Advanced Modern Algebra

Joseph J. Rotman

January 9, 2020

Contents

1 Things Past **2**
1.1 Roots of Unity 2

2 Group I **3**
2.1 Permutations 3
2.2 Groups 5
2.3 Lagrange's theorem 6
2.4 Homomorphisms 9
2.5 Quotient group 11
2.6 Group Actions 16

1 Things Past

1.1 Roots of Unity

Proposition 1.1 (Polar Decomposition). *Every complex number z has a factorization*

$$z = r(\cos\theta + i\sin\theta)$$

where $r = |z| \geq 0$ *and* $0 \leq \theta \leq 2\pi$

Proposition 1.2 (Addition Theorem). *If* $z = \cos\theta + i\sin\theta$ *and* $w = \cos\psi + i\sin\psi$, *then*

$$zw = \cos(\theta + \psi) + i\sin(\theta + \psi)$$

Theorem 1.3 (De Moivre). $\forall x \in \mathbb{R}, n \in \mathbb{N}$

$$\cos(nx) + i\sin(nx) = (\cos x + i\sin x)^n$$

Theorem 1.4 (Euler). $e^{ix} = \cos x + i\sin x$

Definition 1.5. If $n \in \mathbb{N} \geq 1$, an **nth root of unity** is a complex number ξ with $\xi^n = 1$

Corollary 1.6. *Every nth root of unity is equal to*

$$e^{2\pi ik/n} = \cos(\frac{2\pi k}{n}) + i\sin(\frac{2\pi k}{n})$$

for $k = 0, 1, \ldots, n-1$

$$x^n - 1 = \prod_{\xi^n = 1}(x - \xi)$$

If ξ is an nth root of unity and if n is the smallest, then ξ is a **primitive** n**th root of unity**

Definition 1.7. If $d \in \mathbb{N}^+$, then the dth **cyclotomic polynomial** is

$$\Phi_d(x) = \prod(x - \xi)$$

where ξ ranges over all the *primitive dth* roots of unity

Proposition 1.8. *For every integer* $n \geq 1$

$$x^n - 1 = \prod_{d|n}\Phi_d(x)$$

Definition 1.9. Define **Euler} ϕ{-function** as the degree of the nth cyclotomic polynomial

$$\phi(n) = \deg(\Phi_n(x))$$

Proposition 1.10. *If $n \geq 1$ is an integer, then $\phi(n)$ is the number of integers k with $1 \leq k \leq n$ and $(k, n) = 1$*

Proof. Suffice to prove $e^{2\pi i k/n}$ is a primitive nth root of unity if and only if k and n are relatively prime □

Corollary 1.11. *For every integer $n \geq 1$, we have*

$$n = \sum_{d|n} \phi(d)$$

2 Group I

2.1 Permutations

Definition 2.1. A **permutation** of a set X is a bijection from X to itself.

Definition 2.2. The family of all the permutations of a set X, denoted by S_X is called the **symmetric group** on X. When $X = \{1, 2, \ldots, n\}$, S_X is usually denoted by X_n and is called the **symmetric group on n letters**

Definition 2.3. Let $i_1, i_2, \ldots, i_r$ be distinct integers in $\{1, 2, \ldots, n\}$. If $\alpha \in S_n$ fixes the other integers and if

$$\alpha(i_1) = i_2, \alpha(i_2) = i_3, \ldots, \alpha(i_{r-1}) = i_r, \alpha(i_r) = i_1$$

then α is called an textbf{r-cycle}. α is a cycle of **length** r and denoted by

$$\alpha = (i_1 \ i_2 \ \ldots \ i_r)$$

2-cycles are also called the **transpositions**.

Definition 2.4. Two permutations $\alpha, \beta \in S_n$ are **disjoint** if every i moved by one is fixed by the other.

Lemma 2.5. *Disjoint permutations $\alpha, \beta \in S_n$ commute*

Proposition 2.6. *Every permutation $\alpha \in S_n$ is either a cycle or a product of disjoint cycles.*

Proof. Induction on the number k of points moved by α □

Definition 2.7. A **complete factorization** of a permutation α is a factorization of α into disjoint cycles that contains exactly one 1-cycle (i) for every i fixed by α

Theorem 2.8. *Let $\alpha \in S_n$ and let $\alpha = \beta_1 \dots \beta_t$ be a complete factorization into disjoint cycles. This factorization is unique except for the order in which the cycles occur*

Proof. for all i, if $\beta_t(i) \neq i$, then $\beta_t^k(i) \neq \beta_t^{k-1}(i)$ for any $k \geq 1$ $\square$

