Problem Set Mash 1

Section 1.2

15. Find a set of generators and relations for $\mathbb{Z}/n\mathbb{Z}$.

$\langle \bar{1} | \bar{1}^n = \bar{0} \rangle = \mathbb{Z}/n\mathbb{Z}$.

Section 1.4

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.

$$\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 + 0b_2 & a_1b_2 + b_1c_2 \\ 0a_2 + c_10 & 0b_2 + c_1c_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 & a_1b_2 + b_1c_2 \\ 0 & c_1c_2 \end{pmatrix}$$

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

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

(c) Deduce that G is a subgroup of $GL_2(\mathbb{R})$.

Since G is closed under the group operation and inverses, for any $x, y \in G$, $xy^{-1} \in G$ and by the subgroup criterion, G is a subgroup of $GL_2(\mathbb{R})$.

(d) Prove that the set of elements of G whose two diagonal entrees are equal is also a subgroup of $GL_2(\mathbb{R})$.

Let $\begin{pmatrix} a & b \\ b & a \end{pmatrix}, \begin{pmatrix} c & d \\ d & c \end{pmatrix} \in GL_2(\mathbb{R})$

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix} \begin{pmatrix} c & d \\ d & c \end{pmatrix} = \begin{pmatrix} ac + bd & ad + bc \\ bc + ad & bd + ac \end{pmatrix}$$

Thus the set of matrices with equal diagonal entrees is closed under matrix multiplication.

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix} \begin{pmatrix} \frac{a}{a^2-b^2} & \frac{-b}{a^2-b^2} \\ \frac{-b}{a^2-b^2} & \frac{a}{a^2-b^2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Thus $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$ has an inverse in the set and the set of matrices with equal diagonal entrees is closed under inverses. Therefore it is a subgroup.

Section 1.6

9. Prove that D_{24} and S_4 are not isomorphic.

We first prove that the order of an element in S_4 is at most 4. Let σ be a permutation in S_4. Suppose σ is a cycle. Since σ is a permutation on a four element set, it can be at most a 4-cycle. Thus, if σ is a cycle, it has order at most four. Suppose σ is not a cycle, then either σ is the identity or is the product of two disjoint 2-cycles. The product of two disjoint 2-cycles has order 2 and the identity has order 1. Thus, all elements of S_4 have at most order 4.

For all D_{2n}, the element r has order n. Thus, the element $r \in D_{24}$ has order 12. Suppose there exists an isomorphism $\phi : D_{24} \to S_4$, then for all $x \in D_{24}$, $|x| = |\phi(x)|$ but there exists an element of D_{24} with order greater than four, thus leading to a contradiction. Therefore $D_{24} \ncong S_4$.

18. Let G be a group. Prove that the mapping from G to itself defined by $g \mapsto g^2$ is a homomorphism if and only if G is abelian.

Let $\phi : G \to G$ denote the aforementioned map.

Suppose G is abelian, and let a, b be arbitrary elements in G. Then

$$\phi(ab) = (ab)^2 = (ab)(ab) = a(ba)b = a(ab)b = (aa)(bb) = a^2b^2 = \phi(a)\phi(b).$$

Since a and b are arbitrary, ϕ preserves the group operation for all elements of G and is thus a homomorphism.

Now suppose that ϕ is a homomorphism and again let a, b be arbitrary elements of G. Then $\phi(ab) = \phi(a)\phi(b)$ and so $(ab)(ab) = (aa)(bb)$. Multiplication on the left by a^{-1} and on the right by b^{-1} to both sides of the equation gives:

$$\begin{aligned} a^{-1}(abab)b^{-1} &= a^{-1}(aabb)b^{-1} \\ (a^{-1}a)(ba)(bb^{-1}) &= (a^{-1}a)(ab)(bb^{-1}) \\ 1(ba)1 &= 1(ab)1 \\ ba &= ab. \end{aligned}$$

Thus for all $a, b \in G$, $ab = ba$ and G is abelian.

Section 1.7

4. Let G be a group acting on a set A and fix some $a \in A$. Show that the following sets are subgroups of G.

   (a) The kernel of the action.

   Let $b \in A$ be an arbitrary element of A. We first note that $1b = b$ by definition, and since b is arbitrary, the identity of G is in the kernel and thus the kernel is nonempty. Next, let $x \in G$ be an element of the kernel. Then $xb = b$ and since $1 = x^{-1}x$ in G, we have $b = 1b = (x^{-1}x)b = x^{-1}(xb) = x^{-1}b$. Since b is arbitrary, x^{-1} is in the kernel and since

x is arbitrary, the kernel is closed under inverses. Suppose x, y are elements of the kernel, then $(xy)b = x(yb) = xb = b$. Again, since b is arbitrary, xy is in the kernel and thus the kernel is nonempty, closed under the group operation of G, and closed with respect to inverses. Therefore the kernel is a subgroup of G.

(b) $\{g \in G : ga = a\}$.

