Homework 1 Solutions

Based on the third edition of *Abstract Algebra* of Dummit and Foote.

Section 1.1: Basic Axioms and Examples

Section 1, Exercise 25

Prove that if $x^2 = 1$ for all $x \in G$ then G is abelian.

Solution. Let $a, b \in G$. The hypothesis gives $a^2 = b^2 = 1$, so $a^{-1} = a$ and $b^{-1} = b$. It also applies to ab, and hence $(ab)^2 = 1$. Therefore $ab = (ab)^{-1}$. Using the rule for the inverse of a product,

$$ab = (ab)^{-1} = b^{-1}a^{-1} = ba.$$

Thus every two elements of G commute, so G is abelian. □

Section 1, Exercise 26

Assume H is a nonempty subset of $(G, *)$ which is closed under the binary operation on G and is closed under inverses, i.e., for all h and $k \in H$, hk and $h^{-1} \in H$. Prove that H is a group under the operation $*$ restricted to H (such a subset H is called a subgroup of G).

Solution. Closure of the restricted operation is one of the assumptions. Associativity on H is inherited from G: for $h, k, \ell \in H$,

$$(hk)\ell = h(k\ell),$$

because this identity already holds in G.

It remains to locate the identity and inverses inside H. Since H is nonempty, choose $h \in H$. By closure under inverses, $h^{-1} \in H$, and by closure under the operation,

$$1 = hh^{-1} \in H.$$

This element is the identity for the restricted operation. Finally, the assumed inverse closure says that every $k \in H$ has $k^{-1} \in H$, and the equations $kk^{-1} = k^{-1}k = 1$ continue to hold in H. Hence all group axioms hold on H. □

Section 1, Exercise 29

Prove that $A \times B$ is an abelian group if and only if both A and B are abelian.

Solution. We use the group structure on $A \times B$ established in Exercise 28, with coordinatewise multiplication

$$(a, b)(a', b') = (aa', bb').$$

Suppose first that A and B are abelian. For arbitrary $(a, b), (a', b') \in A \times B$,

$$(a, b)(a', b') = (aa', bb') = (a'a, b'b) = (a', b')(a, b),$$

so $A \times B$ is abelian.

Conversely, suppose that $A \times B$ is abelian. For $a, a' \in A$, the elements $(a, 1_B)$ and $(a', 1_B)$ commute. Comparing first coordinates in

$$(a, 1_B)(a', 1_B) = (a', 1_B)(a, 1_B)$$

gives $aa' = a'a$. Thus A is abelian. Applying the same argument to $(1_A, b)$ and $(1_A, b')$ shows that $bb' = b'b$ for all $b, b' \in B$, so B is abelian as well. □

Section 1, Exercise 31

Prove that any finite group G of even order contains an element of order 2. [Let $I(G)$ be the set $\{g \in G \mid g \neq g^{-1}\}$. Show that $I(G)$ has an even number of elements and every nonidentity element of $G - I(G)$ has order 2.]

Solution. The inversion map $g \mapsto g^{-1}$ carries $I(G)$ to itself. No element of $I(G)$ is fixed by this map, and applying the map twice returns the original element. Consequently, the elements of $I(G)$ occur in disjoint two-element pairs $\{g, g^{-1}\}$, so $\operatorname{ord} I(G)$ is even.

Since both $\operatorname{ord} G$ and $\operatorname{ord} I(G)$ are even, the complement $G - I(G)$ also has even cardinality. It contains the identity. Therefore it cannot consist only of the identity, because a one-element set has odd cardinality. Choose $x \in G - I(G)$ with $x \neq 1$. By the definition of the complement, $x = x^{-1}$, so $x^2 = 1$. Since $x \neq 1$, its order is exactly 2. □

Section 1, Exercise 32

If x is an element of finite order n in G, prove that the elements $1, x, x^2, \ldots, x^{n-1}$ are all distinct. Deduce that $\operatorname{ord} x \leq \operatorname{ord} G$.

