Abstract Algebra Supplementary Notes

Spring 2003

David Lyons
Mathematical Sciences
Lebanon Valley College

Abstract Algebra
Supplementary Notes

Spring 2003

David Lyons
Mathematical Sciences
Lebanon Valley College

Contents

1 Further Examples of Groups

1.1 The complex numbers under addition

Let $\mathbf{C}$ denote the complex numbers. The set $\mathbf{C}$, together with the operation of addition, forms an abelian group with identity 0. The inverse of a number z is its negative $-z$.

1.2 The nonzero complex numbers under multiplication

The set $\mathbf{C}^* = \mathbf{C}\backslash\{0\}$ of nonzero complex numbers forms an abelian group under the operation of multiplication. The identity is 1. The inverse of an element z is $1/z$.

1.3 The circle

Let $S^1 = \{z \in \mathbf{C} \mid |z| = 1\}$ be the set of complex numbers of norm 1. The set S^1 is also called the *unit circle* or the *1-dimensional sphere*. The set S^1 forms a group under the operation of complex multiplication.

1.4 The finite quaternion group

Let Q_8 denote the 8 element set $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$. We define a binary operation on Q_8 by the following equations, together with the rule that 1 and -1 are declared to commute with all elements.

$$i^2 = j^2 = k^2 = -1$$

$$ij = k, \qquad jk = i, \qquad ki = j$$

$$ji = -k, \qquad kj = -i, \qquad ik = -j$$

$$1^2 = (-1)^2 = 1$$

1.5 The orthogonal and special orthogonal groups

An *isometry* of n-dimensional euclidean space $\mathbf{R}^n$ is a map $f\colon \mathbf{R}^n \to \mathbf{R}^n$ with the property that $d(f(x), f(y)) = d(x, y)$ where $d(x, y) = |x - y|$ denotes the euclidean distance between points x and y. It can be proved that an isometry f of $\mathbf{R}^n$ which has the additional property that $f(0) = 0$ must be a *linear* map. Let $\mathrm{O}(n)$ denote the set of isometries of $\mathbf{R}^n$ which fix the origin. Let $f \in \mathrm{O}(n)$. It is a fact that the set of column vectors (or row vectors) in the matrix for f form a set of mutually perpendicular vectors of length 1. Such a set of vectors is called an *orthonormal set* of vectors in $\mathbf{R}^n$. For this reason the set $\mathrm{O}(n)$ is called the *orthogonal group*. The group operation on $\mathrm{O}(n)$ is composition.

Another way to describe $\mathrm{O}(n)$ is say it is the set of euclidean symmetries of the $(n-1)$ dimensional sphere S^{n-1} in $\mathbf{R}^n$. (By definition, the sphere S^{n-1} is the set of points 1 unit from the origin in $\mathbf{R}^n$.)

The *special orthogonal group*, denoted $\mathrm{SO}(n)$, is the subgroup of $\mathrm{O}(n)$ of linear maps with determinant 1. In words, the special orthogonal group is the set of orientation preserving isometries of the sphere.

An example of special importance in physics and computer graphics in the set $\mathrm{SO}(3)$, which is the set of rotations of the 3-dimensional space in which we live.

2 Group Actions

2.1 Motivation

Groups are a fundamental algebraic structure which occurs so abundantly and naturally throughout mathematics that the theory of groups constitutes an area of study in its own right. One source of examples is symmetries of geometric figures. In this class, our first examples of groups were the dihedral groups D_3 and D_4, which are the symmetry groups of the equilateral triangle and the square, respectively. We will now use D_4 and the square to introduce the concept of a group action on a set.

