Modern Algebra Self-Study

Evan Kim

November 11, 2020

Contents

1 Groups

1.1 Basic Axioms and Examples

Definition 1.0.1 (binary operation $*$)**.** (1) A *binary operation* $*$ on a set G is a function $*\colon G \times G \to G$.

(2) A binary operation $*$ on a set G is *associative* if for all $a, b, c, \in G$ we have $a * (b * c) = (a * b) * c$.

(3) If $*$ is a binary operation on a set G we say elements a and b of G *commute* if $a * b = b * a$. We say G is *commutative* if for all $a, b, \in G$, $a * b = b * a$.

Definition 1.0.2 (group)**.** A *group* is an ordered pair $(G, *)$ where G is a set and $*$ is a binary operation on G satisfying the following axioms:

(i) For all $a, b, c \in G$, (a*b)*c = a*(b*c) and $*$ is *associative*.

(ii) There exists an element e in G, called an *identity* of G such that for all $a \in G$ we have $A * e = e * a = a$.

(iii) For each $a \in G$ there is an element a^{-1} of G, called an *inverse* of a such that $a * a^{-1} = a^{-1} * a = e$.

The group $(G, *)$ is called *abelian* (or *commutative*) if $a * b = b * a$ for all $a, b \in G$. G is a *finite group* if G is a finite set.

Definition 1.0.3 (order)**.** For a group G and $x \in G$, the *order* of x is the smallest positive integer n such that $x^n = 1$ and is denoted by $|x|$.If no positive power of x is the identity, the order of x is defined to be infinity and x is said to be of infinite order.

1.1.1 Exercises

Exercise 1.1 (§1.1 #9 Dummit, Foote)**.** *Let* $G = \{a + b\sqrt{2} \in \mathbb{R} : a, b, \in \mathbb{Q}\}$.

(a) Prove that G is a group under addition.

(b) Prove that the nonzero elements of G are a group under multiplication. ["Rationalize the denominators" to find multiplicative inverses.]

Proof. First,

(a) (i) associativity holds from the associativity of $\mathbb{R}$.

(ii) $(a + b\sqrt{2}) + 0 = (a + b\sqrt{2})$, 0 is the identity element.

(iii) $((a + b\sqrt{2}) - (a + b\sqrt{2}) = 0$, $-(a + b\sqrt{2})$ is the inverse element.

(b) Note that $a + b\sqrt{2} = a^2 + 2b$.

(i) Associativity holds from the associativity of $\mathbb{R}$.

(ii) $(a^2+2b)(\frac{1}{(a^2+2b)} = 1$

(iii) The inverse of $g = a^2 + 2b$ is $g^{-1} = \frac{1}{a^2+2b}$.

□

Exercise 1.2 (§1.1 #22 Dummit, Foote)**.** *If x and g are elements of the group G, prove that $|x| = |g^{-1}xg|$. Deduce that $|ab| = |ba|$ for all $a, b, \in G$.*

Proof. By definition of order, $x^k = e$. Then

$$(g^{-1}xg)(g^{-1}xg)\dots(g^{-1}xg)$$
$$= g^{-1}xg.$$

□

Exercise 1.3 (§1.1 #33 Dummit, Foote)**.** *Let x be an element of finite order n in G.*

(a) Prove that if n is odd, then $x^j \neq x^{-i}$ for all $i = 1, 2, \dots, n-1$.

(b) Prove that if $n = 2k$ for $1 \leq i < n$ then $x^j = x^{-i}$ if and only if $i = k$.

Proof. First,

(a) Suppose by contradiction that $x^i = x^{-i}$. Then $(x^i)^2 = e$ and the order of x^i is 2. However this contradicts n being odd.

(b) Suppose $|x|$ is even such that $|x|^n = |x|^{2k} = e$. Suppose that $i \neq n$ and by contradiction that $x^i \neq x^{-i}$. Then

$$x^i x^i \neq e$$
$$(x^i)^2 \neq e.$$

Thus $i \neq k$ because otherwise we would have $(x^k)^2 = x^{2k} = e$. However this contradicts the fact that the order of x is even. Thus $x^i = x^{-i}$ when $i = k$.

□

1.2 Dihedral Groups

Definition 1.0.4 (dihedral group)**.** The *dihedral group of order* $2n$ is a set of symmetries of a regular planar n-gon. Each symmetry s is described uniquely by the corresponding *permutation* σ that sends vertex i to vertex j for $i, j \in \{1, 2, 3, \dots, n\}$. Define symmetry composition as st for $s, t \in D_{2n}$.

Definition 1.0.5 (infinite dihedral group)**.** Every dihedral group is generated by a rotation r and a reflection; if the rotation is a rational multiple of a full rotation, then there is some integer n such that r^n is the identity, and we have a finite dihedral group of order $2n$. If the rotation is not a rational multiple of a full rotation, then there is no such n and the resulting group has infinitely elements and is called D_∞. It has presentations

$$\langle r, s : s^2 = 1, srs = r^{-1} \rangle$$
$$\langle x, y : x^2 = y^2 = 1 \rangle.$$

Definition 1.0.6 (generators)**.** A subset S of elements of a group G with the property that every element of G can be written as a finite product of elements of S and their inverses is called a set of *generators* of G and is denoted $G = \langle S \rangle$. Any equations in a general group G that the generators satisfy are called *relations* in G. If some group G is generated by a subset S and there is some collection of relations $R_1, R_2, \ldots, R_m$ such that any relation among the elements of S can be deduced from these, we call this a *presentation* of G and write

$$G = \langle S | R_1, R_2, \ldots, R_m \rangle.$$

The presentation of D_{2n} is

$$D_{2n} = \langle r, s : r^n = s^2 = 1, rs = sr^{-1} \rangle.$$

1.2.1 Exercises

Exercise 1.4 (§1.2 #4 Dummit, Foote)**.** *if $n = 2k$ is even and $n \geq 4$, show that $z = r^k$ is an element of order 2 which commutes with all elements of D_{2n}. Show also that z is the only nonidentity element of D_{2n} which commutes with all elements of D_{2n}. [cf Exercise 33 of §1.1]*