Solution. Suppose two of the displayed powers are equal. Write $x^i = x^j$ with $0 \leq i < j \leq n-1$. Multiplying by x^{-i} gives

$$x^{j-i} = 1.$$

But $0 < j - i < n$, contradicting the definition of $n = \operatorname{ord} x$ as the least positive exponent for which $x^n = 1$. Hence the n displayed elements are distinct. They all belong to G, so G contains at least n elements. Thus $\operatorname{ord} x = n \leq \operatorname{ord} G$ (with the conclusion immediate as well when G is infinite). □

1 Section 1.3: Symmetric Groups

Section 3, Exercise 10

Prove that if σ is the m-cycle $(a_1\ a_2\ \ldots\ a_m)$, then for all $i \in \{1, 2, \ldots, m\}$, $\sigma^i(a_k) = a_{k+i}$, where $k + i$ is replaced by its least residue mod m when $k + i > m$. Deduce that $\operatorname{ord} \sigma = m$.

Solution. By the definition of the cycle, $\sigma(a_j) = a_{j+1}$, with subscripts read cyclically, so that $\sigma(a_m) = a_1$. Induction on i now gives

$$\sigma^i(a_k) = a_{k+i},$$

where the subscript is reduced modulo m to one of $1, \ldots, m$. Indeed, if the formula holds for i, then

$$\sigma^{i+1}(a_k) = \sigma(a_{k+i}) = a_{k+i+1}.$$

Taking $i = m$ shows that σ^m fixes every a_k. It also fixes every point outside the support of the cycle, so $\sigma^m = 1$. On the other hand, if $1 \leq i < m$, then $\sigma^i(a_1) = a_{1+i} \neq a_1$, so $\sigma^i \neq 1$. Hence the least positive exponent producing the identity is m, and $\operatorname{ord} \sigma = m$. □

Section 3, Exercise 11

Let σ be the m-cycle $(1\ 2\ \ldots\ m)$. Show that σ^i is also an m-cycle if and only if i is relatively prime to m.

Solution. Put $d = \gcd(i, m)$. Repeated application of σ^i advances a symbol by i positions modulo m. The length of the orbit of 1 is therefore the least positive integer r for which

$$ri \equiv 0 \pmod{m}.$$

Writing $i = di_0$ and $m = dm_0$, with $\gcd(i_0, m_0) = 1$, the congruence is equivalent to $m_0 \mid r$. Its least positive solution is thus

$$r = m_0 = \frac{m}{\gcd(i, m)}.$$

The permutation σ^i is one m-cycle exactly when the orbit of 1 has all m symbols, i.e., exactly when $m/d = m$. This is equivalent to $d = 1$, or to i being relatively prime to m. □

Section 3, Exercise 12

(a) If $\tau = (1\ 2)(3\ 4)(5\ 6)(7\ 8)(9\ 10)$ determine whether there is a n-cycle σ $(n \geq 10)$ with $\tau = \sigma^k$ for some integer k.

(b) If $\tau = (1\ 2)(3\ 4\ 5)$ determine whether there is a n-cycle σ $(n \geq 5)$ with $\tau = \sigma^k$ for some integer k.

Solution. We use the following consequence of Exercise 10. If σ is an n-cycle and $d = \gcd(n, k)$, then σ^k is a product of exactly d disjoint cycles, all of the same length n/d.

(a) Such a cycle does exist, take $\sigma = (1\ 3\ 5\ 7\ 9\ 2\ 4\ 6\ 8\ 10)$.

(b) No such n-cycle exists since the permutation τ has one cycle of length 2 and one of length 3.

□

Section 3, Exercise 14

Let p be a prime. Show that an element has order p in S_n if and only if its cycle decomposition is a product of commuting p-cycles. Show by an explicit example that this need not be the case if p is not prime.

Solution. Let $\pi \in S_n$, and write its disjoint cycle decomposition using only its nontrivial cycles. Suppose first that $\operatorname{ord} \pi = p$. If C is a cycle of length r occurring in this decomposition, then $\pi^p = 1$ implies $C^p = 1$ on the support of C. By Exercise 10, the order of C is r, so $r \mid p$. Since $r > 1$ and p is prime, $r = p$. Thus every nontrivial cycle is a p-cycle; being disjoint, these cycles commute.