Lemma 2.9. *If $\gamma, \alpha \in S_n$, then $\alpha\gamma\alpha^{-1}$ has the same cycle structure as γ. In more detail, if the complete factorization of γ is*

$$\gamma = \beta_1\beta_2 \dots (i_1 \ i_2 \ \dots) \dots \beta_t$$

then $\alpha\gamma\alpha^{-1}$ is permutation that is obtained from γ by applying α to the symbols in the cycles of γ

Example. Suppose

$$\beta = (1\ 2\ 3)(4)(5)$$
$$\gamma = (5\ 2\ 4)(1)(3)$$

then we can easily find the α

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 4 & 1 & 3 \end{pmatrix}$$

Theorem 2.10. *Permutations γ and σ in S_n has the same cycle structure if and only if there exists $\alpha \in S_n$ with $\sigma = \alpha\gamma\alpha^{-1}$*

Proposition 2.11. *If $n \geq 2$ then every $\alpha \in S_n$ is a product of tranpositions*

Proof. $(1\ 2\ \dots\ r) = (1\ r)(1\ r-1)\dots(1\ 2)$ $\square$

Definition 2.12. A permutation $\alpha \in S_n$ is **even** if it can be factored into a product of an even number of transpositions. Otherwise **odd**

Definition 2.13. If $\alpha \in S_n$ and $\alpha = \beta_1 \dots \beta_t$ is a complete factorization, then **signum** α is defined by

$$\operatorname{sgn}(\alpha) = (-1)^{n-t}$$

Theorem 2.14. *For all $\alpha, \beta \in S_n$*

$$\operatorname{sgn}(\alpha\beta) = \operatorname{sgn}(\alpha)\operatorname{sgn}(\beta)$$

Theorem 2.15. *1. Let $\alpha \in S_n$; if $\operatorname{sgn}(\alpha) = 1$ then α is even. otherwise odd*

2. A permutation α is odd if and only if it's a product of an odd number of transpositions

Corollary 2.16. *Let $\alpha, \beta \in S_n$. If α and β have the same parity, then $\alpha\beta$ is even while if α and β have distinct parity, $\alpha\beta$ is odd*

2.2 Groups

Definition 2.17. A **binary operation** on a set G is a function

$$* : G \times G \to G$$

Definition 2.18. A **group** is a set G equipped with a binary operation * s.t.

1. the **associative law** holds
2. **identity**
3. every $x \in G$ has an **inverse**, there is a $x' \in G$ with $x * x' = e = x' * x$

Definition 2.19. A group G is called **abelian** if it satisfies the **commutative law**

Lemma 2.20. *Let G be a group*

1. *The **cancellation laws** holds: if either $x * a = x * b$ or $a * x = b * x$, then $a = b$*
2. *e is unique*
3. *Each $x \in G$ has a unique inverse*
4. *$(x^{-1})^{-1} = x$*

Definition 2.21. An expression $a_1 a_2 \ldots a_n$ **needs no parentheses** if all the ultimate products it yields are equal

Theorem 2.22 (Generalized Associativity)**.** *If G is a group and $a_1, a_2, \ldots, a_n \in G$ then the expression $a_1 a_2 \ldots a_n$ needs no parentheses*

Definition 2.23. Let G be a group and let $a \in G$. If $a^k = 1$ for some $k > 1$ then the smallest such exponent $k \geq 1$ is called the **order** or a; if no such power exists, then one says that a has **infinite order**

Proposition 2.24. *If G is a finite group, then every $x \in G$ has finite order*

Definition 2.25. A **motion** is a distance preserving bijection $\varphi : \mathbb{R}^2 \to \mathbb{R}^2$. If π is a polygon in the plane, then its **symmetry group** $\Sigma(\pi)$ consists of all the motions φ for which $\varphi(\pi) = \pi$. The elements of $\Sigma(\pi)$ are called the **symmetries** of π

Let π_4 be a square. Then the group $\Sigma(\pi_4)$ is called the **dihedral group** with 8 elements, denoted by D_8

Definition 2.26. If π_n is a regular polygon with n vertices $v_1, \dots, v_n$ and center O, then the symmetry group $\Sigma(\pi_n)$ is called the {dihedral group} with $2n$ elements, and it's denoted by D_{2n}

2.3 Lagrange's theorem

Definition 2.27. A subset H of a group G is a **subgroup** if

1. $1 \in H$
2. if $x, y \in H$, then $xy \in H$
3. if $x \in H$, then $x^{-1} \in H$

If H is a subgroup of G, we write $H \leq G$. If H is a proper subgroup, then we write $H < G$

The four permutations

$$\boldsymbol{V} = \{(1), (12)(34), (13)(24), (14)(23)\}$$

form a group because $\boldsymbol{V} \leq S_4$

Proposition 2.28. *A subset H of a group G is a subgroup if and only if H is nonempty and whenever $x, y \in H$, $xy^{-1} \in H$*

