois group of E over F and $H < G_F(E)$, then $\mathrm{fix}(H)$ is defined as
$$\mathrm{fix}(H) = \{\alpha \in E : \sigma\alpha = \alpha,\ \forall \sigma \in H$$
that is, the biggest subfield fixed under each element in H, and is called the **fixed field** of H.

Galois correspondence The pair (Π, Ω) of maps on the complete lattices of all intermediate fields $\mathcal{F}$ of $F < E$ and all subgroups $\mathcal{G}$ of $G_F(E)$ (both ordered by set inclusion) in which Π assigns to each intermediate field K the subgroup of all automorphisms that fix K, and in which Ω assigns to each subgroup H the fixed field of H

$$\Pi : \mathcal{F} \to \mathcal{G},\ K \mapsto G_K(E)$$

$$\Omega : \mathcal{G} \to \mathcal{F},\ H \to \text{fix}(H)$$

is a Galois connection called the **Galois correspondence** of the extension $F < E$.

Conjugate (of fields) Let $F < K < E$, $L < E$. If there is a $\sigma \in G_F(E)$ for which $\sigma K = L$, then K and L are said to be **conjugate**.

5.2 Galois Connections

Let (Π, Ω) be a Galois connection on (P, Q).

Galois connection induces closure operations The maps

$$\text{cl}(p) = (\Omega\Pi)(p) = p^{*\prime} \text{ and } \text{cl}(q) = (\Pi\Omega)(q) = q'^{*}$$

are closure operations on P and Q respectively, and satisfy

1. $p^{*\prime *} = p^*$, that is, $\text{cl}(p^*) = \text{cl}(p)^* = p^*$.
2. $q'^{*\prime} = q'$, that is, $\text{cl}(q') = \text{cl}(q)' = q'$.

Galois connections are surjective onto the closures The maps $\Pi : P \to \text{Cl}(Q)$ and $\Omega : Q \to \text{Cl}(P)$ are surjective and the restricted maps $\Pi : \text{Cl}(P) \to \text{Cl}(Q)$ and $\Omega : \text{Cl}(Q) \to \text{Cl}(P)$ are inverse bijections.

Closure of a lattice Let (P, Q) be a pair of lattices. If P is a complete lattice, then so is $\text{Cl}(p)$, under the same meet as P. The same holds for Q.

De Morgan's Laws for Galois connections on lattices Let (Π, Ω) be a Galois connection on a pair (P, Q) of lattices. Then De Morgan's Laws hold in $\text{Cl}(P)$ and $\text{Cl}(Q)$, that is, for $p, r \in \text{Cl}(P)$ and $q, s \in \text{Cl}(Q)$,

$$(p \wedge r)^* = p^* \vee r^*, \quad (p \vee r)^* = p^* \wedge r^*$$

$$(q \wedge s)^* = q^* \vee s^*, \quad (q \vee s)^* = q^* \wedge s^*$$

Galois connections are degree-preserving on closed elements If $p, r \in \mathrm{Cl}(P)$, then

$$p \leqslant r \implies (r : p) = (p^* : r^*)$$

The same holds for Q.

Finite extension of closed elements are closed

$$p \in \mathrm{Cl}(P),\ (r : p) < \infty \implies r \in \mathrm{Cl}(P)$$

5.3 Galois Correspondence

Galois correspondence The following are true.

1. The Galois correspondence is a Galois connection.
2. The Galois correspondence is indexed.
3. The restriction of the Galois correspondence to closed elements are order-reversing, degree-preserving inverse bijections as well as lattice anti-isomorphisms, that is, if K_i are closed intermediate fields and H_i are closed subgroups, then

$$G_{\bigcap K_i}(E) = \bigvee G_{K_i}(E), \qquad G_{\bigvee K_i}(E) = \bigcap G_{K_i}(E)$$
$$\mathrm{fix}\left(\bigcap H_i\right) = \bigvee \mathrm{fix}(H_i), \qquad \mathrm{fix}(\bigvee H_i) = \bigcap \mathrm{fix}(H_i)$$

4. The class of Galois extensions is not distinguished.
5. Full extension Galois implies upper step Galois.
6. The class of Galois extensions is closed under lifting.
7. The class of Galois extensions is closed under arbitrary composites and intersections.

