ABSTRACT ALGEBRA

YUNZHI ZHANG

1. Group

1.1. Subgroup.

- Let H be a subgroup of G, $a \in G$. $Ha = \{ha|h \in H\}$ is a right coset of H in G, $[a] = \{x \in G|a \equiv x \mod H\}$ is the equivalence class of a in G. $Ha = [a]$.
  Equivalence class yields a partition of G, thus right cosets of H is G are disjoint.
  If H is a finite group, then any right coset of H in G has $o(H)$ elements. If G is a finite group, then $i_G(H) = o(G)/o(H)$.
- If $p = o(G)$ is a prime, then G is cyclic.
- Let H, K be subgroups of G. $HK = \{x \in G|x = hk, h \in H, k \in K\}$ is a subgroup of G iff $HK = KH$. It is trivially true when G is abelian. $o(HK) = \frac{o(H)o(K)}{o(H \cap K)}$.
- A subgroup N of G is a normal subgroup of G if any of the following holds:
  (1) $\forall g \in G, n \in N, gng^{-1} \in N$.
  (2) $\forall g \in G, gNg^{-1} \subset N$.
  (3) $\forall g \in G, gNg^{-1} = N$.
  (4) Every left coset of N is a right coset of N in G.
  (5) $\forall g \in G, gN = Ng$.
  (6) Product of two right cosets of N in G is a right coset of N in G.
  (7) $\forall a, b \in N, NaNb = Nab$.
- $HH = H$.

1.2. Homomorphism.

- Let G/N denote the collection of right cosets of N in G. Then G/N is the quotient group of G by N.
  Define $\phi : G \to G/N, x \mapsto Nx$. Then ϕ is a homomorphism of G onto G/N.
- If ϕ is a homomorphism of G into $\bar{G}$, define $K_\phi = \{x \in G|\phi(x) = \bar{e}\}$ to be the kernel of ϕ. K is a normal subgroup of G. $\phi^{\text{pre}}(\bar{g}) = Kx \subset G/K$, where $\phi(x) = \bar{g}$.
- Let ϕ be a homomorphism of G onto $\bar{G}$ with kernel K. Then $G/K \approx \bar{G}$.
  Define $\psi : G/K \to \bar{G}, X \mapsto \phi(g)$ where $X = Kg$, and ψ is an isomorphism from G/K to $\bar{G}$.
  There is a one-to-one correspondence between homomorphic images of G and normal subgroups of G.
- (Cauchy's Theorem for abelian groups) Suppose G is a finite abelian group, $p \mid o(G)$, p is prime. Then there is an element $a \neq e \in G$ such that $a^p = e$.

Date: May 17, 2019.

Proof. By induction. If $o(G) = 1$, vacuously true. Assume true for any group with order less than G.

i If $o(G) = p$, then it is cyclic. Obvious.

ii If $o(G) \neq p$, then there exists nontrivial subgroup N. If $p \mid o(N)$, true by assumption.

iii If $p \nmid o(N)$, then $p \mid o(G/N)$. By assumption $\exists X \in G/N, X^p = N, X \neq N$. Let $X = Nb, b \in G$, then $b^p \in N, b \notin N$.

$c = b^{o(N)}$, then $c^p = (b^p)^{o(N)} = e$ by Lagrange's.

If $c = e$, then $X^{o(N)} = N, X^p = N, (p, o(N)) = 1$, then $X = N$, contradiction. Thus $c \neq e$.

□

- (Sylow's Theorem for abelian groups) If G is an abelian group of order $o(G)$, p is prime, $p^\alpha \mid o(G), p^{\alpha+1} \nmid o(G)$, then G has a subgroup of order p^α. Such subgroup is unique.

Proof. If $\alpha = 0$, (e) satisfies the conditions.

If not, let $S = \{x \in G | \exists n, x^{p^n} = e\}$. S is a subgroup of G, $o(S) = p^\beta$ for some $0 < \beta <= \alpha$ (by showing S is non-empty, no prime number other than p divides $o(S)$ by contradicting Cauchy's, and $o(S) \mid o(G)$).