Proposition 2.29. *A nonempty subset H of a finite group G is a subgroup if and only if H is closed; that is, if $a, b \in H$, then $ab \in H$*

Definition 2.30. If G is a group and $a \in G$

$$\langle a \rangle = \{a^n : n \in \mathbb{Z}\} = \{\text{all powers of } a\}$$

$\langle a \rangle$ is called the **cyclic subgroup** of G **generated** by a. A group G is called **cyclic** if there exists $a \in G$ s.t. $G = \langle a \rangle$, in which case a is called the **generator**

Definition 2.31. The **integers mod** m, denoted by $\mathbb{I}_m$ is the family of all congruence classes mod m

Proposition 2.32. *Let $m \geq 2$ be a fixed integer*

1. *If $a \in \mathbb{Z}$, then $[a] = [r]$ for some r with $0 \leq r < m$*
2. *If $0 \leq r' < r < m$, then $[r'] \neq [r]$*
3. *$\mathbb{I}_m$ has exactly m elements*

Theorem 2.33.

1. *If $G = \langle a \rangle$ is a cyclic group of order n, then a^k is a generator of G if and only if $(k, n) = 1$*

2. *If G is a cyclic group of order n and $\mathrm{gen}(G) = \{$all generators of $G\}$, then*

$$\big|\mathrm{gen}(G)\big| = \phi(n)$$

where ϕ is the Euler ϕ-function

Proof. 1. there is $t \in \mathbb{N}$ s.t. $a^{kt} = a$ hence $a^{kt-1} = 1$ and $n \mid kt - 1$ □

Proposition 2.34. *Let G be a finite group and let $a \in G$. Then the order of a is $\big|\langle a \rangle\big|$.*

Definition 2.35. If G is a finite group, then the number of elements in G, denoted by $|G|$ is called the **order** of G

Proposition 2.36. *The intersection $\bigcap_{i \in I} H_i$ of any family of subgroups of a group G is again a subgroup of G*

Corollary 2.37. *If X is a subset of a group G, then there is a subgroup $\langle X \rangle$ of G containing X tHhat is **smallest** in the sense that $\langle X \rangle \leq H$ for every subgroup H of G that contains X*

Definition 2.38. If X is a subset of a group G, then $\langle X \rangle$ is called the **subgroup generated by** X

A **word** on X is an element $g \in G$ of the form $g = x_1^{e_1} \dots x_n^{e_n}$ where $x_i \in X$ and $e_i = \pm 1$ for all i

Proposition 2.39. *If X is a nonempty subset of a group G, then $\langle X \rangle$ is the set of all words on X*

Definition 2.40. If $H \leq G$ and $a \in G$, then the **coset** aH is the subset aH of G, where

$$aH = \{ah : h \in H\}$$

aH **left coset**, Ha **right coset**

Lemma 2.41. *$H \leq G, a, b \in G$*

1. *$aH = bH$ if and only if $b^{-1}a \in H$*
2. *if $aH \cap bH \neq \emptyset$, then $aH = bH$*
3. *$|aH| = |H|$ for all $a \in G$*

Proof. define a relation $a \equiv b$ if $b^{-1}a \in H$ □

Theorem 2.42 (Lagrange's Theorem). *If H is a subgroup of a finite group G, then $|H|$ is a divisor of $|G|$*

Proof. Let $\{a_1H, a_2H, \dots, a_tH\}$ be the family of all the distinct cosets of H in G. Then

$$G = a_1H \cup a_2H \cup \cdots \cup a_tH$$

hence

$$|G| = |a_1H| + \cdots + |a_tH|$$

But $|a_iH| = |H|$ for all i. Hence $|G| = t|H|$ □

Definition 2.43. The **index** of a subgroup H in G denoted by $[G : H]$, is the number of left cosets of H in G

Note that $|G| = [G : H]|H|$

Corollary 2.44. *If G is a finite group and $a \in G$, then the order of a is a divisor of $|G|$*

Corollary 2.45. *If G is a finite group, then $a^{|G|} = 1$ for all $a \in G$*

Corollary 2.46. *If p is a prime, then every group G of order p is cyclic*

Proposition 2.47. *The set $U(\mathbb{I}_m)$, defined by*

$$U(\mathbb{I}_m) = \{[r] \in \mathbb{I}_m : (r, m) = 1\}$$

is a multiplicative group of order $\phi(m)$. If p is a prime, then $U(\mathbb{I}_p) = \mathbb{I}_p^\times$, the nonzero elements of $\mathbb{I}_p$.