Proof. By §1.1 #33 Dummit, Foote, since $n = 2k$ we have $r^i = r^{-i}$ for $1 \leq i < n$ and $k = i$. Then

$$z = r^i = r^{-i}$$
$$zr^i = (r^i)^2 = e$$
$$r^i r^i = (r^i)^2 = e.$$

Thus $|z| = 2$ since $i = k$. Suppose by contradiction that z does not commute with any r. Then $zr \neq rz$ and $r^k r \neq r r^k$ but this contradicts the associativity law of groups. Suppose by contradiction that z does not commute with any s. Then $zs \neq sz$ and $r^k s \neq s r^k = s r^{-k}$ but this contradicts the relation $rs = sr^{-1}$ of D_{2n}.

Finally to show that z is the only nonidentity element of D_{2n}, recall that D_{2n} is generated by two elements r and s. From the relation $rs = sr^{-1}$, we have the relation $zs = sz^{-1}$ and since z is commutative we have

$$zs = sz^{-1}$$
$$zs = z^{-1}s$$
$$z^k = z^{-k}$$

From the relation $(z^k)^2 = r^n = s^2 = 1$ we can derive a new relation

$$z = r^n z^{-1} = s^2 z^{-1} = z^{-1}.$$

This relation tells us that z is the only non-identity element that commmutes because we can derive all generators of D_{2n} by z. □

Exercise 1.5 (§1.2 #10 Dummit, Foote)**.** *Let G be the group of rigid motions in $\mathbb{R}^3$ of a cube. Show that $|G| = 24$.*

Proof. Observe that a cube has 6 sides and each side can be rotated uniquely 4 times so $6 * 4 = 24$. □

1.3 Symmetric Groups

Definition 1.0.7 (symmetric group)**.** Let Ω be any nonempty set and let S_Ω be the set of all bijections from Ω to itself and assign the group operation function composition as a binary operation to make S_Ω into a group. The order of S_n is $n!$.

Definition 1.0.8 (cycle decomposition)**.** *Cycle decomposition* is an efficient notation for writings elements σ of S_n with cycles. A *cycle* is a string of integers which represents the elements of S_n which cyclically permutes these integers while fixing all other integers. The product of all the cycles is called the *cycle decomposition* of σ.

The cycle decomposition of σ^{-1} is obtained by writing the numbers in each cycle of the cycle decomposition of σ in reverse order. The cycle decomposition of each permutation is also a *unique* way of expressing a permutation as a product of disjoint cycles.

1.3.1 Exercises

Exercise 1.6 (§1.3 #13 Dummit, Foote)**.** *Show that an element has order* 2 *in* S_n *if and only if its cycle decomposition is a product of commuting* 2*-cycles.*

Proof. Suppose an element $a \in S_n$ has order 2 in S_n. Then $a = a^{-1}$ so a is its own inverse and commutes with itself. Thus the corresponding cycle of a is a a commuting 2-cycle.

Going in the other direction, suppose that the cycle decomposition of S_n is a product of commuting 2-cycles such that every non-identity element is in a $2 - cycle$ that commutes. Then we have $\sigma(a) \to \sigma(b)$ and $\sigma(b) \to \sigma(a)$ for any non-identity element $a, b, \in S_n$. This implies that $\sigma(a) \circ \sigma(b) = b$, $ab = e$, and b is the inverse of a. Thus $a, b \in S_n$ have order 2. □

1.4 Matrix Groups

Definition 1.0.9 (field)**.** A *field* is a set F together with two binary operations $+$ and $\cdot$ on F such that $(F, +)$ with identity 0 and $(F - \{0\}, \cdot)$ with identity 1 are abelian groups where the distribution law holds and we have for all $a, b, c, \in F$

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c).$$

Note that for any field F, $F^x = F - \{0\}$. Also note (11.18.20) that we will assume a field is either $\mathbb{Q}, \mathbb{R}, or \mathbb{Z}/p\mathbb{Z}$.

Definition 1.0.10 (matrix groups)**.** The general linear group of degree n is the set of all $n \times n$ matrices whose entries come from F and whose determinant is nonzero

$$GL_n(F) = \{A : A \text{ is an } n \times n \text{ matrix with entries from } F \text{ and } \det(A) \neq 0\}.$$

1.4.1 Exercises

Exercise 1.7 (§1.4 #1 Dummit, Foote)**.** *Prove that* $|GL_2(\mathbb{F}_2)| = 6$.

Proof. Recall that $GL_n(F)$ is the general linear group of degree n and is defined as the set of all $n \times n$ matrices. The order of this group is 6 because there are 6 ways that unit matrices of linearly independent columns can be written including the identity.

