Basic Algebra (Solutions)

by Huah Chu

Exercises (§1.12, pp.76–78)

1. Let $\gamma = (12\cdots n)$ in S_n. Show that the conjugacy class of γ in S_n has cardinality $(n-1)!$. Show that the centralizer $C(\gamma) = \langle\gamma\rangle$.

Proof. (1) Let $\gamma = (12\cdots n)$. A permutation is conjugate to γ if and only if it has the form $(i_1 i_2 \cdots i_n)$. Then n permutations $(i_1 i_2 \cdots i_n)$, $(i_2 i_3 \cdots i_n i_1)$, $(i_3 \cdots i_n i_1 i_2)$, …, $(i_n i_1 \cdots i_{n-1})$ are equal. Hence all such permutations has cardinality $n!/n = (n-1)!$

(2) Since the conjugacy class of γ has cardinality $[G : C(\gamma)]$, hence $|C(\gamma)| = n$, $\langle\gamma\rangle \subseteq C(\gamma)$ is obvious. Moreover, $|\langle\gamma\rangle| = n$. Then $\langle\gamma\rangle = C(\gamma)$. □

2. Determine representatives of the conjugacy classes in S_5 and the number of elements in each class. Use this information to prove that the only normal subgroups of S_5 are 1, A_5, S_5.

Sol.

representative	cardinality	parity
1	1	even
(12)	10	odd
(123)	20	even
(12)(34)	15	even
(1234)	30	odd
(12)(345)	20	odd
(12345)	24	even

A normal subgroup H is a union of some conjugacy classes and one of them must be $\{1\}$

Case 1. $H \subset A_5$. Then $|H|||A_5| = 60$.

Hence the possible order of H is $1, 1+20+15+24$. Thus $H = \{1\}$ or A_5.

Case 2. $H \not\subset A_5$. Then $H \cap A_5 \lhd S_5$ and $H/H \cap A_5 \simeq H \cdot A_5/A_5 \simeq S_5/A_5$. Hence $[H : H \cap A_5] = 2$. By Case 1, $H \cap A_5 = \{1\}$ or A_5. If $H \cap A_5 = A_5$, then $H = S_5$. If $H \cap A_5 = \{1\}$, then $|H| = 2$. But a subgroup of order 2 in S_5 cannot be normal by inspecting the table of conjugacy classes constructed above.

3. Let the partition associated with a conjugacy class be $(n_1, n_2, \ldots, n_q)$ where $n_1 = \cdots = n_{q_1} > n_{q_1+1} = \cdots = n_{q_1+q_2} > n_{q_1+q_2+1} = \cdots$. Show that the number of elements in this conjugacy class is $n!/\prod q_i! \prod n_j$.

Proof. Let $S = \{(i_1^1 \cdots i_{n_1}^1)(i_1^2 \cdots i_{n_2}^2) \cdots (i_1^{q_1} \cdots i_{n_{q_1}}^{q_1})(i_1^{q_1+1} \cdots i_{n_{q_1+1}}^{q_1+1}) \cdots (i_1^{n_q} \cdots i_{n_q}^{n_q}) | 1 \leq i_k^j \leq n$ and all i_k^j are distinct$\}$. Then $|S| = n!$.

In S, we define an equivalence relation:

(1) For any cyclic $(i_1^j \cdots i_{n_j}^j), \cdots (i_1^j \cdots i_{n_j}^j) \cdots \sim \cdots (i_2^j \cdots i_{n_j}^j i{-}1^j) \cdots \sim \cdots (i_3^j \cdots i_{n_j}^j i_1^j i_2^j) \cdots \sim \cdots$ and so on. For any element α in S, α is equivalent to $\prod_{j=1}^{q} n_j$ elements under this relation.

(2) For the first q_1 cycles $(i_1^1 \cdots i_{n_1}^1), \ldots, (i_1^{q_1} \cdots i_{n_{q_1}}^{q_1})$, any permutation of these cycles are equivalent: $(i_1^1 \cdots i_{n_1}^1)(i_2^1 \cdots i_{n_2}^1) \cdots \sim (i_2^1 \cdots i_{n_2}^1)(i_1^1 \cdots i_{n_1}^1) \cdots$, and so on. The same equivalence also defined for the second q_2 cycles, ... Hence any element in S is equivalent to $\prod q_i!$ elements.

A equivalence class under this two relations determine a partition in this conjugacy class. Hence the number of partitions is $n!/\prod q_i! \prod n_j$. □

4. Show that if a finite group G has a subgroup H of index n then H contains a normal subgroup of G of index a divisor of $n!$.