Conversely, suppose that π is a nonempty product of disjoint p-cycles. The cycles commute and each has pth power equal to the identity, so $\pi^p = 1$. If $1 \leq r < p$, then the rth power of each p-cycle is nonidentity, so $\pi^r \neq 1$. Therefore $\operatorname{ord} \pi = p$.

In the above, the assumption that p is a prime is essential. Indeed, in S_5 the permutation

$$(1\ 2)(3\ 4\ 5)$$

has order 6: its sixth power is the identity, while an exponent killing it must be divisible by both 2 and 3. Nevertheless, its cycle decomposition is not a product of 6-cycles (indeed, S_5 contains no 6-cycle). □

Section 3, Exercise 15

Prove that the order of an element in S_n equals the least common multiple of the lengths of the cycles in its cycle decomposition. [Use Exercise 10 and Exercise 24 of Section 1.]

Solution. Let the disjoint cycle decomposition of $\pi \in S_n$ be

$$\pi = C_1 C_2 \cdots C_r,$$

where C_j has length m_j. Disjoint cycles commute, and Exercise 10 gives $\operatorname{ord} C_j = m_j$. Set $L = \operatorname{lcm}(m_1, \ldots, m_r)$. Since every m_j divides L, we have $C_j^L = 1$ for every j. Using commutativity (as in Exercise 24 of Section 1),

$$\pi^L = (C_1 C_2 \cdots C_r)^L = C_1^L C_2^L \cdots C_r^L = 1.$$

Thus $\operatorname{ord} \pi$ divides L.

Conversely, if $\pi^t = 1$, restrict this equality to the support of C_j. All the other disjoint cycles act trivially there, so $C_j^t = 1$. Hence $m_j \mid t$ for every j, and consequently $L \mid t$. $\square$

Section 1.4: Matrix Groups

Section 4, Exercise 10

Let

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \;\middle|\; a, b, c \in \mathbb{R},\ a \neq 0,\ c \neq 0 \right\}.$$

(a) Compute the product of $\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix}$ and $\begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix}$ to show that G is closed under matrix multiplication.

(b) Find the matrix inverse of $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ and deduce that G is closed under inverses.

(c) Deduce that G is a subgroup of $GL_2(\mathbb{R})$ (cf. Exercise 26, Section 1).

(d) Prove that the set of elements of G whose two diagonal entries are equal (i.e., $a = c$) is also a subgroup of $GL_2(\mathbb{R})$.

Solution.

(a) Direct multiplication gives

$$\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix} = \begin{pmatrix} a_1 a_2 & a_1 b_2 + b_1 c_2 \\ 0 & c_1 c_2 \end{pmatrix}.$$

The product is upper triangular, and $a_1 a_2 \neq 0$ and $c_1 c_2 \neq 0$. Its upper-right entry is a real number, so the product lies in G.

(b) We have

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}^{-1} = \begin{pmatrix} a^{-1} & -\dfrac{b}{ac} \\ 0 & c^{-1} \end{pmatrix}.$$

Both diagonal entries are nonzero, so this inverse belongs to G. Hence G is closed under inverses.

(c) The identity matrix belongs to G. Part (a) gives closure under multiplication, part (b) gives closure under inverses, and associativity is inherited from matrix multiplication in $GL_2(\mathbb{R})$. Equivalently, Exercise 26 applies. Thus G is a subgroup of $GL_2(\mathbb{R})$.

(d) Let

$$H = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \;\middle|\; a, b \in \mathbb{R},\ a \neq 0 \right\}.$$

It is nonempty because $I \in H$. If two matrices in H have parameters (a_1, b_1) and (a_2, b_2), their product is

$$\begin{pmatrix} a_1a_2 & a_1b_2 + b_1a_2 \\ 0 & a_1a_2 \end{pmatrix} \in H.$$

The inverse formula from part (b), with $c = a$, becomes

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}^{-1} = \begin{pmatrix} a^{-1} & -b/a^2 \\ 0 & a^{-1} \end{pmatrix} \in H.$$

Thus H is nonempty and closed under products and inverses, so Exercise 26 shows that H is a subgroup of $GL_2(\mathbb{R})$.

$\square$