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$
$$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

□

Exercise 1.8 (§1.4 #4 Dummit, Foote)**.** *Show that if n is not prime then $\mathbb{Z}/n\mathbb{Z}$ is not a field.*

Proof. Suppose by contradiction that n is not prime and $\mathbb{Z}/n\mathbb{Z}$ is a field. Then nonidentity elements in $\mathbb{Z}/n\mathbb{Z}$ are only prime numbers. Let $a, b, c \in \mathbb{Z}/n\mathbb{Z}$. By the distribution law of fields we have

$$a(b + c) = ab + ac$$

where ab and ac are both prime. However this is a contradiction because ab and ac can be divided by integers besides 1 so they aren't prime. Thus $\mathbb{Z}/n\mathbb{Z}$ is not a field. □

Exercise 1.9 (§1.4 #11 Dummit, Foote)**.** *Let $H(F)$ be the* Heisenberg group *over F be defined as*

$$H(F) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in F \right\}.$$

Let $X, Y \in H(F)$. Then

(a) Compute the matrix product XY and deduce that $H(F)$ is closed under matrix multiplication. Exhibit explicit matrices such that $XY \neq YX$ to show that $H(F)$ is always non-abelian.

(b) Find an explicit formula for the matrix inverse X^{-1} and deduce that $H(F)$ is closed under inverses.

(c) Prove the associative law for $H(F)$ and deduce that $H(F)$ is a group of order $|F|^3$. (Do not assume that matrix multiplication is associative).

(d) Find the order of each element of the finite group $H(\mathbb{Z}/2\mathbb{Z})$.

(e) Prove that every nonidentity element of the group $H(\mathbb{R})$ has infinite order.

Proof. Incomplete proof (see notes)

(a)

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & d + a & e + af + b \\ 0 & 1 & c + c \\ 0 & 0 & 1 \end{pmatrix}.$$

However $H(F)$ is not commutative because

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

and

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

(b) From part a) it suffices to solve the following system of linear equations

$$\begin{aligned} d + a = 0 &\to a = -d \\ f + c = 0 &\to c = -f \\ e + af + b = 0 &\to e = -af - b = ac - b \end{aligned}$$

Then this leads to the inverse matrix

$$\begin{pmatrix} 1 & -a & ac - b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix}$$

(c) The associative law works in each coordinate of the matrix because all entries are real numbers. This implies that matrix multiplication is associative because real numbers are associative with the addition operation. Since each $a, b, c \in F$ is chosen from F, the order of the group is $|F|^3$ (?).

(d) The additive group $\mathbb{Z}/2\mathbb{Z}$ is isomorphic to a finite cyclic group of order $n = 2$. Thus the order of $H(\mathbb{Z}/2\mathbb{Z})$ is

$$|H(\mathbb{Z}/2\mathbb{Z})| = |2|^3 = 8.$$

The order of each matrix depends on the number and placement of the 0's in the upper half of the matrix.

(e) By matrix calculations we have

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}^2 = I$$

and these two matrices have order 4 because

$$\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

(f) Given

$$X = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$$

then we have

$$X^n = \begin{pmatrix} 1 & na & 2nb \\ 0 & 1 & nc \\ 0 & 0 & 1 \end{pmatrix}.$$

Since $\mathbb{R}$ does not have non-identity elements of finite order, then $a = b = c = 0$ which implies that for $X^n = I$, X must be the identity matrix.

□

1.5 Quaternion Groups

Definition 1.0.11 (quaternion)**.** The *quaternion group,* Q_8 is defined by

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

under multiplication. It is given by the group presentation

$$Q_8 = \langle 1, i, j, k : 1^2 = e, i^2 = j^2 = k^2 = ijk = 1 \rangle.$$

1.6 Homomorphisms and Isomorphisms

Definition 1.0.12 (homomorphism)**.** Let $(G, \star)$ and $(H, \diamond)$ be groups. Define a *homomorphism* $\varphi : G \to H$

$$\varphi(x \star y) = \varphi(x) \diamond \varphi(y)$$

for all $x, y \in G$.

Definition 1.0.13 (isomorphism)**.** The map $\varphi : G \to H$ is called an *isomorphism* and G and H are said to be *isomorphic* if φ is both a homomorphism and a bijection. An isomorphism between two groups is written as $G \cong H$.

The homomorphism $\varphi : G \to G'$ is called a *monomorphism* if φ is $1 - 1$. A monomorphism that is onto is called an *isomorphism*. An isomorphism from G to G is called an *automorphism*.

Theorem 1.1 (Cayley's theorem 2.5.1 (Herstein))**.** *Every group G is isomorphic to some subgroup of $A(S)$ for an appropriate S. (pg 69)*

1.6.1 Exercises

Exercise 1.10 (§1.6 #9 Dummit, Foote)**.** *Prove that D_{24} and S_4 are not isomorphic.*

Proof. Let $S = \{r, s\}$ be the set of elements that generate D_{24} and let $\Omega = \{1, 2, 3, 4\}$ be the set of elements in S_4. Define a map $\varphi : S \to \Omega$. If φ was a homomorphism, then we would have

$$\varphi(r^n) = \varphi(r)_1 \dots \varphi(r)_n.$$

However there is no unique cycle decomposition such that $(\varphi(r)_1 \dots \varphi(r)_n)$ because the largest cycle in S_4 is a 4-cycle. Thus φ is not a homomorphism and $D_{24} \ncong S_4$. □

Exercise 1.11 (§1.6 #20 Dummit, Foote)**.** *Leg G be a group and let $Aut(G)$ be the set of all isomorphisms from G onto G. Prove that $Aut(G)$ is a group under function composition (called the* automorphism group *of G and the elements of $Aut(G)$ are called* automorphisms *of G).*

Proof. Let $f, g, h \in Aut(G)$. Then

(a) Associativity -

$$\begin{aligned}(fg)h &= f(gh)\\ fg(h) &= f(g(h))\\ f(g(h)) &= f(g(h))\end{aligned}$$

(b) The identity function is trivially an isomorphism

(c) The inverse exists for every $f \in Aut(G)$ because every isomorphism is bijective by definition.