Suppose $\beta < \alpha$, than $p \mid o(G/S)$. By Cauchy's, $\exists x \in G$ such that $Sx^p = S, Sx \neq S$. $x^p \in S$ gives $x^{p \cdot o(S)} = x^{p^{\beta+1}} = e$, then $x \in S$, contradiction. Thus $\beta = \alpha$. □

- Let ϕ be a homomorphism of G onto $\bar{G}$ with kernel K. There is a one-to-one correspondance between H a subgroup of G containing K, and $\bar{H}$ a subgroup of $\bar{G}$, where $\bar{H} = \phi(H)$, $H = \phi^{\text{pre}}(\bar{H})$. Moreover, if $\bar{H}$ is normal, then H is normal.
- Let ϕ be a homomorphism of G onto $\bar{G}$ with kernel K, $\bar{N}$ a normal subgroup of $\bar{G}$, $N = \phi^{\text{pre}}(\bar{N})$. Then $G/N \approx \bar{G}/\bar{N} \approx (G/K)/(N/K)$.

1.3. **Automorphism.**

- If G is abelian and has some element with order larger than 2, then $T : G \to G, x \mapsto x^{-1}$ defines an non-identity automorphism of G.
- $g \in G$, $T_g : G \to G, x \mapsto g^{-1}xg$ defines an automorphism of G. When G is non-abelian, there exists $T_a \neq I$.

  $\mathscr{I}(G) = \{T_g \in \mathscr{A}(G) | g \in G\}$, the group of inner automorphisms of G, is a subgroup of $\mathscr{A}(G)$, where $\mathscr{A}(G)$ is the group of automorphisms of G.

  Consider $\phi : G \to \mathscr{A}(G), g \mapsto T_g$. ϕ is a homomorphism with image $\mathscr{I}(G)$. Kernel $K = Z = \{g \in G | xg = gx, \forall x \in G\}$ is the certer group of G. $\mathscr{I}(G) \approx G/Z$.
- $\forall \phi \in \mathscr{A}(G), a \in G, o(a) > 0$, then $o(\phi(a)) = o(a)$.
- Determine $\mathscr{A}(G)$ for all cyclic groups.
  (1) If $G = (a)$ has finite order r, $S : G \to G, a^i \mapsto a^{si}$ defines an automorphism of G, where $0 < s < r$, s relatively prime to r. Any automorphism of G can be represented in this form. That is, $\mathscr{A}(G) \approx \mathbb{U}_r$.
  (2) If $G = (a)$ has infinite order, then $\mathscr{A}(G) \approx \mathbb{Z}_2$. Either $T = I$ or $T : g \mapsto g^{-1}$.

1.4. **Cayley's Theorem.**

- (Cayley) Every group is isomorphic to a subgroup of $A(S)$ for some S.

Proof. Let H be a subgroup of G, $S = \{Hg | g \in G\}$. (S is a iff H is normal.)

Define $t_g : S \to S, Hx \mapsto Hxg$, the action of g on set S. Then $\theta : G \to A(S), g \mapsto t_g$ defines a homomorphism. Kernel $K = \{b \in G | Hxb = Hx, \forall x \in G\}$ is the largest (by showing $n \in N \trianglelefteq H \Rightarrow n \in K$) normal subgroup of G which is contained in H.

In particular, let S be the set of elements of G. For $g \in G$, define $\tau_g : S \to S, x \mapsto xg$. $\psi : G \to A(S), g \mapsto \tau_g$ defines a homomorphism with trivial kernel. $\square$

- If G is a finite group, and $H \neq G$ is a subgroup of G such that $o(G) \nmid i(H)!$ then H must contain a nontrivial normal subgroup of G. In particular, G cannot be simple.

  Proof. θ is an isomorphism if and only it has trivial kernel, if and only if H has no nontrivial normal subgroup. Then $o(G) = o(\theta(G)) \mid o(A(S)) = o(S)! = i(H)!$. $\square$

- A finite group G can be represented as a subgroup of S_n for some n.

1.5. **Permutation Groups.**

- Let S be a set, $\theta \in A(S)$. Define an equivalence class $a \equiv_\theta b$ if and only if $b = a\theta^i$ for some interger i. For $s \in S$, $[s]_\theta = \{x \in S | x \equiv_\theta s\} = \{s\theta^i, i \in \mathbb{Z}\}$ is the orbit of s under θ.
- Every permutation can be uniquely expressed as a product of disjoint cycles.
- Every permutation is a product of 2-cycles (transpositions).
- Let A_n be the subset of S_n consisting of all even permutaions, then A_n is a subgroup.