Let X be the square in the coordinate plane with vertices $A = (1,1)$, $B = (-1,1)$, $C = (-1,-1)$ and $D = (1,-1)$, together with its interior. In other words, $X = \{(x,y) \mid -1 \leq x \leq 1, -1 \leq y \leq 1\}$. Let us write the elements of D_4 following Gallian's notation.

$$D_4 = \{e = R_0, R_{90}, R_{180}, R_{270}, H, V, D, D'\}$$

One way to describe the elements of D_4 is to say that each is a function or mapping $\mathbf{R}^2 \to \mathbf{R}^2$. For example, we view R_{90} as a function $R_{90}\colon \mathbf{R}^2 \to \mathbf{R}^2$ and write $R_{90}(A) = (B)$, $R_{90}(4,3) = (-3,4)$, and so on. Since each of the 8 elements of D_4 takes X to itself (that is, for any $x \in X$, $g \in D_4$, we have $g(x) \in X$) we may view any element in D_4 as a function $X \to X$. For example, if we set $g = H$, $a = (1/2, -1)$ and $b = (1/2, 1)$ it is natural to write $g(a) = b$. It is customary in this context to replace the parentheses by a dot, and write $g \cdot a = b$ to indicate the value of the function $g = H$ in the point $a = (1/2, -1)$.

This example motivates the following definition.

2.2 Definition of group action, first version

An *action of a group G on a set X* is a map $\varphi\colon G \times X \to X$ which satisfies the following properties (we write $g \cdot x$ to denote $\varphi(g,x)$).

$$e \cdot x = x \qquad \text{for all } x \in X \tag{2.2.1}$$

$$g \cdot (h \cdot x) = (gh) \cdot x \qquad \text{for all } x \in X, g, h \in G \tag{2.2.2}$$

Given an element $x \in X$, the *stabilizer* or *isotropy subgroup of x*, denoted $\mathrm{Stab}(x)$ or I_x, is the subset of all elements of G which fix x under the given action. To be precise,

$$\mathrm{Stab}(x) = I_x = \{g \in G \mid g \cdot x = x\}.$$

The *orbit of x*, denoted $\mathrm{Orb}(x)$ or O_x, is the set

$$\mathrm{Orb}(x) = O_x = \{g \cdot x \mid g \in G\}.$$

2.3 Examples of group actions

D_n acts on the regular n-gon

The elements of D_n are by definition the symmetries of the regular n-gon X. The natural action of D_n on X is defined by declaring $g \cdot x$ to be the value of the element $g \in D_n$, thought of as a function $g\colon X \to X$, on the element $x \in X$.

$\mathbf{Z}_n$ acts on the regular n-gon

We can think of $\mathbf{Z}_n$ as the subgroup of rotations

$$\mathbf{Z}_n = \{R_0, R_{360/n}, R_{2\cdot 360/n}, \ldots, R_{(n-1)360/n}\}$$

of D_n. In this way, $\mathbf{Z}_n$ inherits from D_n the natural action on the regular n-gon.

The permutation group of a set X acts on X

Given a nonempty set X, let $\mathrm{Perm}(X)$ denote the set of bijections of X to itself. The set $\mathrm{Perm}(X)$, called the *permutation group of the set* X, forms a group under the operation of composition. To be precise, let $f\colon X \to X$ and $g\colon X \to X$ be two bijections from X to itself. In the group $\mathrm{Perm}(X)$, the product fg is the map given by $(fg)(x) = f(g(x))$.

There is a natural action of $\mathrm{Perm}(X)$ on X given by $g\cdot x = g(x)$ for $g \in \mathrm{Perm}(X)$, $x \in X$.

Any group acts on itself by conjugation

Let G be a group and let $C\colon G \times G \to G$ be given by $C(g,h) = ghg^{-1}$. This defines an action of G on itself (exercise!) called *conjugation*.

2.4 First exercises on group actions

Let G be a group acting on a set X.