□

Exercise 1.12 (§1.6 #23 Dummit, Foote)**.** *Let G be a finite group which possesses an automorphism σ (cf. §1.6 #20 Dummit, Foote) such that $\sigma(g) = g$ if and only if $g = 1$. If σ^2 is the identity map from G to G, prove that G is abelian (such an automorphism σ is called* fixed point free *of order 2). [Show that every element of G can be written in the form $x^{-1}\sigma(x)$ and apply σ to such an expression.]*

Proof. Suppose σ^2 is the identity map from G to G. Then for $x, y, \in G$, we have

$$\sigma^2(x) = \sigma(\sigma(x)) = e.$$

Then we can derive the relation

$$\begin{aligned}\sigma(x) &= x\\ x^{-1}\sigma(x) &= e.\end{aligned}$$

Applying σ to the element above gives $\sigma(x^{-1}\sigma(x)) = x^{-1}\sigma(x) = e$. Thus for all $x, y \in G$ we have $x^{-1}\sigma(x)y^{-1}\sigma(y) = e = y^{-1}\sigma(y)x^{-1}\sigma(x)$. Thus G is abelian. □

Exercise 1.13 (§2.5 #2 Herstein)**.** *Recall that $G \simeq G'$ means that G is isomorphic to G'. Prove that for all groups G_1, G_2, G_3:*

(a) $G_1 \simeq G_1$

(b) $G_1 \simeq G_2$ *implies that* $G_2 \simeq G_1$

(c) $G_1 \simeq G_2$, $G_2 \simeq G_3$ *implies that* $G_1 \simeq G_3$.

Proof. Let $\varphi : G_1 \to G_2$ be a map defined by $\varphi(a) = a$.

(a) Then $\varphi(ab) = ab = \varphi(a)\varphi(b)$ and because G is closed under group operations, φ is a homomorphism. φ is a monomorphism because $\varphi(a) = \varphi(b) \implies a = b$. Thus G_1 is isomorphic to itself.

(b) Suppose $G_1 \simeq G_2$. Then $\varphi : G_1 \to G_2$ is bijective. This implies the existence of $\varphi^{-1} : G_2 \to G_1$ which is onto and 1-1. Thus $G_2 \simeq G_1$.

(c) Let $\varphi_1 : G_1 \to G_2$ and $\varphi_2 : G_2 \to G_3$. Then we have for $a \in G_3$ and $\varphi_1(a) \in G_2$

$$\varphi_2(var\phi_1(ab)) = \varphi_2(\varphi_1(a)\varphi_2(b)) = ab = \varphi_2(\varphi_1(a))\varphi_2(\varphi_1(b))$$

so the function composition is a homomorphism. If $a = b$, then $\varphi_2(\varphi_1(a)) = \varphi_2(\varphi_1(b))$ so its a monomorphism. Finally since φ_2 is isomorphic, this implies the function comp is onto so $G_1 \simeq G_3$.

□

Exercise 1.14 (§2.5 #3 Herstein)**.** *Let G be any group and $A(G)$ the set of all $1-1$ mappings of G, as a set, onto itself. Define $L_a : G \to G$ by $L_a(x) = xa^{-1}$. Prove that*

(a) $L_a \in A(G)$.

(b) $L_a L_b = L_{ab}$

(c) The mapping $\psi : Gt\ A(G)$ defined by $\psi(a) = L_a$ is a monomorphism of G into $A(G)$.

Proof. (a) Suppose that $a = b$. Then we have $L_a(x) = xa^{-1} = xb^{-1} = L_b(x)$ so L_a is 1-1.

(b) By function composition, we have

$$L_a L_b = L_a(xb^{-1}) = xb^{-1}a^{-1} = x(ab)^{-1} = L_{ab}.$$

(c) If $a = b$, then

$$\psi(a) = L_a = L_b = \psi(b).$$

□

Exercise 1.15 (§2.5 #6 Herstein)**.** *Prove that if $\varphi : G \to G'$ is a homomorphism, then $\varphi(G)$, the image of G, is a subgroup of G'.*

Proof. Since φ is a homomorphism, the group operations of G are preserved and for any $a, b \in G$ we have $\varphi(ab) = \varphi(a)\varphi(b)$ so φ is closed under the group operation.

From Lemma 2.52 (Herstein), for any $a^{-1} \in G$ we have $\varphi(a^{-1}) = \varphi(a)^{-1}$ which gives us $\varphi(a)^{-1} \in G'$ as desired. □

Exercise 1.16 (§2.5 #7 Herstein)**.** *Show that $\varphi : G \to G'$, where φ is a homomorphism, is a monomorphism if and only if $Ker\varphi) = (e)$.*

Proof. Suppose φ is a monomorphism and by contradiction that $Ker(\varphi) \neq (e)$. Then there exists $\varphi \in Ker(\varphi)$ such that $Ker\varphi = g \neq e$. Then for $g \in G$ we have $(Ker\varphi)g = xg = g$ and $\varphi(g) = eg = g$, which contradicts φ being a monomorphism.