  Let W be the group of $1, -1$ under multiplication. $\phi : S_n \to W, s \mapsto \text{parity(s)}$ defines a homomorphism with kernel A_n. Thus $S_n/A_n \approx W$, A_n is a normal subgroup with index 2, $o(A_n) = \frac{o(S_n)}{o(W)} = \frac{1}{2}n!$. A_n is called the alternating group of degree n.

1.6. **Cauchy's Theorem.**

- Conjugacy defined by $a \sim b : \exists c \in G, b = c^{-1}ac$ is an equivalence relation. $C(a) = \{x \in G | a \sim x\} = \{y^{-1}ay | y \in G\}$ is the equivalence class of a.
- $N(a) = \{x \in G | xa = ax\}$ is the normalizer of a in G, which consists of all elements in G that commute with a. $N(a)$ is a subgroup of G.
- $x, y \in G, x^{-1}ax = y^{-1}ay$ if and only if $x \equiv_{N(a)} y$. That is, $o(G) = o(C(a))o(N(a))$.
- When G is finite,
$$c_a = o(C(a)) = i_G(N(a)) = \frac{o(G)}{o(N(a))}, o(G) = \sum c_a = \sum \frac{o(G)}{o(N(a))}$$
- $a \in Z$ if and only if $N(a) = G$. If G is finite, $a \in Z$ if and only if $c_a = 1$ if and only if $o(N(a)) = o(G)$.
- If $o(G) = p^n$ where p is a prime number, then $Z(G) \neq (e)$.

  Proof. $o(N(a)) = p^{n_a}$ for some integer n_a by Lagrange's.
$$p^n = o(Z) + \sum_{n_a < n} \frac{p^n}{p^{n_a}}$$
  Then $p \mid o(Z), e \in Z, o(Z) \geq 1$. $o(Z) \geq p$. $\square$

- If $o(G) = p^2$, p is prime, then G is abelian.

Proof. It suffices to show $o(Z) \neq p$. If not, let $a \in G, a \notin Z$. Then $o(N(a)) < o(G) = p^2$. $a \in N(a), Z \subset N(a)$, then $o(N(a)) > o(Z) = p$. But $N(a) \mid o(G)$, contradiction. □

- (Cauchy) If p is a prime number and $p \mid o(G)$, then G has element of order p.

  Proof. By induction. Assume true for all groups T with $o(T) < o(G)$. Assume no proper subgroup of G is divisible by p.
  $$o(G) = o(Z) + \sum \frac{o(G)}{o(N(a))}$$
  By assumption $p \nmid o(N(a))$, then $p \mid o(Z)$. $o(Z)$ cannot be a proper subgroup, thus $o(Z) = G$, G is abelian. Revoking Cauchy's theorem for finite abelian group completes the proof. □

- Two permutations in S_n are conjugate if and only if they have the same cycle decomposition. It follows that S_n has exactly $p(n)$ conjugate classes, where $p(n)$ is the number of partitions of n.

  Proof. Consider $\sigma, \theta \in S_n$. If $\sigma(i) = j, \theta(i) = s, \theta(j) = t$, then $\theta^{-1}\sigma\theta(s) = t$. It shows that to compute $\theta^{-1}\sigma\theta$, replace every symbol in σ by its image under θ. Thus the number of partition after conjugation is unchanged. □

1.7. **Sylow's Theorem.**

- (Sylow) If p is prime and $p^\alpha \mid o(G)$, then G has a subgroup of order p^α.