Proof. Let H be a subgroup of index n. Consider the action of G on G/H by left translations, $T : G \to \mathrm{Sym}(G/H)$.

The kernel K of this action is a normal subgroup of G contained in H. And $G/K \sim \mathrm{Im}\, T$ is a subgroup of $\mathrm{Sym}(G/H) = S_n$. Hence $|G/K|$ is a divisor of $n!$. □

5. Let p be the smallest prime dividing the order of a finite group. Show that any subgroup H of G of index p is normal.

Proof. Let H be a subgroup of index p. Applying exercise 4, H contains a subgroup K which is normal in K and $[G : K] | p!$. The relation $p = [G : H] | [G : K] | p!$ implies that $[G : K] = p$ since p is the smallest prime dividing $|G|$. Thus $H = K$ and H is normal in G. □

6. Show that every group of order p^2, p a prime, is abelian. Show that up to isomorphism there are only two such groups.

Proof. (1) Let G be a group of order p^2 and $C(G)$ the center of G. Suppose G is not abelian, then $|C(G)| = p$ by Theorem 1.11. Take any $g \in G - C(G)$. Since $[G : C(G)] = p$, g and $C(G)$ generate G. Any element of G can be written in the form $g^i h$ for $h \in C(G)$, $0 \leq i \leq p-1$. Thus for any two elements $g^i h_1, g^i h_g \in G$, $h_1, h_2 \in C(G)$, $(g^i h_1)(g^j h_2) = g^i g^j h_2 h_1 = (g^j h_2)(g^i h_1)$. G is abelian. A contradiction.

(2) Let G be a group of order p^2, then G must be a cyclic group or an elementary abelian group $\langle a, b | a^p = b^p = 1, ab = ba \rangle$:

Case 1. G has an element with order p^2. Then G is cyclic.

Case 2. All non-identity element of G has order p. Take any $1 \neq a \in G$. Then $|\langle a\rangle| = p$. Choose $b \in G - \langle a\rangle$. Then a, b generate a group of order p^2, hence $G = \langle a, b\rangle$. □

Remark. ¿From the Sylow's Theorems (§1.13), a group G with $|G| = p_1^{e_1} \cdots p_n^{e_n}$ contains, for each i, a subgroup of order $p_i^{e_i}$ and all subgroups of this order are isomorphic. Thus the problem of constructing finite groups may be regarded as having two parts: (1) constructing p-groups, and (2) combining p-groups to form a group of order n. Neither of these problems is solved in general.

The known results about first problem are
(1) If $|G| = p$, G is cyclic,
(2) If $|G| = p^2$, G is abelian,
(3) If $|G| = p^3$, there are five such groups up to isomorphism. (See M. Hall: The theory of groups, pp.49–53.)
(4) If $|G| = p^4$, there are 15 groups for $p \geq 3$ and 16 groups for $p = 2$.
(5) There are 51 groups with order 2^5 and 267 groups with order 2^6. (M. Hall and J. K. Senior.)
(6) Rodemich claimed that there are 2356 groups with order 2^7. For more details, we refer to Huppert: Endlich. Gruppen Chap. 3.

7. Let H be a proper subgroup of a finite group G, show that $G \neq \bigcup_{g\in G} gHg^{-1}$.

8. Let G act on S, H act on T, and assume $S \cap T = \emptyset$. Let $U = S \cup T$ and define for $g \in G$, $h \in H$, $s \in S$, $t \in T$, $(g, h)s = gs$, $(g, h)t = ht$. Show that this defines an actio of $G \times H$ on U.

Proof. Omitted. □

9. A group H is said to act on a group K by automorphisms if we have an action of H on K and for every $h \in H$ the map $k \to hk$ of K is an automorphism. Suppose this is the case and let G be the product set $K \times H$. Define a binary composition in $K \times H$ by

$$(k_1, h_1)(k_2, h_2) = ((h_2^{-1}k_1)k_2, h_1h_2)$$

and define $1 = (1, 1)$ — the units of K and H respectively. Verify that this defines a group such that $h \to (1, h)$ is a monomorphism of H into $K \times H$ and $k \to (k, 1)$ is a monomorphism of K into $K \times H$ whose image is a normal subgroup. G is called a semi-direct product of K and H. Note that if H and K are finite then $|K \times H| = |K||H|$.

Proof. (1) The composition $(k_1, h_1)(k_2, h_2) = ((h_2^{-1}k_1)k_2, h_1h_2)$ on $H \times K$ defines a group.