Going in the other direction, suppose $Ker\varphi \neq (e)$ and by contradiction that φ is a monomorphism. Using the same reasoning above, this will contradict that φ is a monomorphism. Thus $Ker\varphi = (e)$. □

Exercise 1.17 (§2.5 #14 Herstein)**.** *If G is abelian and $\varphi : G \to G'$ is a homomorphism of G onto G', prove that G' is abelian.*

Proof. Suppose by contradiction that G is abelian and G' isn't. Then

$$\varphi(ab) = \varphi(a)\varphi(b)$$

and $\varphi(b)\varphi(a) = \varphi(ba)$ so $\varphi(ab) \neq \varphi(ba)$, but this is a contradiction. □

1.7 Group Actions

Definition 1.1.1 (group action)**.** A *group action* of a group G on a set A is a map from $G \times A$ to A (written as $g \cdot a$ for all $g \in G$ and $a \in A$) satisfying the following properties for all $g_1, g_2 \in G$ and $a \in A$:

(1) $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$

(2) $1 \cdot a = a$

Let the group G act on a set A. For each fixed $g \in G$ we get a map σ_g defined by

$$\sigma_g : A \to A$$
$$\sigma_g(a) = g \cdot a$$

There are two important facts associated with this group action:

(1) for each fixed $g \in G$, σ_g is a *permutation* of A and

(2) the map from G to S_A defined by $g \mapsto \sigma_g$ is a homomorphism, which is also called a *permutation representation*.

If G acts on a set B and distinct elements of G induce *distinct* permutations of B, the action is said to be *faithful*. A faithful action is therefore one in which the associated permutation representation is injective. The *kernel* of the action of G on B is defined to be $\{g \in G : gb = b \forall b \in B\}$.

1.7.1 Exercises

Exercise 1.18 (§1.7 #8 Dummit, Foote)**.** *Let A be a nonempty set and let k be a positive integer with $k \leq |A|$. The symmetric group S_A acts on the set B consisting of all subsets of A of cardinality k by $\sigma \cdot \{a_1, \ldots, a_k\} = \{\sigma(a_1), \ldots, \sigma(a_k)\}$.*

(a) Prove that this is a group action.

(b) Describe explicitly how the elements (12) *and* (123) *act on the six 2-element subsets of* $\{1, 2, 3, 4.\}$

Proof. For $\sigma \in G$ and $a_i \in B$, we have $\sigma(\sigma(a_i)) = (\sigma \circ \sigma)a_i$ by function composition and $1 \cdot a_i = a_i$ so σ is a group action on A. □

2 Subgroups

2.1 Definitions and Examples

Lemma 2.0.1 (proposition 1 (subgroup criterion))**.** *A subset H of a group G is a subgroup if and only if*

(1) $H \neq \emptyset$

(2) for all $x, y \in H$, $xy^{-1} \in H$.

Furthermore, if H is finite, then it suffices to check that H is nonempty and closed under multiplication.

Theorem 2.1 (theorem 2.4.1 (Herstein))**.** *If $\approx$ is an equivalence relation on a set S, then $S = \bigcup_{a \in S}[a]$, where this union runs over one element from each class, and where $[a] \neq [b]$ implies $[a] \cap [b] = \emptyset$. That is, $\approx$ partitions S into equivalence classes. (pg 59)*

Lemma 2.1.1 (proposition 1 (subgroup criterion))**.** *A subset H of a group G is a subgroup if and only if*

(1) $H \neq \emptyset$

(2) for all $x, y \in H$, $xy^{-1} \in H$.

Furthermore, if H is finite, then it suffices to check that H is nonempty and closed under multiplication.

2.1.1 Exercises

Exercise 2.1 (§2.1 #6 Dummit, Foote)**.** *Let G be an abelian group. Prove that $\{g \in G : |g| < \infty\}$ is a subgroup of G (called the* torsion subgroup *of G. Give an explicit example where this set is not a subgroup when G is non-abelian.*

Proof. The torsion subset of a non-abelian group, in general, is not a subgroup. For example, the infinite dihedral group which contains infinite elements and is not abelian for $n \geq 3$. The presentation is

$$\langle x, y : x^2 = y^2 = 1 \rangle.$$

The element xy is a product of two torsion elements, but has infinite order. □

Exercise 2.2 (§2.1 #10 Dummit, Foote)**.** *(a) Prove that if H and K are subgroups of G then so is their intersection $H \cap K$.*

(b) Prove that the intersection of an arbitrary nonempty collection of subgroups of G is again a subgroup of G.

Proof. (a) Since H and K are subgroups, $e \in H$ and $e \in K$ so $e \in H \cap K$. Associativity is inherited from G. Finally since H and K are subgroups, they are closed under inverses. By proposition 1 (subgroup criterion), for $x, y, \in H$, $xy^{-1} \in H$ and similarly for K. Let $y = x$. For every $x \in H \cap K$, we have $xy^{-1} \in H \cap K$. Thus $H \cap K$ is closed under inverses and multiplication.

(b) The argument is the same as (a) except we take an arbitrary number of subgroups.

□

Exercise 2.3 (§2.3 #20 Herstein)**.** *Give an example of a group G and two subgroups A, B of G such that AB is not a subgroup of G.*

Proof. Initially created a stackexchange post here and found that I was making some catastrophic elementary mistakes. Answer to the problem was provided in the stackexchange post.