  (1) *Proof.* If $n = p^\alpha m$, where $p^r \mid m, p^{r+1} \nmid m$, then
  $$p^r \mid \binom{p^\alpha m}{p^\alpha}, p^{r+1} \nmid \binom{p^\alpha m}{p^\alpha}$$
  Let $\mathscr{M}$ be the collection of subsets (not necessarily groups) of G that have p^α elements, then $o(\mathscr{M}) = \binom{p^\alpha m}{p^\alpha}$. Given $M_1, M_2 \in \mathscr{M}$, define equivalence class $M_1 \sim M_2 : \exists g \in G, M_1 = M_2 g$. By analysis above $\exists M \in \mathscr{M}, p^{r+1} \nmid o([M]), [M] = \{Mx | x \in G\}$. $H(x) := \{g \in G : Mxg = Mx\}, H = H(e)$, then $H(x) = x^{-1}Hx, o(G) = o([M])o(H)$. Then $p^\alpha \mid o(H)$. $M \subset H, o(H) \geq o(M) = p^\alpha$, then $o(H) = p^\alpha$. □

  (2) *Proof.* First show the existence of p-Sylow subgroups of G for every prime p dividing $o(G)$. Induction on $o(G)$, consider the case when no subgroups of G is divisible by p^α. Then by the class equation, $p \mid o(Z)$, and by Cauchy's $\exists b \in Z, o(b) = p$. Let $B = (b) \trianglelefteq G, \bar{G} = G/B$. Apply induction hypothesis, $\exists \bar{P} \subset \bar{G}, o(\bar{P}) = p^{\alpha-1}$. $P := \{x \in G | xB \in \bar{P}\} = \{x \in G | [x] \in \bar{P}\}$. Since $o([x]) = o([B]) = p, o(\bar{P}) = p^{\alpha-1}, o(P) = p^\alpha$.
  Then show that any group of order p^m has subgroups of order $p^\alpha, \forall 0 \leq \alpha \leq m$. □

  (3) *Proof.* (a) Show S_{p^k} has a p-Sylow subgroup by induction.
  $$\{1, 2, \ldots, p^{k-1}\},$$
  $$\{p^{k-1}+1, p^{k-1}+2, \ldots, 2p^{k-1}\},$$
  $$\ldots,$$
  $$\{(p-1)p^{k-1}+1, (p-1)p^{k-1}+2, \ldots, p^k\}$$
  $\sigma := (1, p^{k-1}+1, \ldots, (p-1)p^{k-1}+1) \ldots (p^{k-1}, 2p^{k-1}, \ldots, p^k), A := \{\tau \in S_{p^k} | \tau(i) = i, \forall i > p^{k-1}\} \approx S_{p^{k-1}}$. By induction there is p-Sylow subgroup P_0 of A, $o(P_0) = p^{n(k-1)}$. $P_j := \sigma^{-j} P_0 \sigma^j$, then P_j only permutes elements in $\{jp^{k-1}+1, jp^{k-1}+2, \ldots, (j+1)p^{k-1}\}$.
  $T := P_0 P_1 \ldots P_{p-1}$. Distinct P_i's permute non-overlapping sets of intergers, hence commute. Thus

T is a subgroup of S_{p^k}, $o(T) = o(P_0)^p = p^{p \cdot n(k-1)}$.

$P := \{\sigma^i t | t \in T, 0 \le t \le p-1\}, \sigma^p = e$, then $\sigma^{-1} T \sigma = T$, P is a subgroup of S_{p^k}. $o(P) = p \cdot o(T) = p^{1+p\cdot n(k-1)} = p^{n(k)}$. P is a p-Sylow subgroup of S_{p^k}.

(b) Let G be a finite group, G is a subgroup of the finite group M, and that M has a p-Sylow subgroup Q. Then G has a p-Sylow subgroup P. In fact, $P = G \cap xQx^{-1}$ for some $x \in M$.

Lemma: Let G be a group, A, B subgroups of G. If $x, y \in G$ define $x \sim y$ if $y = axb$ for some $a \in A, b \in B$. It defines a relation in G, $[x] = AxB = \{axb | a \in A, b \in B\}$ is called a double coset of A, B in G.

$$o(AxB) = \frac{o(A)o(B)}{o(A \cap xBx^{-1})}$$

$M = \bigcup GxQ$. Let $o(G \cap xQx^{-1}) = p^{m_x}$, then $o(M) = \sum o(G)p^{m-m_x} = \sum p^{m+n-m_x} t$ where $o(G) = p^n t$, $p \nmid t$. Thus for some x, $m_x = n, G \cap xQx^{-1} = p^n$ is a p-Sylow subgroup of G.