(i) The associativity:

$$\begin{aligned}((k_1,h_1)(k_2,h_2))(k_3,h_3) &= ((h_2^{-1}k_1)k_2, h_1h_2)(k_3,h_3)\\ &= ((h_3^{-1}((h_2^{-1}k_1)k_2)k_3, h_1h_2h_3)\\ (k_1,h_1)((k_2,h_2)(k_3,h_3)) &= (k_1,h_1)((h_3^{-1}k_2)k_3, h_2h_3)\\ &= ((h_2h_3)^{-1}k_1(h_3^{-1}k_2)k_3, h_1h_2h_3).\end{aligned}$$

We have

$$\begin{aligned}&(h_2h_3)^{-1}k_1(h_3^{-1}k_2)k_3\\ =\ &(h_3^{-1}h_2^{-1})k_1(h_3^{-1}k_2)k_3\\ =\ &(h_3^{-1}(h_2^{-1}k_1))(h_3^{-1}k_2)k_3 \quad \text{(By the definition (ii) of actions)}\\ =\ &h_3^{-1}((h_2^{-1}k_1)k_2)k_3 \quad (k \to hk \text{ is an automorphism}).\end{aligned}$$

Hence the associative law holds.

(ii) (1,1) is the unit and $((h_1k_1)^{-1}, h_1^{-1})$ is the inverse of (k_1,h_1). All the verifications are left to the reader.

(2) From $(1,h_1)(1,h_2) = (1,h_1h_2)$ and $(k_1,1)(k_2,1) = (k_1k_2,1)$, we know that $h \to (1,h)$ and $k \to (k,1)$ are monomorphisms.

(3) K is normal subgroup of $K \times H$: Since

$$(k_1,h_1)(k_2,1)((h_1k_1)^{-1}, h_1^{-1}) = ((h_1(k_1k_2))(h_1k_1)^{-1}, 1). \qquad \square$$

Remark. The Jordan-Hölder Theorem claims: for any finite group G admits a composition series

$$G \in G_1 \triangleright G_2 \triangleright \cdots \triangleright G_k = 1,$$

the composition factor $G_i/G_{i+1} = Q_i$ is simple and is uniquely determined by G (§4.6, p.241). The inverse question is: given the factor group Q_i, how can we recapture G? We want to construct G inductively. That is, given Q_i and G_{i+1}, we want to determine G_i such that G_{i+1} is normal in G_i and $G_i/G_{i+1} \simeq Q_i$. This problem is called "The extension problem". Where G_i is called an extension of G_{i+1} by Q_i.

Given K and H, the most simple extension of K by Q is the direct product $G = K \times H$. A natural generalization of it is semidirect product G of K by H: G contains subgroup K and H such that $K \triangleleft G$, $KH = G$ and $K \cap H = 1$. It is not difficult to see that this definition is the same as that given in exercise.

The extension problem was solved by O. Schreier in 1926.

10. Let G be a group, H a transformation group acting on a set S and let G^S denote the set of maps of S into G. Then G^S is a group (the S-direct power of G) if we define $(f_1f_2)(s) = f_1(s)f_2(s)$, $f_i \in G^S$, $s \in S$. If $h \in H$ and $f \in G^S$ define hf by

$(hf)(s) = f(h^{-1}s)$. Verify that this defines an action of H on G^S by automorphisms. The semi-direct product of H and G^S is called the (unrestricted) wreath product $G \wr H$ of G with H.

Proof. If $h \in H$, $f \in G^S$ define hf by $(hf)(s) = f(h^{-1}s)$.

(1) we first check that this is an action:

$$(1f)(s) = f(1^{-1}s) = f(s) \Rightarrow 1f = f.$$

$$\begin{aligned}(h_1h_2, f)(f) &= f((h_1h_2)^{-1}s) = f(h_2^{-1}(h_1^{-1}s)) = (h_2f)(h_1^{-1}s) \\ &= h_1(h_2f)(s) \Rightarrow (h_1h_2)f = h_1(h_2f).\end{aligned}$$

(2) The map $f \to hf$ is an automorphism on G^S:

(i) $(h(f_1f_2))(s) = (f_1f_2)(h^{-1}s) = f_1(h^{-1}s)f_2(h^{-1}s) = hf_1(s) \cdot hf_2(s)$.

Hence $f \to hf$ is a homomorphism.

(ii) Note that the unit in G^S is the map $1 : s \to 1$.