Let $G = D_8$. Let $B = \langle s \rangle$ and $A = \langle rs \rangle$. Then $AB = \{e, s, rs, r\}$ is not a subgroup of D_8. □

Exercise 2.4 (§2.3 #21 Herstein)**.** *If A, B are subgroups of G such that $b^{-1}Ab \subset A$ for all $b \in B$, show that AB is a subgroup of G*

Proof. The first observation is that $A \subset b^{-1}Ab$ for all $b \in B$ from §2.3 #29 Herstein so it suffices to show that $b^{-1}AbB$ is a subgroup. Additionally we have

$$b^{-1}Ab = \{a \in A : b^{-1}ab \; \forall b \in B\}$$
$$B = \{b \in B : b^{-1}Ab \subset A\}.$$

First we see that $b^{-1}AbB$ is closed under multiplication. Take any element $x \in b^{-1}Ab$ and $y \in B$, both of which have the form $x = b^{-1}ab$ and $y = b^{-1}Ab$. Then

$$\begin{aligned} xy &= (b^{-1}ab)(b^{-1}Ab) \\ &= b^{-1}aAb \\ &= b^{-1}Ab. \end{aligned}$$

To check that $b^{-1}AbB$ is closed under inverses, we have

$$\begin{aligned} (xy)^{-1} &= (b^{-1}Abb^{-1}a^{-1}b) \\ &= b^{-1}Aa^{-1}b \\ &= b^{-1}Ab. \end{aligned}$$

Thus AB is a subgroup of G. □

Exercise 2.5 (§2.3 #29 Herstein)**.** *If M is a subgroup of G such that $x^{-1}Mx \subset M$ for all $x \in G$, prove that actually $x^{-1}Mx = M$.*

Proof. We have

$$\begin{aligned} x^{-1}Mx &\subset M \\ x^{-1}M &\subset Mx^{-1} \\ M &\subset xMx^{-1} \subset M \end{aligned}$$

where $xMx^{-1} \subset M$ is true because $x^{-1}Mx$ is a subgroup so is closed under inverses (Example 12 in §2.3 Herstein. □

Exercise 2.6 (§2.4 #5 Herstein)**.** *Let G be a group and H a subgroup of G. Define, for $a, b \in G$, $a \sim b$ if $a^{-1}b \in H$. Prove that this defines an equivalence relation on G, and show that $[a] = aH = \{ah : h \in H\}$. The sets aH are called* left cosets *of H in G.*

Proof. First we verify that $a \sim b$ is an equivalence relation.

i) If $a \sim a$, then $a^{-1}a = e \in H$.

ii) If $a^{-1}b \in H$, then $(a^{-1}b)^{-1} = b^{-1}a \in H$ so $a \sim b$ implies $b \sim a$.

iii) If $a \sim b$ and $b \sim c$, then $a^{-1}b \in H$ and $b^{-1}c \in H$ and $(a^{-1}b)(b^{-1}c) = (a^{-1}c) \in H$.

Since $a \sim b$ is an equivalence relation, then $a \sim b$ if $a^{-1}b \in H$ and $a^{-1}b = h$ for some $h \in H$. Going in the other direction, suppose $a = bk$ for some $k \in H$. Then $b^{-1}a = b^{-1}(bk) = k \in H$. Thus $[a] = aH$. □

Exercise 2.7 (§2.4 #6 Herstein)**.** *If G is S_3 and $H = \{i, f\}$, where $f : S \to S$ is defined by $f(x_1) = x_2, f(x_2) = x_1, f(x_3) = x_3$, list all the right cosets of H in G and list all the left cosets of H in G. Is every right coset of H in G also a left coset of H in G?*

Proof. The elements of S_3 in permutation form are

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}.$$

In cycle form we have

$$S_3 = \{e, (23), (123), (12), (13), (132)\}.$$

The right cosets of H are then

$$\begin{aligned} He &= \{e, (12)\} \\ H(23) &= \{(23), (123)\} \\ H(123) &= \{(123), (23)\} \\ H(12) &= \{(12), e\} \\ H(13) &= \{(13), (132)\} \\ H(132) &= \{(132), (13)\}. \end{aligned}$$

If two cosets are not disjoint, then they are not equivalent by the contrapositive of theorem 2.4.1 (Herstein). Thus there are three cosets

$$\begin{aligned} He = H(12) &= \{e, (12)\} \\ H(23) = H(123) &= \{(23), (123)\} \\ H(13) = H(132) &= \{(13), (132)\}. \end{aligned}$$

The left cosets of H are

$$\begin{aligned} eH &= \{e, (12)\} \\ (23)H &= \{(23), (132)\} \\ (123)H &= \{(123), (13)\} \\ (12)H &= \{(12), e\} \\ (13)H &= \{(13), (123)\} \\ (132)H &= \{(132), (23)\}. \end{aligned}$$

The three disjoint cosets are

$$\begin{aligned} He = H(12) &= \{e, (12)\} \\ H(23) = H(123) &= \{(23), (132)\} \\ H(13) = H(132) &= \{(13), (123)\}. \end{aligned}$$

In general, right cosets do not equal left cosets. Here only $eH = (12)H = He = H(12)$. The elements e and (12) commute with every element in H so they are elements in the normalizer group of H denoted $N_G(H)$. □

Exercise 2.8 (§2.4 #8 Herstein)**.** *If every right coset of H in G is a left coset of H in G, prove that $aHa^{-1} = H$ for all $a \in G$.*

Proof. If every right coset of H is a left coset, then they will be in the same equivalence classes and therefore we have

$$\begin{aligned} aH &= Ha \\ aHa^1 &= H \end{aligned}$$

for all $a \in G$. □

Exercise 2.9 (§2.4 #13 Herstein)**.** *Find the orders of all the elements of U_{18}. Is U_{18} cyclic?*

Proof. $U_{18} = \{[1], [5], [7], [11], [13], [17]\}$. Upon inspection, we have

$$\begin{aligned} 5^1 &= 5 \\ 5^2 &= 25 = 7 \\ 5^3 &= 35 = 17 \\ 5^4 &= 85 = 13 \\ 5^5 &= 65 = 11 \\ 5^6 &= 55 = 1 \end{aligned}$$

This shows that U_{18} is a generated by the cyclic group generated 5 and has order 6. □

Exercise 2.10 (§2.4 #19 Herstein)**.** *Find all the distinct conjugacy classes of* S_3.