□

- (Second part of Sylow's Theorem) If G is a finite group, then any two p-Sylow subgroups of G are conjugate.

  Proof. $G = \bigcup AxB, o(G) = \sum o(AxB)$. For some $x \in G$, $o(A \cap xBx^{-1}) = o(A)$, then $A = xBx^{-1}$. □

- The number of p-Sylow subgroups in G equals $o(G)/o(N(P))$, where P is any p-Sylow subgroup of G.

  Proof. $N(P) = \{x \in G | xPx^{-1} = P\}$ is the normalizer of P. The number of distinct conjugates of P in G is the index of $N(H)$ in G. □

- (Third part of Sylow's Theorem) The number of p-Sylow subgroups in G, for a given prime, is of the form $1 + kp$.

  Proof. $P = \bigcup PxP, o(P) = \sum o(PxP) = \sum_{x \in N(P)} o(Px) + \sum_{x \notin N(P)} o(PxP) = o(N(P)) + p^{n+1}u$ for some u. $p^{n+1} \nmid o(N(P))$ because $p^{n+1} \nmid o(G)$, then $p \mid p^{n+1}u/o(N(P))$.

  Frome above, the number of p-Sylow groups is $o(P)/o(N(P)) = 1 + kp$. □

- If there is exactly 1 p-Sylow subgroup, then it is normal.

1.8. **Direct Product.**

- Let G be a group and $N_1, N_2, \ldots, N_n$ normal subgroups of G such that
  (1) $G = N_1 N_2 \ldots N_n$.
  (2) Given $g \in G$ then $g = m_1 m_2 \ldots m_n, m_i \in N_i$ in a unique way.

  Then G is the internal direct product of $N_1, N_2, \ldots, N_n$.
- Suppose that G is the internal direct product of $N_1, \ldots, N_n$. Then for $i \ne j, N_i \cap N_j = (e)$. If $a \in N_i, b \in N_j$, then $ab = ba$. The reverse is not always true.
- Let G be a group and G is the internal direct product of $N_1, N_2, \ldots, N_n$. Let $T = N_1 \times N_2 \times \cdots \times N_n$. Then G and T are isomorphic.

1.9. **Finite Abelian Groups.**

- Every finite abelian group is the direct product of cyclic groups.

  Proof. (1) Any finite abelian group G is the direct product of its Sylow subgroups.

(2) Every abelian group of order p^n is the direct product of cyclic groups.

□

2. Ring

2.1. Special classes of Rings.

- If R is a commutative ring, then $a \neq 0 \in R$ is said to be a zero-divisor if there exists a $b \in R, b \neq 0, ab = 0$.
- A commutative ring is an integral domain if it has no zero-divisors.
- A ring is a division ring if its nonzero elements form a group under multiplication. A field is a commutative division ring.
- A finite integral domain is a field.

  Proof. Let $x_1, x_2, \ldots, x_n$ be all elements of D, and suppose that $a \neq 0 \in D$. By pigeonhole principle, $a = x_i a$ for some x_i. Then x_i can be proved to be the identity element. $x_i = x_i' a$, then there exists a multpilicative inverse for any a. □
- An integral domain D is of characteristic 0 if the relation $ma = 0$, where $a \neq 0$ is in D and m is an integer, holds only if $m = 0$.

  An integral domain D is said to be of finite characteristic if there exists a (smallest) positive integer m such that $ma = 0, \forall a \in D$.

  If D has finite characteristic p, then p is prime.
- Every integral domain can be imbedded in a field. In particular, it can be embedded into the field of quotients.
- Any finite field has finite characteristic. The reverse is not necessarily true.

2.2. Homomorphisms.

- Given $\phi : R \to R'$ is a homomorphism, $1 \in R, 1' \in R$. If R' is an integral domain, or if ϕ is onto, then $\phi(1) = 1'$ must be true.

2.3. Ideals and Quotient Rings.

- If U is an ideal of the ring R, then R/U is a ring and is a homomorphic image of R.
- Let R, R' be rings and ϕ a homomorphism of R onto R' with kernel U. $R' \approx R/U$.