Closed intermediate fields Let $F < E$ be algebraic. The closed intermediate fields are precisely the fixed fields, that is, the fields of the form $\mathrm{fix}(H)$ for some $H \leqslant G_F(E)$. The following are true.

1. An intermediate field K is closed if and only if $K < E$ is Galois.
2. Any extension of a closed intermediate field is closed. In particular, if F is closed, then $F < E$ is completely closed.
3. If $F < \mathrm{cl}(K) < L < E$ and

$$[L : K] = (G_K(E) : G_L(E)) < \infty$$

then K is closed. In particular, if

$$[E : K] = |G_K(E)| < \infty$$

then K is closed.

Closed groups The closed subgroups of $G_F(E)$ are precisely the Galois groups of E, that is, the subgroups of the form $G_K(E)$, for some intermediate field K.

1. Any finite extension of a closed subgroup is closed.
2. $G_E(E) = \{\text{id}\}$ is closed and so any finite subgroup of $G_F(E)$ is closed.
3. When $F < E$ is finite, so is $G_F(E)$ and so $G_E(E) = \{\text{id}\} < G_F(E)$ is completely closed.

Finite Galois extension is completely closed If F is a finite Galois extension, then the correspondence is completely closed.

5.4 Normal Extensions

Conjugate fields and their Galois groups The following are true.

1. If $F < K < E$, then for any $\sigma \in \text{Hom}_F(E, \overline{E})$,

$$\sigma G_K(E)\sigma^{-1} = G_{\sigma K}(\sigma E)$$

2. If $F \lhd K < E$, then for any $\sigma \in \text{Hom}_F(E, \overline{E})$,

$$\sigma G_K(E)\sigma^{-1} = G_K(\sigma E)$$

3. If $F < K < E$ with $F \lhd E$, then for any $\sigma \in \text{Hom}_F(E, \overline{E})$,

$$\sigma G_K(E)\sigma^{-1} = G_{\sigma K}(E)$$

4. If $F < K < E$, $L < E$, with $F < E$ Galois, then

$$K \text{ and } L \text{ are conjugate} \iff G_K(E) \text{ and } G_L(E) \text{ are conjugate}$$

Normality Let $F < K < E$. Let $\phi : G_F(E) \to \text{Hom}_F(K, E)$ be the restriction map

$$\phi(\sigma) = \sigma|_K$$

1. If $F \lhd K$ then $G_K(E) \lhd G_F(E)$ and ϕ induces an embedding

$$\frac{G_F(E)}{G_K(E)} \hookrightarrow G_F(K)$$

   which is an isomorphism if the full extension $F < E$ is normal.

2. If $G_K(E) \lhd G_F(E)$ and in addition, $F \lhd E$ and K is closed (that is, $K < E$ is Galois), then $F \lhd K$ and ϕ induces an isomorphism

$$\frac{G_F(E)}{G_K(E)} \cong G_F(K)$$

3. If $F < E$ is Galois, then $F \lhd K \iff G_K(E) \lhd G_F(E)$.

5.5 Galois Groups

The Galois group of a lifting (1) Let $F < E$ be normal and let $F < K$. The restriction map

$$\phi : G_K(EK) \to G_{E\cap \mathrm{cl}(K)}(E)$$

where $\mathrm{cl}(K) = \mathrm{fix}(G_K(EK))$, defined by $\phi\sigma = \sigma|_E$ is an isomorphism and

$$G_K(EK) \cong G_{E\cap \mathrm{cl}(K)}(E)$$

The Galois group of a lifting (2) The lifting $K < EK$ of a Galois extension $F < E$ by an arbitrary extension $F < K$ is Galois. Moreover, the restriction map $\phi : G_K(EK) \to G_{E\cap K}(E)$ defined by $\phi\sigma = \sigma|_E$ is an isomorphism and

$$G_K(EK) \cong G_{E\cap K}(E)$$

Also,

1. $F = E \cap K \implies G_K(EK) \cong G_F(E)$
2. If $F < E$ is finite, then $G_K(EK) \implies G_F(E) \implies E \cap K = F$

Corollary: degree of a lifting Suppose $F < E$ is finite Galois and $F < K$. The following are true.