Proof. $(r, m) = 1 = (r', m)$ implies $(rr', m) = 1$. Hence $U(\mathbb{I}_m)$ is closed under multiplication. If $(x, m) = 1$, then $rs + sm = 1$. There fore $(r, m) = 1$. Each of them have inverse. □

Corollary 2.48 (Fermat)**.** *If p is a prime and $a \in \mathbb{Z}$, then*

$$a^p \equiv a \mod p$$

Proof. suffices to show $[a^p] = [a]$ in $\mathbb{I}_p$. If $[a] = [0]$, then $[a^p] = [a]^p = [0]$. Else, since $\left|\mathbb{I}_p^\times\right| = p - 1$, $[a]^{p-1} = [1]$ □

Theorem 2.49 (Euler)**.** *If $(r, m) = 1$, then*

$$r^{\phi(m)} \equiv 1 \mod m$$

Proof. Since $\left|U(\mathbb{I}_m)\right| = \phi(m)$. Lagrange's theorem gives $[r]^{\phi(m)} = [1]$ for all $[r] \in U(\mathbb{I}_m)$.

In fact we construct a group to prove this. □

Theorem 2.50 (Wilson's Theorem)**.** *An integer p is a prime if and only if*

$$(p-1)! \equiv -1 \mod p$$

Proof. Assume that p is a prime. If $a_1, \ldots, a_n$ is a list of all the elements of finite abelian group, then product $a_1 a_2 \ldots a_n$ is the same as the product of all elements a with $a^2 = 1$. Since p is prime, $\mathbb{I}_p^\times$ has only one element of order 2, namely $[-1]$. It follows that the product of all the elements in $\mathbb{I}_p^\times$ namely $[(p-1)!]$ is equal to $[-1]$.

Conversly assume that m is composite: there are integers a and b with $m = ab$ and $1 < a \leq b < m$. If $a < b$ then $m = ab$ is a divisor of $(m-1)!$. If $a = b$, then $m = a^2$. if $a = 2$, then $(a^2 - 1)! \equiv 2 \mod 4$. If $2 < a$, then $2a < a^2$ and so a and $2a$ are factors of $(a^2 - 1)!$ □

2.4 Homomorphisms

Definition 2.51. If $(G, *)$ and $(H, \circ)$ are groups, then a function $f : G \to H$ is a **homomorphism** if

$$f(x * y) = f(x) \circ f(y)$$

for all $x, y \in G$. If f is also a bijection, then f is called an **isomorphism**. G and H are called **isomorphic**, denoted by $G \cong H$

Lemma 2.52. *Let $f : G \to H$ be a homomorphism*

1. $f(1) = 1$
2. $f(x^{-1}) = f(x)^{-1}$
3. $f(x^n) = f(x)^n$ *for all* $n \in \mathbb{Z}$

Definition 2.53. If $f : G \to H$ is a homomorphism, define

$$\ker f = \{x \in G : f(x) = 1$$

and

$$\operatorname{im} f = \{h \in H : h = f(x) \text{ for some } x \in G$$

Proposition 2.54. *Let $f : G \to H$ be a homomorphism*

1. $\ker f$ *is a subgroup of* G *and* $\operatorname{im} f$ *is a subgroup of* H
2. *if* $x \in \ker f$ *and if* $a \in G$*, then* $axa^{-1} \in \ker f$
3. f *is an injection if and only if* $\ker f = \{1\}$

Proof. 3. $f(a) = f(b) \Leftrightarrow f(ab^{-1}) = 1$

□

Definition 2.55. A subgroup K of a group G is called a **normal subgroup** if $k \in K$ and $g \in G$ imply $gkg^{-1} \in K$, denoted by $K \lhd G$

Definition 2.56. If G is a group and $a \in G$, then a **conjugate** of a is any element in G of the form

$$gag^{-1}$$

where $g \in G$

Definition 2.57. If G is a group and $g \in G$, define **conjugation** $\gamma_g : G \to G$ by

$$\gamma_g(a) = gag^{-1}$$

for all $a \in G$

Proposition 2.58.

1. *If G is a group and $g \in G$, then conjugation $\gamma_g : G \to G$ is an isomorphism*
2. *Conjugate elements have the same order*

Proof. 1. bijection: $\gamma_g \circ \gamma_{g^{-1}} = 1 = \gamma_{g^{-1}} \circ \gamma_g$.

$\square$

Example 2.1. Define the **center** of a group G, denoted by $Z(G)$, to be

$$Z(G) = \{z \in G : zg = gz \text{ for all } g \in G\}$$

Example 2.2. If G is a group, then an **automorphism** of G is an isomorphism $f : G \to G$. For example, every conjugation γ_g is an automorphism of G (it is called an **inner automorphism**), for its inverse is conjugation by g^{-1}. The set $\mathrm{Aut}(G)$ of all the automorphism of G is itself a group.

$$\mathrm{Inn}(G) = \{\gamma_g : g \in G\}$$

is a subgroup of $\mathrm{Aut}(G)$

Proposition 2.59.