  There is a one-to-one correspondence between the set of ideals of R' and the set of ideals of R which contain U: given W' an ideal in R', $W := \{x \in R | \phi(x) \in W'\}$, then $R/W \approx R'/W'$.
- If F is a field, then its only ideals are (0) and F. That is, a field has no homomorphic images other than itself or the trivial image.
- Let R be a commutative ring with unit element whose only ideals are (0) and R itself. Then R is a field.

  Proof. $Ra = \{xa | x \in R\}$ is an ideal of R. $a \neq 0$ forces $Ra = R$, then R must be a field by finding the unit element and multiplicative inverse. □
- Let R be the ring of all the real-valued, continuous functions on the closed unit interval. Then M is a maximal ideal of R if and only if

$$M = M_\gamma = \{f(x) \in R | f(\gamma) = 0\}$$

for some $\gamma \in [0,1]$.

- If R is a commutative ring with unit element and M is an ideal of R, then M is a maximal ideal of R if and only if R/M is a field. M is prime (that is, $a, b \in M \Rightarrow a \in M$ or $b \in M$) if and only if R/M is an integral domain.

2.4. **Euclidean Rings.**

- An integral domain R is a Euclidean ring if every $a \neq 0, a \in R$ is associated with a nonnegative integer $d(a)$ such that
  (1) $\forall a, b \neq 0, a, b \in R$, $d(a) \leq d(ab)$.
  Indeed, if $b \neq 0$ is not a unit, then $d(a) < d(ab)$. That is, $d(a) = d(ab)$ enforces that b is a unit.
  (2) $\forall a, b \neq 0, a, b \in R, \exists t, r \in R$ such that $a = tb + r$, where $r = 0$ or $d(r) < d(b)$.
- Every Euclidean rings is a principal ideal ring. That is, every ideal A in R is of the form $A = (a) = \{xa | x \in R\}$ for $a \in R$. The reverse is not necessarily true.

Proof. Let a be the element in A such that $d(a)$ is minimal. □

- A Euclidean domain possesses a unit element.
- Let R be a Euclidean ring. $\forall a, b \in R, \exists d = (a, b)$ the greatest common divisor of a, b in R. Moreover $d = \lambda a + \mu b$ for some $\lambda, \mu \in R$.

Proof. $(d) = \min\{ra + sb | r, s \in R\}$. □

- Let R be a communicative ring with unit element. An element $a \in R$ is a unit in R if there exists some $b \in R$ such that $ab = 1$.
  u is a unit if and only if $d(u) = d(1)$.
  Two elements a, b are associates if $b = ua$ for some unit u. It is an equivalence relation.
- Let R be an integral domain. If $a, b \in R, a \mid b, b \mid a$, the a, b are associates.
- In Euclidean ring R a nonunit π is a prime element if $\pi = ab \Rightarrow$ either a or b is a unit.
- Every nonzero element in a Euclidean ring R can be uniquely written (up to associates) as a product of prime elements or is unit in R.
- The ideal $A = (a_0)$ is a maximal ideal of the Euclidean ring R if and only if a_o is a prime element of R.

2.5. **Gaussian Integers.**

- Gausshian Integers $J[i]$ form an integral domain.

2.6. **Polynomial Rings.**

- Let F be a field, then $F[x]$ is an integral domain. It can be extended to the field of rational functions in x over F which merely consists of all quotients of polynomials.
- $F[x]$ is a Euclidean ring. As a result, $F[x]$ is a principle ideal ring. Any polynomial in $F[x]$ can be written uniquely as a product of irreducible polynomials in $F[x]$.
- The ideal $A = (p(x))$ in $F[x]$ is a maximal ideal if and only if $p(x)$ is irreducible over F.

2.7. **Polynomials over Commutative Rings.**

- If R is an integral domain, then so is $R[x]$, and so is $R[x_1, \dots, x_n]$.
- A non-unit element a in R is irreducible (or prime) if $a = bc \Rightarrow b$ or c is a unit.
- Euclidean ring $\Rightarrow$ P.I.D. $\Rightarrow$ U.F.D. The converse is not true, as $F[x_1, x_2]$ is not a principal ideal ring, but a unique factorization domain.
- If R is U.F.D., then so is $R[x]$.
- In an integer domain, prime $\Rightarrow$ irreducible. In P.I.D., irreducible $\Rightarrow$ prime.