1. $[EK : K] = [E : E \cap K]$ and so $[EK : K] \big| [E : F]$
2. If $F < K$ is finite, then $[EK : F] = [E : E \cap K][K : F]$
3. If $F < K$ is finite, then $[EK : F] \big| [E : F][K : F]$, with equality if and only if $E \cap K = F$

4. The formulas for multiple extensions are omitted.

The Galois group of a composite

1. Let $\mathcal{F} = \{E_i \mid i \in I\}$ be a family of fields, with $F < E_i$ normal for all $i \in I$. Let $G = \prod G_F(E_i)$ be the direct product of the Galois groups $G_F(E_i)$ and let $\pi_i : G \to G_F(E_i)$ be projection onto the ith coordinate. Then the map
$$\phi : G_F(\bigvee E_i) \to \prod G_F(E_i)$$

6 Vector Spaces

6.1 Correspondence Theorems

The correspondence theorem (for vector spaces) Let S be a subspace of V. Then the function that assigns to each intermediate subspace $S \subset T \subset V$ the subspace T/S of V/S is an order-preserving (with respect to set inclusion) one-to-one correspondence between the set of all subspaces of V containing and the set of all subspaces of V/S.

6.2 Decompositions of Linear Operators and Matrices

Polar decomposition (of an operator) Let τ be a nonzero linear operator on a finite-dimensional complex inner product space V.

1. There exists a positive operator ρ and a unitary operator ν for which $\tau = \nu\rho$. Moreover, ρ is unique and if τ is invertible, then ν is also unique.
2. Similarly, there exists a positive operator σ and a unitary operator μ for which $\tau = \sigma\mu$. Moreover, σ is unique and if τ is invertible, then μ is also unique.
3. (Polar decomposition) Let τ There is a positive operator ρ and a self-adjoint operator σ for which τ has the polar decomposition
$$\tau = \rho e^{i\sigma}$$
Moreover, ρ is unique and if τ is invertible, then σ is also unique.

6.3 Isomorphism Theorems

The isomorphism theorem (for vector spaces) Let $\tau : V \to W$ be a linear transformation. Then the linear transformation $\tau' : V/\ker(\tau) \to W$ defined by

$$\tau'(v + \ker(\tau)) = \tau v$$

is injective and

$$\frac{V}{\ker(\tau)} \xrightarrow{\cong} \operatorname{im}(\tau)$$

6.4 Riesz Representation Theorem

The Riesz representation theorem (for inner product spaces) Let V be a finite-dimensional inner product space.

1. The map $\tau : V \to V^*$ defined by

   $$\tau x = \langle \cdot, x \rangle$$

   is a conjugate isomorphism. In particular, for each $f \in V^*$, there exists a unique vector $x \in V$ for which $f = \langle \cdot, x \rangle$, that is,

   $$fv = \langle v, x \rangle$$

   for all $v \in V$. We call x the Riesz vector for f and denote it by R_f.

2. The map $R : V^* \to V$ defined by

   $$Rf = R_f$$

   is also a conjugate isomorphism, being the inverse of τ. We will call this map the Riesz map.

The Riesz representation theorem (for metric spaces) Let V be a finite-dimensional nonsingular metric vector space. The map $\tau : V \to V^*$ defined by

$$\tau x = \langle \cdot, x \rangle$$

is an isomorphism from V to V^*. It follows that for each $f \in V^*$ there exists a unique vector $x \in V$ for which

$$fv = \langle v, x \rangle$$

for all $v \in V$.

The Riesz representation theorem (for metric subspaces) Let S be a subspace of a metric vector space V. If either V or S is nonsingular, the linear map $\tau : V \to S^*$ defined by

$$\tau x = \langle \cdot, x \rangle|_S$$

is surjective and has kernel $S^\perp$. Hence, for any linear functional $f \in S^*$, there is a (not necessarily unique) vector $x \in V$ for which $fs = \langle s, x \rangle$ for all $x \in S$. Moreover, if S is nonsingular, then x can be taken from S, in which case it is unique.