1. *If H is a subgroup of index 2 in a group G, then $g^2 \in H$ for every $g \in G$*
2. *If H is a subgroup of index 2 in a group G, then H is a normal subgroup of G*

Definition 2.60. The group of **quaternions** is the group $\boldsymbol{Q}$ of order 8 consisting of the following matrices in $GL(2, \mathbb{C})$

$$\boldsymbol{Q} = \{I, A, A^2, A^3, B, BA, BA^2, BA^3\}$$

where I is the identity matrix

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \text{ and } B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

Example 2.3. Q is normal. By Lagrange's theorem the only possible orders of subgroups are 1,2,4 or 8. The only subgroup of order 2 is $\langle -I \rangle$ since $-I$ is the only element of order 2

Proposition 2.61. *The alternating group A_4 is a group of order 12 having no subgroup of order 6*

2.5 Quotient group

$\mathcal{S}(G)$ is the set of all nonempty subsets of a group G. If $X, Y \in \mathcal{S}(G)$, define

$$XY = \{xy : x \in X \text{ and } y \in Y\}$$

Lemma 2.62. *$K \leq G$ is normal if and only if*

$$gK = Kg$$

A natural question is that whether HK is a subgroup when H and K are subgroups. The answer is no. Let $G = S_3, H = \langle (1\ 2) \rangle, K = \langle (1\ 3) \rangle$

Proposition 2.63.

1. *If H and K are subgroups of a group G, and if one of them is normal, then $HK \leq G$ and $HK = KH$*
2. *If $H, K \lhd G$, then $HK \lhd G$*

Theorem 2.64. *Let G/K denote the family of all the left cosets of a subgroup K of G. If $K \lhd G$, then*

$$aKbK = abK$$

for all $a, b \in G$ and G/K is a group under this operation

Proof. $aKbK = abKK = abK$ □

G/K is called the **quotient group** G mod K

Corollary 2.65. *Every $K \lhd G$ is the kernel of some homomorphism*

Proof. Define the **natural map** $\pi : G \to G/K$, $a \mapsto aK$ □

Theorem 2.66 (First Isomorphism Theorem)**.** *If $f : G \to H$ is a homomorphism, then*

$$\ker f \lhd G \quad \textit{and} \quad G/\ker f \cong \operatorname{im} f$$

If $\ker f = K$ and $\varphi : G/K \to \operatorname{im} f \leq H, aK \mapsto f(a)$, then φ is an isomorphism

Remark.
$$\begin{tikzcd} G \arrow[rr, "f"] \arrow[dr, "\pi"'] & & H \\ & G/K \arrow[ur, "\varphi"'] & \end{tikzcd}$$

Example 2.4. What's the quotient group $\mathbb{R}/\mathbb{Z}$? Define $f : \mathbb{R} \to S^1$ where S^1 is the circle group by
$$f : x \mapsto e^{2\pi i x}$$
$\mathbb{R}/\mathbb{Z} \cong S^1$

Proposition 2.67 (Product Formula). *If H and K are subgroups of a finite group G, then*
$$|HK||H \cap K| = |H||K|$$

Proof. Define a function $f : H \times K \to HK, (h,k) \mapsto hk$. Show that $\left|f^{-1}(x)\right| = |H \cap K|$.

Claim that if $x = hk$, then
$$f^{-1}(x) = \{(hd, d^{-1}k) : d \in H \cap K\}$$
□

Theorem 2.68 (Second Isomorphism Theorem). *If $H \lhd G, K \leq G$, then $HK \leq G, H \cap K \lhd G$ and*
$$K/(H \cap K) \cong HK/H$$

Proof. $hkH = kk^{-1}hkH = kh'H = kH$ □

Theorem 2.69 (Third Isomorphism Theorem). *If $H, K \lhd G$ with $K \leq H$, then $H/K \lhd G/K$ and*
$$(G/K)/(H/K) \cong G/H$$

Theorem 2.70 (Correspondence Theorem). *If $K \lhd G, \pi : G \to G/K$ is the natural map, then*
$$S \mapsto \pi(S) = S/K$$
is a bijection between $Sub(G;K)$, the family of all those subgroups S of G that contain K, and $Sub(G/K)$, the family of all the subgroups of G/K. If we denote S/K by S^*, then

1. *$T \leq S \leq G$ if and only if $T^* \leq S^*$, in which case $[S:T] = [S^* : T^*]$*
2. *$T \lhd S$ if and only if $T^* \lhd S^*$, in which case $S/T \cong S^*/T^*$*

$$
\begin{tikzcd}
G \arrow[d, dash] \arrow[dr] & \\
S \arrow[d, dash] \arrow[dr] & G/K \arrow[d, dash] \\
T \arrow[d, dash] \arrow[dr] & S/K = S^* \arrow[d, dash] \\
K \arrow[dr] & T/K = T^* \arrow[d, dash] \\
& \{1\}
\end{tikzcd}
$$

Proof. Use $\pi^{-1}\pi = 1$ and $\pi\pi^{-1} = 1$ to prove injectivity and surjectivity respectively.