Proof. Recall that $S_3 = \{e, (23), (123), (12), (13), (132)\}$. Upon observations of the rotation and reflections of a triangle, the distinct conjugacy classes are

$$\{e\}, \{(23), (12), (13)\}, \{(123)(132)\}$$

□

2.2 Centralizers and Normalizers, Kernels and Normal Subgroups

Definition 2.1.1 (centralizer and normalizer)**.** The *centralizer* of a subset S of a group G is the set of elements of G that commute with each element of S, whereas the *normalizer* of S is the set of elements that satisfy a weaker condition. The *centralizer* of a subset S of a group G is defined as

$$C_G(S) = \{g \in G : gs = sg \forall s \in S\}.$$

The *normalizer* of S in the group G is defined as

$$N_G(S) = \{g \in G : gS = Sg\}.$$

Definition 2.1.2 (kernel)**.** If $\varphi : G \to G'$ is a homomorphism, then the *kernel* of φ, Ker(φ) is defined by

$$Ker(\varphi) = \{a \in G | \varphi(a) = e'\}.$$

Lemma 2.5.4 Herstein states that if $w' \in G'$ is of the form $\varphi(x) = w'$, then

$$(Ker\varphi)x = \{x \in G | \varphi(x) = w'\}.$$

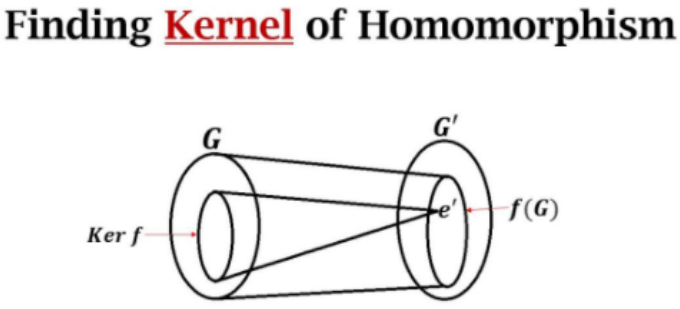


Figure 1: source - mathematical science channel on youtube

Theorem 2.2 (theorem 2.5.5 (Herstein))**.** *Some basic properties of kernels of homomorphism is summed up in this theorem. If* $\varphi : G \to G'$ *is a homomorphism, then*

(a) $Ker(\varphi)$ *is a subgroup of* G.

(b) Given $a \in G$, $a^{-1}(Ker\varphi)a \subset Ker\varphi$.

A corollary to this given $\varphi : G \to G'$, then φ is a monomorphism if and only if $Ker\varphi = (e)$. (pg 71)

Definition 2.2.1 (normal subgroup)**.** The subgroup N of G is said to be a *normal subgroup* of G if $a^{-1}Na \subset NN$ for every $a \in G$ and is denoted as $N \triangleleft G$. Theorem 2.5.6 Herstein says that $N \triangleleft G$ if and only if every left coset of N in G is a right coset of N in G.

2.2.1 Exercises

Exercise 2.11 (§2.2 #4 Dummit, Foote)**.** *For each of S_3, D_8, and Q_8, compute the centralizers of each element and find the center of each group. Does Lagrange's Theorem (Exercise 19 in Section 1.7) simplify your work?*

Proof. For D_8, we have

$$\begin{pmatrix} C_{D_8}(r) = \{1, r, r^2, r^3\}, & Z(r) = \{1, r^2\} \\ C_{D_8}(r) = \{1, r, r^2, r^3\}, & Z(r) = \{1, r^2\} \end{pmatrix}$$

For S_3, which is isomorphic to D_6, we have

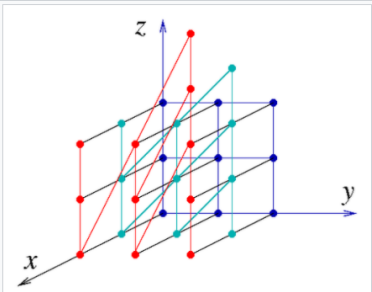
$$\begin{pmatrix} C_{D_6}(r) = \{1, r, r^2\}, & Z(r) = \{1, r^2\} \\ C_{D_6}(r) = \{1, r, r^2\}, & Z(r) = \{1, r^2\} \end{pmatrix}$$

For Q_8 we have:

$$\begin{pmatrix} C_{Q_8}(e) = \{Q_8\} & \\ C_{Q_8(a)} = \{1, a, a^2, a^3\}, & Z(r) = \{1, r^2\} \end{pmatrix}$$

□

Exercise 2.12 (§2.2 #14 Dummit, Foote)**.** *Let $(H(F)$ be the Heisenberg group over the field F(cf Section 1.4 Exercise 11). Determine which matrices lie in the center of $H(F)$ and prove that $Z(H(F))$ is isomorphic to the additive group F.*



A portion of the Cayley graph of the discrete Heisenberg group, with generators x,y,z as in the text. (The coloring is only for visual aid.)