6.5 Spectral Theorem for Normal Operators

The spectral theorem for normal operators: complex case Let V be a finite-dimensional complex inner product space and let $\tau \in \mathcal{L}(V)$. The following are equivalent:

1. τ is normal.
2. τ is unitarily diagonalizable, that is, $V_\tau = \mathcal{E}_{\lambda_1} \odot \cdots \odot \mathcal{E}_{\lambda_k}$
3. τ has an orthogonal spectral resolution

$$\tau = \lambda_1 \rho_1 + \cdots + \lambda_k \rho_k$$

where $\rho_1 + \cdots + \rho_n = \mathrm{id}$ and ρ_i is orthogonal for all i, in which case, $\{\lambda_1, \cdots, \lambda_k\}$ is the spectrum of τ and

$$\mathrm{im}(\rho_i) = \mathcal{E}_{\lambda_i}, \quad \ker(\rho_i) = \bigodot_{j \neq i} \mathcal{E}_{\lambda_j}$$

The spectral theorem for normal operators: real case A linear operator τ on a finite-dimensional real inner product space is normal if and only if

$$V = \mathcal{E}_{\lambda_1} \odot \cdots \odot \mathcal{E}_{\lambda_k} \odot W_1 \odot \cdots \odot W_m$$

where $\{\lambda_1, \cdots, \lambda_k\}$ is the spectrum of τ and each W_i is an indecomposable two-dimensional τ-invariant subspace with an ordered basis $\mathcal{B}_i$ for which

$$[\tau]_{\mathcal{B}} = \begin{pmatrix} a_i & -b_i \\ b_i & a_i \end{pmatrix}$$

6.6 Structure Theorem for Normal Operators

The structure theorem for normal operators: complex case Let V be a finite-dimensional complex inner product space.

1. The following are equivalent for $\tau \in \mathcal{L}(V)$:
   - τ is normal.
   - τ is unitarily diagonalizable, that is, $V_\tau = \mathcal{E}_{\lambda_1} \odot \cdots \odot \mathcal{E}_{\lambda_k}$
   - τ has an orthogonal spectral resolution
   $$\tau = \lambda_1 \rho_1 + \cdots + \lambda_k \rho_k$$
2. Among the normal operators, the Hermitian operators are precisely those for which all complex eigenvalues are real.
3. Among the normal operators, the unitary operators are precisely those for which all complex eigenvalues have norm 1.

The structure theorem for normal operators: real case Let V be a finite-dimensional complex inner product space.

1. τ is normal if and only if
   $$V = \mathcal{E}_{\lambda_1} \odot \cdots \odot \mathcal{E}_{\lambda_k} \odot W_1 \odot \cdots \odot W_m$$
   where $\{\lambda_1, \cdots, \lambda_k\}$ is the spectrum of τ and each W_i is an indecomposable two-dimensional τ-invariant subspace with an ordered basis $\mathcal{B}_i$ for which
   $$[\tau]_{\mathcal{B}} = \begin{pmatrix} a_i & -b_i \\ b_i & a_i \end{pmatrix}$$
2. Among the real normal operators, the symmetric operators are those for which there are no subspaces W_i in the aforementioned decomposition. Hence, the following are equivalent for $\tau \in \mathcal{L}(V)$:
   - τ is symmetric.
   - τ is orthogonally diagonalizable.
   - τ has the orthogonal spectral resolution
   $$\tau = \lambda_1 \rho_1 + \cdots + \lambda_k \rho_k$$
3. Among the real normal operators, the orthogonal operators are precisely those for which the eigenvalues are equal to ± 1 and the matrices $[\tau]_{\mathcal{B}_i}$ described in the aforementioned decomposition have rows (and columns) of norm 1, that is,
   $$[\tau]_{\mathcal{B}_i} = \begin{pmatrix} \sin\theta & -\cos\theta \\ \cos\theta & \sin\theta \end{pmatrix}$$
   for some $\theta \in \mathbb{R}$.

6.7 Structure Theorem for Normal Operators

The structure theorem for normal matrices: complex case

1. A complex matrix A is normal $\iff$ it is unitarily diagonalizable, that is, there is a unitary matrix U for which
$$UAU^* = \operatorname{diag}(\lambda_1, \cdots, \lambda_k)$$
2. A complex matrix A is Hermitian $\iff$ it is unitarily diagonalizable and all eigenvalues of A are real.
3. A complex matrix A is unitary $\iff$ it is unitarily diagonalizable and all eigenvalues of A have norm 1.