For $[S : T] = [S^* : T^*]$, show there is a bijection between the family of all cosets of the form sT and the family of all the cosets of the form s^*T^*.

injective:

$$
\begin{aligned}
\pi(m)T^* = \pi(n)T^* &\Leftrightarrow \pi(m)\pi(n)^{-1} \in T^* \\
&\Leftrightarrow mn^{-1}K \in T/K \\
&\Rightarrow mn^{-1}t^{-1} \in K \\
&\Rightarrow mn^{-1} = tk \in T \\
&\Leftrightarrow mT = nT
\end{aligned}
$$

surjective:

If G is finite, then

$$
\begin{aligned}
[S^* : T^*] &= \left|S^*\right| / \left|T^*\right| \\
&= \left|S/K\right| / \left|T/K\right| \\
&= (|S| / |K|)/(|T| / |K|) \\
&= |S| / |T| \\
&= [S : T]
\end{aligned}
$$

If $T \lhd S$, by third isomorphism theorem, $T/S \cong (T/K)/(S/K) = T^*/S^*$

If $T^* \lhd S^*$,

$$\pi(sts^{-1}) \in \pi(s)T^*\pi(s)^{-1} = T^*$$

so that $sts^{-1} \in \pi^{-1}(T^*) = T$ $\square$

Proposition 2.71. *If G is a finite abelian group and d is a divisor of $|G|$, then G contains a subgroup of order d*

Proof. Abelian group's subgroup is normal and hence we can build quotient groups. p90 for proof. Use the correspondence theorem □

Definition 2.72. If H and K are grops, then their **direct product**, denoted by $H \times K$, is the set of all ordered pairs (h, k) with the operation

$$(h, k)(h', k') = (hh', kk')$$

Proposition 2.73. *Let G and G' be groups and $K \triangleleft G$, $K' \triangleleft G'$. Then $K \times K' \triangleleft G \times G'$ and*

$$(G \times G')/(K \times K') \cong (G/K) \times (G'/K')$$

Proof. □

Proposition 2.74. *If G is a group containing normal subgroups H and K and $H \cap K = \{1\}$ and $HK = G$, then $G \cong H \times K$*

Proof. Note $|HK||H \cap K| = |H||K|$. Consider $\varphi : G \to H \times K$. Show it's homo and bijective. □

Theorem 2.75. *If m, n are relatively prime, then*

$$\mathbb{I}_{mn} \cong \mathbb{I}_m \times \mathbb{I}_n$$

Proof.

$$\begin{aligned} f :& \mathbb{Z} \to \mathbb{I}_m \times \mathbb{I}_n \\ & a \mapsto ([a]_m, [a]_n) \end{aligned}$$

is a homo. $\mathbb{Z}/\langle mn \rangle \cong \mathbb{I}_m \times \mathbb{I}_n$ □

Proposition 2.76. *Let G be a group, and $a, b \in G$ be commuting elements of orders m, n. If $(m, n) = 1$, then ab has order mn*

Corollary 2.77. *If $(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$*

Proof. Theorem 2.75 shows that $f : \mathbb{I}_{mn} \cong \mathbb{I}_m \times \mathbb{I}_n$. The result will follow if we prove that $f(U(\mathbb{I}_{mn})) = U(\mathbb{I}_m) \times U(\mathbb{I}_n)$, for then

$$\begin{aligned} \phi(mn) &= \left|U(\mathbb{I}_{mn})\right| = \left|f(U(\mathbb{I}_{mn}))\right| \\ &= \left|U(\mathbb{I}_m) \times U(\mathbb{I}_n)\right| = \left|U(\mathbb{I}_m)\right| \cdot \left|U(\mathbb{I}_n)\right| \end{aligned}$$

If $[a] \in U(\mathbb{I}_{mn})$, then $[a][b] = [1]$ for some $[b] \in \mathbb{I}_{mn}$ and

$$f([ab]) = ([ab]_m, [ab]_n) = ([a]_m[b]_m, [a]_n[b]_n) = ([a]_m, [a]_n)([b]_m, [b]_n) = ([1]_m, [1]_n)$$