1. Prove that $\mathrm{Stab}(X)$ is a subgroup of G for any $x \in X$.
2. Let $x, y \in X$. Prove that either $O_x = O_y$ or $O_x \cap O_y = \emptyset$.
3. Prove or give a counterexample: if X is finite, then the number of elements in the orbit O_x is the same for every $x \in X$.
4. Verify that conjugation, defined above, does indeed define an action of G on itself.
5. Let $g \in G$, and define the function $\varphi_g\colon X \to X$ by $\varphi_g(x) = g \cdot x$. Show that φ_g is one-to-one and onto.

3 Group Homomorphisms

A defining characteristic of modern mathematics is the exploitation of the fact that the maps between objects can teach us about the nature of the objects themselves. In group theory, the maps between groups which "respect" the group operations, called *homomorphisms*, are central to the study of groups themselves.

3.1 Definition of group homomorphism

A *homomorphism φ from a group G to a group H* is a map $\varphi\colon G \to H$ which satisfies

$$\varphi(gh) = \varphi(g)\varphi(h)$$

for all g, h in G. The equation above says that the homomorphism φ "respects" the group operations of the domain and codomain. It is a consequence of the definition that a homomorphism respects the other basic elements of group structure, namely identity and inverses. The proof of the following proposition is an exercise.

(3.1.1) **Proposition.** Let $\varphi\colon G \to H$ be a group homomorphism, and let $1_G, 1_H$ denote the identity elements in G, H, respectively. Then we have the following.

$$\begin{aligned} \varphi(1_G) &= 1_H \\ \varphi(g^{-1}) &= \varphi(g)^{-1} \quad \text{for all } g \in G \end{aligned}$$

3.2 Examples

The sign map on the symmetric group

Let S_n denote the symmetric group on n symbols and let $\{-1, 1\} \subseteq \mathbf{R}^*$ be the two element subgroup of $\mathbf{R}^*$ under multiplication. The map $S_n \to \{-1, 1\}$ given by

$$\alpha \mapsto \begin{cases} 1 & \text{if } \alpha \text{ is even} \\ -1 & \text{if } \alpha \text{ is odd} \end{cases}$$

is a homomorphism called the *sign* or *determinant* map.

Multiplication times n

Let $n \in \mathbf{Z}$. Then the map $\mathbf{Z} \to \mathbf{Z}$ given by $k \mapsto kn$ is a homomorphism from the additive group of integers to itself.

Modulo n

Let $n \in \mathbf{N}$. Then the map $\mathbf{Z} \to \mathbf{Z}_n$ given by $k \mapsto k (\mathrm{mod}\ n)$ is a homomorphism of additive groups.

The exponential map

The map $\mathbf{R} \to \mathbf{R}^+$ given by $x \mapsto e^x$ is a group homomorphism from the group of real numbers under addition to the group of nonnegative reals under multiplication. In fact, this homomorphism is a bijection with inverse given by the natural log function. A bijective homomorphism is called an *isomorphism*.

Another exponential map

The map $\mathbf{R} \to S^1$ given by $t \mapsto e^{2\pi it} = \cos 2\pi t + i \sin 2\pi t$ is a homomorphism from the additive reals to the circle.

3.3 Further vocabulary about homomorphisms

Let $\varphi: G \to H$ be a group homomorphism. The set $K \subset G$ given by

$$K = \{g \in G \mid \varphi(g) = 1_H\}$$

is called the *kernel* of φ. The set $I = \varphi(G)$

$$I = \{h \in H \mid h = \varphi(g) \quad \text{for some } g \in G\}$$

is called the *image* of φ.

3.4 Exercises on group homomorphisms

1. Give a proof of Proposition (3.1.1).
2. Prove that the kernel of a homomorphism is a subgroup of the domain.
3. Prove that the image of a homomorphism is a subgroup of the codomain.
4. Identify the kernel and image for each of the examples in section 3.2 above.
5. Let K be the kernel of the homomorphism $\varphi: G \to H$. Show that, for any $g \in G, k \in K$, we have $gkg^{-1} \in K$.
6. Let $\varphi: G \times X \to X$ be a group action. Define $\Phi: G \to \mathrm{Perm}(X)$ by $\Phi(g)(x) = \varphi(g, x) = g \cdot x$. Show that Φ is a group homomorphism.
7. Let G be a group, let X be a set and let $\Phi: G \to \mathrm{Perm}(X)$ be a homomorphism of groups. Show that $\varphi: G \times X \to X$ given by $\phi(g, x) = \Phi(g)(x)$ defines an action of the group G on the set X.