The structure theorem for normal matrices: real case

1. A real matrix A is normal $\iff$ there is an orthogonal matrix O for which
$$OAO^{\mathrm{T}} = \operatorname{diag}\left(\lambda_1, \cdots, \lambda_k, \begin{pmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{pmatrix}, \cdots, \begin{pmatrix} a_m & -b_m \\ b_m & a_m \end{pmatrix}\right)$$
2. A real matrix A is symmetric $\iff$ it is orthogonally diagonalizable, that is, there is an orthogonal matrix O for which
$$OAO^{\mathrm{T}} = \operatorname{diag}(\lambda_1, \cdots, \lambda_k)$$
3. A real matrix is orthogonal $\iff$ there is an orthogonal matrix O for which
$$OAO^{\mathrm{T}} = \operatorname{diag}\left(\lambda_1, \cdots, \lambda_k, \begin{pmatrix} \sin\theta_1 & -\cos\theta_1 \\ \cos\theta_1 & \sin\theta_1 \end{pmatrix}, \cdots, \begin{pmatrix} \sin\theta_m & -\cos\theta_m \\ \cos\theta_m & \sin\theta_m \end{pmatrix}\right)$$

7 Modules

7.1 Isomorphism Theorems

The isomorphism theorem (for modules) Let $\tau : M \to N$ be an R-homomorphism. Then the map $\tau' : M/\ker(\tau) \to N$ defined by
$$\tau'(v + \ker(\tau)) = \tau v$$
is an R-embedding and so
$$\frac{M}{\ker(\tau)} \xrightarrow{\cong} \operatorname{im}(\tau)$$

7.2 Correspondence Theorems

The correspondence theorem (for modules) Let S be a submodule of M. Then the function that assigns to each intermediate submodule $S \subset T \subset M$ the quotient space T/S of M/S is an order-preserving (with respect to set inclusion) one-to-one correspondence between submodules of M containing S and all submodules of M/S.

7.3 Decompositions of Modules

Primary decomposition (of a module) Let M be a torsion module over a principal ideal domain R, with order

$$\mu = p_q^{e_1} \cdots p_n^{e_n}$$

where the p_i's are distinct nonassociate primes in R.

1. M is the direct sum

$$M = M_{p_1} \oplus \cdots \oplus M_{p_n}$$

where

$$M_{p_i} = \frac{\mu}{p_i^{e_i}} M = \{v \in M : p_i^{e_i} v = 0\}$$

is a primary submodule of order $p_i^{e_i}$. This decomposition of M into primary submodules is called the primary decomposition of M.

2. The primary decomposition of M is unique up to order of the summands. That is, if

$$M = N_{q_1} \oplus \cdots \oplus N_{q_m}$$

where N_{q_i} is primary of order $q_i^{f_i}$ and $q_1, \cdots, q_m$ are distinct nonassociate primes, then $m = n$ and, after a possible reindexing, $N_{q_i} = M_{p_i}$. Hence, $f_i = e_i$ and $q_i \sim p_i$, for $i = 1, \cdot, n$.

3. Two R-modules M and N are isomorphic $\iff$ the summands in their primary decompositions are pairwise isomorphic, that is, if

$$M = M_{p_1} \oplus \cdots \oplus M_{p_n}$$

and

$$N = N_{q_1} \oplus \cdots \oplus N_{q_m}$$

are primary decompositions, then $m = n$ and, after a possible reindexing, $M_{p_i} \approx N_{q_i}$ for $i = 1, \cdots, n$.

Cyclic decomposition (of a primary module) Let M be a primary finitely generated torsion module over a principal ideal domain R, with order p^e.

1. M is a direct sum
$$M = \langle\langle v_1 \rangle\rangle \oplus \cdots \oplus \langle\langle v_n \rangle\rangle$$
of cyclic submodules with annihilators $\operatorname{ann}(\langle\langle v_i \rangle\rangle) = \langle p^{e_i} \rangle$, which can be arranged in ascending order
$$\operatorname{ann}(\langle\langle v_1 \rangle\rangle) \subseteq \cdots \subseteq \operatorname{ann}(\langle\langle v_n \rangle\rangle)$$
or equivalently,
$$e = e_1 \geqslant \cdots \geqslant e_n$$