Hence $f([a]) = ([a]_m, [a]_n) \in U(\mathbb{I}_m) \times U(\mathbb{I}_n)$

For the reverse inclusion, if $f([c]) = ([c]_m, [c]_n) \in U(\mathbb{I}_m) \times U(\mathbb{I}_n)$, then we must show that $[c] \in U(\mathbb{I}_{mn})$. There is $[d]_m \in \mathbb{I}_m$ with $[c]_m[d]_m = [1]_m$, and there is $[e]_n\mathbb{I}_n$ with $[c]_n[e]_n = [1]_n$. Since f is surjective, there is $b \in \mathbb{Z}$ with $([b]_m, [b]_n) = ([d]_m, [e]_n)$, so that

$$f([1]) = ([1]_m, [1]_n) = ([c]_m[b]_m, [c]_n[b]_n) = f([c][b])$$

Since f is an injection, $[1] = [c][b]$ and $[c] \in U(\mathbb{I}_{mn})$ $\square$

Corollary 2.78. *1. If p is a prime, then $\phi(p^e) = p^e - p^{e-1} = p^e(1 - \frac{1}{p})$*

2. If $n = p_1^{e_1} \dots p_t^{e_t}$, then

$$\phi(n) = n(1 - \frac{1}{p_1}) \dots (1 - \frac{1}{p_t})$$

Lemma 2.79. *A cyclic group of order n has a unique subgroup of order d, for each divisor d of n, and this subgroup is cyclic.*

Define an equivalence relation on a group G by $x \equiv y$ if $\langle x\rangle = \langle y\rangle$. Denote the equivalence class containing x by $\mathrm{gen}(C)$, where $C = \langle x\rangle$. Equivalence classes form a partition and we get

$$G = \coprod_C \mathrm{gen}(C)$$

where C ranges over all cyclic subgroups of G. Note $\left|\mathrm{gen}(C)\right| = \phi(n)$

Theorem 2.80. *A group G of order n is cyclic if and only if for each divisor d of n, there is at most one cyclic subgroup of order d*

Theorem 2.81. *If G is an abelian group of order n having at most one cyclic subgroup o f order p for each prime divisor p of n, then G is cyclic*

Exercise:

- 2.71 Suppose $H \leq G$,$|H| = |K|$. Since $|H| = [H : K]|K|$, $[H : K] = 1$. Hence $H = K$
- 2.67 1. $\mathrm{Inn}(S_3) \cong S_3/Z(S_3) \cong S_3$ and $\left|\mathrm{Aut}(S_3)\right| \leq 6$. Hence $\mathrm{Aut}(S_3) = \mathrm{Inn}(S_3)$

2.6 Group Actions

Theorem 2.82 (Cayley). *Every group G is isomorphic to a subgroup of the symmetric group S_G. In particular, if $|G| = n$, then G is isomorphic to a subgroup of S_n*

Proof. For each $a \in G$, define $\tau_a(x) = ax$ for every $x \in G$. τ_a is a bijection for its inverse is $\tau_{a^{-1}}$

$$\tau_a \tau_{a^{-1}} = \tau_1 = \tau_{a^{-1}} \tau_a$$

□

Theorem 2.83 (Representation on Cosets). *Let G be a group and $H \leq G$ having finite index n. Then there exists a homomorphism $\varphi : G \to S_n$ with $\ker \varphi \leq H$*

When $H = \{1\}$, this is the Cayley theorem.

Proposition 2.84. *Every group G of order 4 is isomorphic to either $\mathbb{I}_4$ or the four-group $\boldsymbol{V}$. And $\mathbb{I}_4 \ncong \boldsymbol{V}$*

Proof. By lagrange's theorem, every element in G other than 1 has order 2 or 4. If 4, then G is cyclic.

Suppose $x, y \neq 1$, then $xy \neq x, y$. Hence $G = \{1, x, y, xy\}$. □

Proposition 2.85. *If G is a group of order 6, then G is isomorphic to either $\mathbb{I}_6$ or S_3. Moreover $\mathbb{I}_6 \ncong S_3$*

Proof. If G is not cyclic. Since $|G|$ is even, it has some elements having order 2, say t.

If G is abelian. Suppose it has another different element a with order 2. Then $H = \{1, a, t, at\}$ is a subgroup which contradict. Hence it must contain an element b of order 3. Then bt has order 6 and G is cyclic.

If G is not abelian. If G doesn't have elements of order 3, then it's abelian. Hence G has an element s of order 3.

Now $\left|\langle s \rangle\right| = 3$, so $[G : \langle s \rangle] = |G| / \left|\langle s \rangle\right| = 2$ and $\langle s \rangle$ is normal. Since $t = t^{-1}$, $tst \in \langle s \rangle$. If $tst = s^0 = 1$, $s = 1$. If $tst = s$, $\left|\langle st \rangle\right| = 6$. If $tst = s^2 = s^{-1}$.

