Groups and Symmetry HW2 Solutions

Tair Akhmejanov

September 22, 2014

Exercise 1. 3.1

Proof. In all cases addition is associative, the identity element is 0, check that inverses exist. Checking that the set is closed under addition is the most nontrivial.

□

Exercise 2. 3.2

Proof. The inverse to $(a + b\sqrt{2})$ is

$$\begin{aligned}\frac{1}{a+b\sqrt{2}} &= \frac{1}{a+b\sqrt{2}} \cdot \frac{a-b\sqrt{2}}{a-b\sqrt{2}} \\ &= \frac{a-b\sqrt{2}}{a^2-2b^2}.\end{aligned}$$

Note that this is well defined because if $a-2b^2 = 0$ then $a/b = \sqrt{2}$ if b is nonzero and $b/a = 1/\sqrt{2}$ if a is nonzero, both of which are impossible since a, b are both rational. If both a, b are zero then $a + b\sqrt{2}$ is zero, so is not even contained in the set. So setting $c = \frac{a}{a^2-2b^2}$ and $d = \frac{-b}{a^2-2b^2}$ we see that $a+b\sqrt{2}$ has an inverse.

It can be seen that the set is closed under multiplication by multiplying out two such elements and grouping like terms. Multiplication is associative because it is the restriction of multiplication of real numbers. The identity element $1+0\sqrt{2}$ is contained in the set. □

Exercise 3. 3.3

Proof. Let $z, w \in \mathbb{C}$ such that $z^n = 1$ and $w^n = 1$. Then $(zw)^n = z^n w^n = 1$ where the penultimate equality holds because multiplication of complex numbers is commutative. Thus, zw is in G, so G is closed under multiplication. Multiplication of complex numbers is associative, so multiplication restricted to the subset $G \subseteq \mathbb{C}$ is associative. The complex number 1 satisfies 1^n and is the multiplicative identity. Each complex number z has an inverse $1/z$, but we must check that $(1/z)^n = 1$ when $z^n = 1$. We have $1 = (z \cdot 1/z)^n = z^n(1/z)^n = (1/z)^n$, as desired. Thus, G is a group (G is called the set of nth roots of unity). □

Exercise 4. 3.6

Proof. Find the inverses of each of the elements and make sure that they are contained in the set. □

Exercise 5. 3.8

Proof. The elements 11 and 2 do not have inverses $\mod 22$, so if they are in the subset then the subset cannot form a group. □

Exercise 6. 3.9

Proof. For a prime p and integers n, m, if p does not divide n nor m, then p does not divide $n \cdot m$. Given $1 \leq x, y \leq p-1$, we have the p does not divide x nor y, so p does not divide $x \cdot y$ either. Thus, none of $x, 2x, 3x, \cdots, (p-1)x$ is a multiple of p.

We claim that the list $x, 2x, 3x, \cdots, (p-1)x$ is a list of $p-1$ distinct numbers $\mod p$. To get a contradiction suppose that this is not the case, i.e. $ax \equiv bx \mod p$ for $1 \leq a < b \leq p-1$. Then $(b-a)x \equiv 0 \mod p$ where $1 \leq b-a < p-1$, but we just proved that this cannot happen. Since $x, 2x, 3x, \cdots, (p-1)x$ is a list of $p-1$ distinct numbers $\mod p$, one of them must be equal to $1 \mod p$, so there exists a z such that $xz \equiv 1 \mod p$. □

Exercise 7. 3.10

Proof. When n is prime exercise 3.9 shows that the set $\{1, \ldots, n-1\}$ is closed under multiplication $\mod n$. The set contains the identity element 1. Exercise 3.5 shows that multiplications $\mod n$ is associative. And finally exercise 3.9 also shows that every element has an inverse. If n is composite, then $n = ab$ for two numbers $1 \leq a, b \leq n-1$, so that $ab \equiv 0 \mod n$, so $\{1, \ldots, n-1\}$ is not closed under multiplication. □

Exercise 8. 4.1

Proof. The dihedral group D_n can be written as the set of $2n$ elements

$$\{e, s, r, r^2, \ldots, r^{n-1}, rs, r^2s, \ldots, r^{n-1}s\}$$

where s is the reflection through a vertex and opposite side of the n-gon if n is odd and is the reflection through opposite vertices of the n-gon if n is even, and r is the rotation $2\pi/n$. Recall from the text the identity $sr = r^{n-1}s$ from which we see the general relation $sr^k = r^{n-k}s$. Then squaring any r^ks gives $r^ksr^ks = r^kr^{n-k}s^2 = r^n \cdot e = e$, so r^ks has order two for every $0 \leq k \leq n-1$, which is n elements. An element of the form r^k has order $lcm(k, n)/k$, which is 2 only if n is even and $k = n/2$. Thus, if n is even then there are $n+1$ elements of order two and if n is odd then there are n element of order two. □

Exercise 9. 4.9

Proof. (a) For a matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, the value $ad - bc$ is the determinant. The determinant is a multiplicative function, i.e. $\det(A \cdot B) = \det(A) \cdot \det(B)$. So if $\det(A) = 1 = \det(B)$, then $\det(AB) = 1$ showing that the set is closed under multiplication. If you did not know this, then simply multiply out two matrices in the set and check that the resulting determinant equals 1.

Matrix multiplication is associative so its restriction to this subset of matrices is also associative.

The identity matrix $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the multiplicative identity and satisfies $1 \cdot 1 - 0 \cdot 0 = 1$.

The inverse to matrix A above is $A^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$, which has $ad - ((-b)(-c)) = ad - bc = 1$. Or note that any matrix A with nonzero determinant has an inverse A^{-1} and by the multiplicativity of the determinant $1 = \det(I) = \det(AA^{-1}) = \det(A)\det(A^{-1}) = \det(A^{-1})$.

(b) Multiply A to see that $A^4 = I$, so has order 4. Multiply out B to see $B^3 = I$, so has order 3. On the other hand, $AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, and $(AB)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$, so has infinite order. Likewise, $BA = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$ and $(BA)^n = \begin{pmatrix} 1 & 0 \\ -n & 1 \end{pmatrix}$, so BA also has infinite order.

□

Exercise 10. 4.10

Proof. Note that the base case $n = 3$ holds because it is the usual associativity law. Assume the inductive hypothesis: for all $1 \leq k \leq n - 1$ when given any k elements $x_1, \ldots, x_k \in G$, the product $x_1 \cdots x_k$ gives the same element no matter in which order the group multiplication is carried out, i.e. the product is well-defined. Now consider a product of n elements $x_1 \cdots x_n$ and bracket the element in two different ways,

$$(x_1 \cdots x_r)(x_{r+1} \cdots x_n)$$
$$(x_1 \cdots x_s)(x_{s+1} \cdots x_n),$$

where $1 \leq r < s \leq n-1$. By the inductive hypothesis the elements $(x_1 \cdots x_r), (x_{r+1} \cdots x_s), (x_{s+1} \cdots x_n)$ are well-defined. Then

$$\begin{aligned}(x_1 \cdots x_r)(x_{r+1} \cdots x_n) &= (x_1 \cdots x_r)\left[(x_{r+1} \cdots x_s)(x_{s+1} \cdots x_n)\right] \\ &= \left[(x_1 \cdots x_r)(x_{r+1} \cdots x_s)\right](x_{s+1} \cdots x_n) \text{ the usual associativity law} \\ &= (x_1 \cdots x_s)(x_{s+1} \cdots x_n).\end{aligned}$$