Comment: The last two exercises in the section above prove that the following definition of group action is equivalent to the definition given in the earlier supplementary notes handout.

(3.4.1) **Definition.** An *action of a group G on a set X* is a group homomorphism $\Phi: G \to \mathrm{Perm}(X)$.

3.5 Left and right group actions, cosets

Recall that we have previously defined a left group action of G on a set X to be a map $\varphi\colon G \times X \to X$ satisfying $\varphi(e, x) = x$ and $\varphi(g, \varphi(h, x)) = \varphi(gh, x)$ for all $x \in X$, $g, h \in G$. Similarly, we define a *right* action of G on a set X to be a map $\varphi\colon X \times G \to X$ satisfying $\varphi(x, e) = x$ and $\varphi(\varphi(x, g), h) = \varphi(x, gh)$ for all $x \in X$, $g, h \in G$. Usually we will write $x \cdot g$ or simply xg to denote $\varphi(x, g)$. In this notation the defining properties of a right action $X \times G \to X$ are $x \cdot e = x$ and $(x \cdot g) \cdot h = x \cdot (gh)$.

Let G be a group and let H be a subgroup of G. The map $R\colon G \times H \to G$ given by $(g, h) \mapsto gh$ defines a right action of H on G. Similarly, the map $L\colon H \times G \to G$ given by $(g, h) \mapsto gh$ defines a left action of H on G. The orbit $\mathcal{O}_g$ of g under the right action R is called the *left coset gH of H in G*. Similarly, the orbit of g under the left action L is called the *right coset Hg of H in G*.

We denote by G/H, pronounced "G mod H," the set of left cosets of H in G. Similarly, we write $H\backslash G$ to denote the set of right cosets of H in G. The *natural (or canonical) projection* of G onto G/H is the map $\pi\colon G \to G/H$ given by $g \mapsto gH$. We usually think of the coset gH as an equivalence class in G and denote the class by $\overline{g}$ or $[g]$. The number of left cosets of H in G, which may be infinite, is called the *index* of H in G.

3.6 Exercises on cosets

1. Let G be a group and let H be a subgroup of G. Prove that the map $R\colon G \times H \to G$ given by $(g, h) \mapsto gh$ defines a right action of H on G. Similarly, prove that the map $L\colon H \times G \to G$ given by $(g, h) \mapsto gh$ defines a left action of H on G.

2. Prove that there is a bijection between any two cosets of H in G. (It follows that if H is finite, all the cosets have the same number of elements, equal to $|H|$.) Prove that there is a bijection between the set of left cosets and the set of right cosets of H in G. (This shows that the index of H in G also equals the number of right cosets of H.) Prove that the relation $\sim$ on G, defined by $x \sim y$ if x and y lie in the same left coset of H in G, is an equivalence relation on G.

3. Let G be a group and let H be a subgroup of G. Prove that the canonical projection is indeed *onto*. Prove that the subset of G that maps to $eH = \overline{e}$ is precisely the set $H \subseteq G$.

4. (Orbit-Stabilizer Theorem) Let G be a group which acts on a set X, and let $x \in X$. Show that there is a bijection between the orbit set O_x and the set G/I_x of left cosets of the stabilizer I_x. Use Lagrange's theorem to conclude that when G is finite, then $|G| = |O_x||I_x|$.