Let $H = \langle t \rangle$, $\varphi : G \to S_{G/\langle t \rangle}$ given by

$$\varphi(g) : x\langle t \rangle \to gx\langle t \rangle$$

By representation on cosets, $\ker \varphi \leq \langle t \rangle$. Hence $\ker \varphi = \{1\}$ or $\ker \varphi = \langle t \rangle$. Since

$$\varphi(t) = \begin{pmatrix} \langle t \rangle & s\langle t \rangle & s^2\langle t \rangle \\ t\langle t \rangle & ts\langle t \rangle & ts^2\langle t \rangle \end{pmatrix}$$

If $\varphi(t)$ is the identity permutation, then $ts\langle t\rangle = s\langle t\rangle$, so that $s^{-1}ts \in \langle t\rangle = \{1, t\}$. But now $s^{-1}ts = t$. Therefore $t \notin \ker\varphi$ and $\ker\varphi = \{1\}$. Therefore φ is injective. Because $|G| = |S_3|$, $G \cong S_3$ $\square$

Definition 2.86. If X is a set and G is a group, then G **acts** on X if there is a function $G \times X \to X$, denoted by $(g, x) \to gx$ s.t.

1. (gh)x=g(hx) for all $g, h \in G$ and $x \in X$
2. $1x = x$ for all $x \in X$

X is a G-set if G acts on X

Definition 2.87. If G acts on X and $x \in X$, then the **orbit** of x, denoted by $\mathcal{O}(x)$, is the subset of X

$$\mathcal{O}(x) = \{gx : g \in G\} \subseteq X$$

the **stabilizer** of x, denoted by G_x, is the subgroup

$$G_x = \{g \in G : gx = x\} \leq G$$

G acts **transitively** on X if there is only one orbit. *centralizer} $C_G(x) = \{g \in G : gxg^{-1} = x$

Normalizer

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

When a group G acts on itself by conjugation, then

$$\mathcal{O}(x) = \{y \in G : y = axa^{-1} \text{ for some } a \in G\}$$

In this case, $\mathcal{O}(x)$ is called the **conjugacy class** of x, denoted by x^G

Proposition 2.88. *If G acts on a set X, then X is the disjoint union of the orbits. If X is finite, then*

$$|X| = \sum_i \left|\mathcal{O}(x_i)\right|$$

where x_i is chosen from each orbit

Proof. $x \equiv y \Leftrightarrow$ there exists $g \in G$ with $y = gx$ is an equivalence relation $\square$

Theorem 2.89. *If G acts on a set X and $x \in X$ then*

$$\left|\mathcal{O}(x)\right| = [G : G_x]$$

Proof. Let G/G_x denote the family of cosets. Construct a bijection $\varphi : G/G_x \to \mathcal{O}(x)$ $\square$

Corollary 2.90. *If a finite group G acts on a set X, then the number of elements in any orbit is a divisor of* $|G|$

Corollary 2.91. *If x lies in a finite group G, then the number of conjugates of x is the index of its centralizer*

$$\left|x^G\right| = [G : C_G(x)]$$

and hence it's a divisor of G

Proposition 2.92. *If H is a subgroup of a finite group G, then the number of conjugates of H in G is $[G : N_G(H)]$*

Proof. Similar to theorem 2.89 □

Theorem 2.93 (Cauchy). *If G is a finite group whose order is divisible by a prime p, then G contains an element of order p*

Proof. Prove by induction on $m \geq 1$, where $|G| = mp$. If $m = 1$, it's obvious.

If $x \in HG$, then $\left|x^G\right| = [G : C_G(x)]$. If $x \notin Z(G)$, then x^G has more than one element, so $absC_G(x) < |G|$. If $p \mid \left|C_G(x)\right|$, by inductive hypothesis, we are done. Else if $p \nmid \left|C_G(x)\right|$ for all noncentral x and $|G| = [G : C_G(x)]\left|C_G(x)\right|$, we have

$$p \mid [G : C_G(x)]$$

$Z(G)$ consists of all those elements with $\left|X^G\right| = 1$, we have

$$|G| = \left|Z(G)\right| + \sum_i [G : C_G(x_i)]$$

Hence $p \mid \left|Z(G)\right|$ and by proposition 2.71 □

Definition 2.94. The **class equation** of a finite group G is

$$|G| = \left|Z(G)\right| + \sum_i [G : C_G(x_i)]$$

where each x_i is selected from each conjugacy class having more than one element

Definition 2.95. If p is a prime, then a finite group G is called a **p-group** if $|G| = p^n$ for some $n \geq 0$

Theorem 2.96. *If p is a prime and G is a p-group, then $Z(G) \neq \{1\}$*

Proof. Consider

$$|G| = \left|Z(G)\right| + \sum_i [G : C_G(x_i)]$$

□