Suppose that $hf = 1$, that is, $hf(s) = f(h^{-1}s) = 1$ for all $s \in S$. Since H is a transformation group acting on S, this implies that $f(t) = 1$ for all $t \in S$. Thus $f = 1$ and $f \to hf$ is injective.

(iii) For any $g \in G^S$, set $f(s) = g(h(s))$. Then $(hf)(s) = f(h^{-1}s) = g(h(h^{-1}s)) = g(s)$. Hence $hf = g$ and $f \to hf$ is surjective. □

11. Let G, H, S be as in exercise 10 and suppose G acts on a set T. Let $(f, h) \in G \wr H$ where f is a map of S into G. If (f_1, h_1), $(f-2, h_2)$ are two such elements, the product in $G \wr H$ is $((h_2^{-1}f_1)f_2, h_1h_2)$. If $(t, s) \in T \times S$ define $(f, h)(t, s) = (f(s)t, hs)$. Verify that this defines an action of $G \wr H$ on $T \times S$. Note that if everything is finite then $|G \wr H| = |G|^{|S|}|H|$ and the degree of the action, defined to be the cardinality of the set on which the action takes place, is the product of the degrees of the actions of H and of G.

Proof. For $(f, h) \in G \wr H$, $(t, s) \in T \times S$, define $(f, h)(t, s) = (f(s)t, hs)$. We verify that this defines an action.

(1) (1,1) is the unit of $G \wr H$ where the first 1 is the unit $1(s) = 1$ in G^S, the second 1 is the unit in H. Then

$$(1, 1)(t, s) = (1(s)t, 1s) = (1t, 1s) = (t, s).$$

(2) $(f_1, h_1)((f_2, h_2)(t, s)) = (f_1, h_1)(f_2(s)t, h_2 s) = (f_1(h_2 s)f_2(s)t, h_1 h_2 s)$
On the other hand

$$\begin{aligned}((f_1, h_1)(f_2, h_2))(t, s) &= ((h_2^{-1} f_1)f_2, h_1 h_2)(t, s) \\ &= (((h_2^{-1} f_1)f_2)(s)t, h_1 h_2 h_3) \\ &= ((h_2^{-1} f_1(s)f_2(s))t, h_1 h_2 s) \quad \text{(by the multiplication in } G^S\text{)} \\ &= (f_1(h_2 s))f_2(s)t, h_1 h_2 s) \\ &= (f_1, h_1)((f_2, h_2)(t, s)).\end{aligned}$$

□

Remark. An example of wreath product is the Sylow p-subgroups of symmetric group S_n (see exercise 16, 17 in §1.13).

12. Let G act on S. Then the action is called k-fold transitive for $k = 1, 2, 3, \ldots$, if given any two elements $(x_1, \ldots, x_k)$, $(y_1, \ldots, y_k)$ in $S^{(k)}$, where the x_i and the y_i are distinct, there exists a $g \in G$ such that $gx_i = y_i$, $1 \leq i \leq k$. Show that if the action of G is doubly transitive then it is primitive.

Proof. Let the action of G on S be doubly transitive and $\pi(S)$ be any nontrivial partition. Hence there is $A \in \pi(S)$ such that $|A| \geq 2$ and $A \neq S$. Choose $x, y \in A$ and $z \in S - A$. By the hypothesis on G, there exists $g \in G$ such that $g(x) = x$ and $g(y) = z$. Thus $\pi(S)$ is not stabilized by G and the action is not primitive. □

13. Show that if the action of G on S is effective and primitive then the induced action on S by any normal subgroup $N \neq 1$ of G is transitive.

Proof. Suppose that N $(\neq 1)$ is not transitive on S. Then the set of orbits of N, $\{Ns\}_{s \in S}$, forms a partition $\pi(S)$ of S with $|\pi(s)| \geq 2$. For all $g \in G$ and $Ns \in \pi(S)$, $gNs = Ngs \in \pi(S)$ since N is normal. Thus $\pi(S)$ is stabilized by G. Since G is not primitive, $\pi(S) = \{\{S\} | s \in S\}$. Hence $hs = s$ for all $h \in N$, $s \in S$. Since the action of G is effective, it follows that $N = \{1\}$. □

Remark. If G is not effective on S, the above exercise is not true. In fact, let G_1 be any primitive action on S, G_2 any group. We define a group action of $G_1 \times G_2$ on S by $(g_1, g_2) \cdot s = g_1 s$. Clearly $\{1\} \times G_2$ is normal in $G_1 \times G_2$. But $\{1\} \times G_2$ is transitive only when $|S| = 1$.