3.7 Normal subgroups and quotient groups

It sometimes happens that the set G/H of left cosets of a subgroup H of G is itself a group with the group operation given by $(aH)(bH) = (ab)H$. When this happens, the group G/H is called a *factor group* or *quotient group* of G, and H

is called a *normal* subgroup of G, denoted $H \lhd G$. Observe that when G/H is a factor group, the canonical projection $\pi\colon G \to G/H$ is a group homomorphism.

(3.7.1) **Group structure on coset space.** Let G be a group and let H be a subgroup of G. The following are equivalent.

(i) The subgroup H is the kernel of some group homomorphism $\varphi\colon G \to G'$ (where G' is some group).

(ii) We have $ghg^{-1} \in H$ for all $g \in G, h \in H$.

(iii) We have $gH = Hg$ for all $g \in G$.

(iii') For any $g \in G$, we have $\varphi^{-1}(\varphi(g)) = gH = Hg$.

(iv) The set of left cosets G/H is a group with operation $(aH)(bH) = (ab)H$ for $a, b \in G$.

(iv') The set of left cosets G/H is a group such that the canonical projection $\pi\colon G \to G/H$ is a group homomorphism.

3.8 Exercise on normal subgroups and factor groups

1. Prove theorem (3.7.1).
2. Prove that if G is abelian, then every subgroup of G is normal.
3. Prove that the alternating group A_n is a normal subgroup of the symmetric group S_n.
4. Let G be the integers $\mathbf{Z}$ and let $H = n\mathbf{Z} = \{nj\colon j \in \mathbf{Z}\}$. Identify the quotient group G/H as a familiar group.
5. Let G be the real numbers $\mathbf{R}$ and let H be the integers $\mathbf{Z}$. Identify the quotient group G/H as a familiar group.

4 Maps on Factor Groups

4.1 Motivation

A basic notion in mathematics is that of the equivalence class. Many useful sets arise as equivalence classes on larger sets. For example, the set

$$\mathbf{Z}_n = \{0, 1, \ldots, n-1\}$$

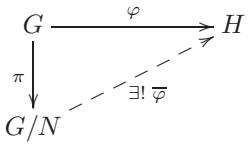
is on the one hand merely a finite set of n symbols, but more to the point, is a set of equivalence classes defined on the integers. For example, the element denoted by 2 in the set $\mathbf{Z}_5$ is the equivalence class

$$\{\ldots, -3, 2, 7, 12, \ldots\} \subseteq \mathbf{Z}.$$

As commented in the introductory paragraph to the supplementary notes on group homomorphisms, it is desirable to study functions defined on an object in order to study the object. Since sets of equivalence classes are widespread, we often want to construct functions on these sets. This installment of supplementary notes presents the key theorem in a special case of this general problem, namely, the construction of group homomorphisms on factor groups.

4.2 Main theorem for maps on factor groups

(4.2.1) **Maps on Factor Groups.** Let $\varphi: G \to H$ be a group homomorphism, let $N \subseteq G$ be a normal subgroup of G, and let $\pi: G \to G/N$ be the natural projection. There is a unique homomorphism $\overline{\varphi}: G/N \to H$ such that $\overline{\varphi} \circ \pi = \varphi$ if and only if $N \subseteq \ker\varphi$. This is summarized by the following commutative diagram.



To construct maps on a factor group G/N, theorem (4.2.1) says you should look for maps on G. Then you get a map on G/N if N is contained in the kernel of the map on G. Further, all maps on G/N arise in this manner.

4.3 Exercises

1. Prove theorem (4.2.1).
2. Use the theorem to describe the set of all homomorphisms $\mathbf{Z}_2 \to \mathbf{Z}_6$.
3. Same for $\mathbf{Z}_6 \to \mathbf{Z}_2$.
4. Same for $\mathbf{Z}_p \to \mathbf{Z}_q$ where p, q are distinct primes.
5. Formulate and prove a theorem that describes the set of homomorphisms $\mathbf{Z}_n \to \mathbf{Z}_m$.