2. As to uniqueness, suppose that M is also the direct sum
$$M = \langle\langle u_1 \rangle\rangle \oplus \cdots \oplus \langle\langle u_m \rangle\rangle$$
of cyclic submodules with annihilators $\operatorname{ann}(\langle\langle u_i \rangle\rangle) = \langle q^{f_i} \rangle$, arranged in ascending order
$$\operatorname{ann}(\langle\langle u_1 \rangle\rangle) \subseteq \cdots \subseteq \operatorname{ann}(\langle\langle u_m \rangle\rangle)$$
or equivalently
$$f_1 \geqslant \cdots \geqslant f_m$$
Then the two chains of annihilators are identical, that is, $m = n$ and
$$\operatorname{ann}(\langle\langle u_i \rangle\rangle) = \operatorname{ann}(\langle\langle v_i \rangle\rangle)$$
for all i. Thus, $p \sim q$ and $f_i = e_i$ for all i.

3. Two p-primary R-modules
$$M = \langle\langle v_1 \rangle\rangle \oplus \cdots \oplus \langle\langle v_n \rangle\rangle$$
and
$$N = \langle\langle u_1 \rangle\rangle \oplus \cdots \oplus \langle\langle u_m \rangle\rangle$$
are isomorphic $\iff$ they have the same annihilator chains, that is, $m = n$ and, after a possible reindexing
$$\operatorname{ann}(\langle\langle u_i \rangle\rangle) = \operatorname{ann}(\langle\langle v_i \rangle\rangle)$$

Primary cyclic decomposition (of a module) Let M be a finitely generated torsion module over a principal ideal domain R.

1. If M has order
$$\mu = p_1^{e_1} \cdots p_n^{e_n}$$
where the p_i's are distinct nonassociate primes in R, then M can be uniquely decomposed (up to the order of the summands) into the direct sum
$$M = M_{p_1} \oplus \cdots \oplus M_{p_n}$$
where
$$M_{p_i} = \frac{\mu}{p_i^{e_i}} M = \{v \in M : p_i^{e_i} v = 0\}$$
is a primary submodule with annihilator $\langle p_i^{e_i} \rangle$. Finally, each primary submodule M_{p_i} can be written as a direct sum of cyclic submodules, so that
$$M = \underbrace{[\langle\langle v_{1,1} \rangle\rangle \oplus \cdots \oplus \langle\langle v_{1,k_1} \rangle\rangle]}_{M_{p_1}} \oplus \cdots \oplus \underbrace{[\langle\langle v_{n,1} \rangle\rangle \oplus \cdots \oplus \langle\langle v_{n,k_n} \rangle\rangle]}_{M_{p_n}}$$
where $\operatorname{ann}(\langle\langle v_{i,j} \rangle\rangle) = \langle p_i^{e_{i,j}} \rangle$ and the terms in each cyclic decomposition can be arranged so that, for each i,
$$\operatorname{ann}(\langle\langle v_{i,1} \rangle\rangle) \subseteq \cdots \subseteq \operatorname{ann}(\langle\langle v_{i,k_i} \rangle\rangle)$$
or, equivalently,
$$e_i = e_{i,1} \geqslant \cdots \geqslant e_{i,k_i}$$
2. As for uniqueness, suppose that
$$M = \underbrace{[\langle\langle u_{1,1} \rangle\rangle \oplus \cdots \oplus \langle\langle u_{1,j_1} \rangle\rangle]}_{N_{q_1}} \oplus \cdots \oplus \underbrace{[\langle\langle u_{m,1} \rangle\rangle \oplus \cdots \oplus \langle\langle u_{m,j_m} \rangle\rangle]}_{N_{q_m}}$$
is also a primary cyclic decomposition of M. Then,
   - The number of summands is the sam in both decompositions; in fact, $m = n$ and after possible reindexing, $k_u = j_u$ for all u.
   - The primary submodules are the same; that is, after possible reindexing, $q_i \sim p_i$ and $N_{q_i} = M_{p_i}$.
   - For each primary submodule pair $N_{q_i} = M_{p_i}$, the cyclic submodules have the same annihilator chains; that is, after possible reindexing,
   $$\operatorname{ann}(\langle\langle u_{i,j} \rangle\rangle) = \operatorname{ann}(\langle\langle v_{i,j} \rangle\rangle)$$
   for all i, j.

   In summary, the primary submodules and annihilator chains are uniquely determined by the module M.
3. Two R-modules M and N are isomorphic $\iff$ they have the same annihilator chains.