Figure 2: source - wikipedia

Proof. sdf □

Exercise 2.13 (§2.3 #5 Herstein)**.** *If $C(a)$ is the centralizer of a in G (Example 10), prove that $Z(G) = \bigcap_{a\in G} C(a)$.*

Proof. First let's consider a simple case for $a, b \in G$. Then the intersection of $C(a)$ and $C(b)$ is

$$C(a) \cap C(b) = \{g \in G : ag = ga \text{ and } bg = gb\}.$$

Now extending this to a general case, for any $a \in G$, we have

$$\bigcap_{a\in G} C(a) = \{g \in G : ag = ga \forall a \in G\}$$

which is precisely $Z(G)$ by definition. □

Exercise 2.14 (§2.5 #12 Herstein)**.** *Prove that if $Z(G)$ is the center of G, then $Z(G) \triangleleft G$*

Proof. Any element in the center $Z(G)$ commutes with every other element in G. Since each element commutes, each right coset will equal each left coset for every element in G. Thus $Z(G) \triangleleft G$ by definition normal subgroup. □

2.3 Cyclic Groups and Subgroups

Lemma 2.2.1 (proposition 5)**.** *Let G be a group, let $x \in G$ and let $a \in \mathbb{Z}/\{0\}$.*

(1) If $|x| = \infty$, then $|x^a| = \infty$.

(2) If $|x| = n < \infty$, then $|x^a| = \frac{n}{(n,a)}$.

(3) In particular, if $|x| = n < \infty$ and a is a positive integer dividng n, then $|x^a| = \frac{n}{a}$.

2.3.1 Exercises

Exercise 2.15 (§2.3 #21 Dummit, Foote)**.** *Let p be an odd prime and let n be a positive integer. use the Binomial Theorem to show that $(1+p)^{p^{n-1}} \cong 1(\mod p^n)$ but $(1+p)^{p^{n-2}} \ncong 1(\mod p^n)$. Deduce that $(1+p)$ is an element of order p^{n-1} in the multiplicative group $(\mathbb{Z}/p^n\mathbb{Z})^\times$.*

Proof. I spent too much time attempting to solve this question, but it is too difficult for me because I currently don't have any background in number theory (11.29.20). Thus I will leave a couple of stackexchange posts that give good hints to the solution of this problem for future reference.

$$\begin{pmatrix} Post1 & Post2 \end{pmatrix}$$

□

Exercise 2.16 (§2.3 #26 Dummit, Foote)**.** *Let Z_n be a cyclic group of order n and for each integer a let*

$$\sigma_a : Z_n \to Z_n$$

by $\sigma_a(x) = x^a$ for all $x \in Z_n$.

(a) *Prove that σ_a is an automorphism of Z_n if and only if a and n are relatively prime.*

(b) *Prove that $\sigma_a = \sigma_b$ if and only if $a \cong b(\mod n)$.*

(c) *Prove that every automorphism of Z_n is equal to σ_a for some integer a.*

(d) *Prove that $\sigma_a \circ \sigma_b = \sigma_{ab}$. Deduce that the map $\bar{a} \to \sigma_a$ is an isomorphism of $(\mathbb{Z}/p^n\mathbb{Z})^\times$ ont o the automorphism group of Z_n (so Aut(Z_n) is an abelian group of order $\varphi(n)$).*

Proof. (a) Note that $|x| = n$, so we have

$$\sigma_a(x) = (x^n)^a = x^{na}.$$

Developed further we get

$$x^{na} = x^n x^a \implies x^a = x^{-n} = e. \tag{1}$$

Since Z_n is a cyclic group, n is prime. Then (1) implies the gcd is 1 so a and n are relatively prime. If a and n are not relatively prime for any integer a, then σ_a is not injective which contradicts σ_a being an automorphism on Z_n.

(b) If $\sigma_a = \sigma_b$, then $\sigma_a(x) = x^a = x^b = \sigma_b(x)$ for $x^a, x^b \in Z_n$ and $0 \leq a, b < n$. Then by proposition 5, we have $|x^a| = n/a$ and $|x^b| = n/b$ so both a, b divide n and $a \cong b(\mod n)$.

Going in the other direction suppose $a \cong b(\mod n)$. Then $0 \leq a, b < n$ and by the division algorithm we have

$$\begin{aligned} (x^{n-a})(x^a) = e = (x^{n-b})(x^b) \\ (x^{n-b})^{-1}(x^{n-a})(x^a) = x^b \end{aligned} \tag{2}$$

Then by repeated use of the abelian property of Z_n (2) reduces down to $x^b x^a = x^b = x^a$ and this implies $x^b = x^a$. Thus $\sigma_a(x) = \sigma_b(x)$.

(c) Using the results from (a) and (b), every automorphism of Z_n has order α with each α being relatively prime to n by (a). Thus for a fixed integer a, we have $\sigma_a = \sigma_\alpha$ because $a = \alpha(\mod n)$ from (b).

(d) We have

$$\sigma_a \circ \sigma_b = \sigma_a(x^b) = (x^b)^a = x^{ab} = \sigma_{ab}(x).$$

This implies σ is a homomorphism. Then (b) implies that $\bar{a} \to \sigma_a$ is bijective so $\bar{a} \to \sigma_a$ is an isomorphism. Thus $Aut(Z_n)$ is abelian and has order $\varphi(n)$.

□

Theorem 2.3 (group theorem)**.** *Groups are cool if and only if they are groups.*

Proof. We use the group definition to prove something about this theorem. □

Corollary 2.3.1 (group corollary)**.** *A corollary goes here.*

Proof. The corollary is a result of group theorem. □

Lemma 2.3.1 (cool lemma)**.** *Blah blah cool stuff regarding groups.*

Thus we used the group definition to prove the group theorem to get cool results!

3 References

Reference 3.1 (Dummit, Foote)**.** Abstract Algebra, 3rd edition: Dummit, Foote (1991)

Reference 3.2 (Hungerford)**.** Algebra (Graduate Texts in Mathematics) 8th edition by Hungerford (1980)

Reference 3.3 (Herstein)**.** Abstract Algebra, 3rd edition ny Herstein (1999)