The set above is commonly called the stabilizer of a in G. By definition, $1a = a$ and so the identity element of G is in the stabilizer of a. Let $g \in G$ be an element of the stabilizer of a in G. Then $ga = a$ and since $1 = g^{-1}g$ in G, we have $a = 1a = (g^{-1}g)a = g^{-1}(ga) = g^{-1}a$. Thus g^{-1} is in the stabilizer and the stabilizer of a is closed under inverses. Let g, h be elements of the stabilizer of a. Then $(gh)a = g(ha) = ga = a$ and so the stabilizer is closed under the group operation. Thus, the stabilizer is nonempty, closed with respect to the group operation, and closed with respect to inverses and therefore the stabilizer of a is a subgroup of G.

Section 2.1

10. (a) Prove that if H and K are subgroups of G, then their intersection $H \cap K$ is a subgroup of G.

The identity element of G is in both H and K and thus $H \cap K$ is nonempty. Let $x \in H \cap K$, then x is an element of both H and K. Since H and K are both closed under inverses, x^{-1} is in both H and K and thus is in $H \cap K$. Suppose $x, y \in H \cap K$. Then x and y are in both H and K. Since both H and K are closed with respect to the group operation, xy is in both H and K and thus xy is in $H \cap K$. Thus $H \cap K$ is nonempty, closed under inverses, and closed under group operation in G so $H \cap K$ is a subgroup.

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

Let $H = \bigcap_{i \in I} G_i$ denote the intersection of a collection of subgroups G_i indexed by a set I. For every $i \in I$, the subgroup G_i contains the identity element in G. Thus $1 \in H$ and so H is nonempty. Suppose $x \in H$. Then x is an element of G_i for every $i \in I$. For each $i \in I$, G_i is closed under inverses, and thus $x^{-1} \in G_i$ for each $i \in I$. Thus, x^{-1} is in H. Suppose x, y are elements of H. Then for each $i \in I$, both x and y are in G_i. Since each G_i is closed under the group operation, for each $i \in I$, $xy \in G_i$. Therefore $xy \in H$ and H is closed under the group operation. Thus H is a subgroup of G.

Section 2.2

6. Let H be a subgroup of G.

(a) Show that $H \leq N_G(H)$ Give an example to show that this is not necessarily true if H is not a subgroup.

Since H is a subgroup of G, it is already closed under inverses, we need only show that it is closed under the group operation with respect to $N_G(H)$. To do this, it is sufficient to show that $H \subseteq N_G(H)$.

Let h be a fixed, arbitrary element of H and let g be an arbitrary element of H. By closure of H under inverses and the group operation, $hgh^{-1} \in H$. Since g is arbitrary, $hgh^{-1} \in H$ for any $g \in H$. Therefore $h \in N_G(H)$. Since h is arbitrary, for each $h \in H$, $h \in N_G(H)$ and thus $H \subseteq N_G(H)$.

Let $G = \mathbb{Z}/2\mathbb{Z}$. Let $A = \{\bar{1}\}$. Then $\bar{0}\bar{1}\bar{0} = \bar{1}$ and $\bar{1}\bar{1}\bar{1} = \bar{1}$ so $N_G(A) = \{\bar{0}, \bar{1}\}$. The subset does not contain the identity element and thus cannot be a subgroup of $N_G(A)$.

(b) Show that $H \leq C_G(H)$ if and only if H is abelian.

If $H \leq C_G(H)$, then H is abelian because $C_G(H)$ is abelian and any subgroup of an abelian group is abelian. Suppose H is abelian, since all elements of H commute with one another, $H \subseteq C_G(H)$. Since H is a subgroup of G, we have that G is closed under the group operation with respect to $C_G(H)$ and closed under inverses with respect to $C_G(H)$. Hence, $H \leq C_G(H)$.

Section 2.3

16. Assume $|x| = n$ and $|y| = m$. Suppose that x and y commute. Prove that $|xy|$ divides the least common multiple of m and n. Need this be true if x and y does not commute? Give an example of commuting elements that the order of xy is not equal to the least common multiple of $|x|$ and $|y|$.

We first show that if x and y commute, then for all $k \in \mathbb{N}$, $(xy)^k = x^k y^k$. We proceed by induction. For $k = 1$, we have $(xy)^1 = x^1 y^1$. Suppose that the result holds true for all numbers less than or equal to k. Then $(xy)^{k+1} = (xy)^k(xy) = (xy)^k(yx) = (x^k y^{k+1} x) = x^k x y^{k+1} = x^{k+1} y^{k+1}$. By induction, $x^k y^k = (xy)^k$ for all $k \in \mathbb{N}$.

Since $\text{lcm}(m, n)$ is a multiple of m and n, $x^{\text{lcm}(m,n)} = 1$ and $y^{\text{lcm}(m,n)} = 1$. Therefore $(xy)^{\text{lcm}(m,n)} = x^{\text{lcm}(m,n)} y^{\text{lcm}(m,n)} = 1$ by the previous result.

Suppose $|xy| = l$ does not divide $\text{lcm}(m, n)$, then there exists $k, r \in \mathbb{N}$ with $0 < r < l$ such that $\text{lcm}(m, n) = kl + r$. Then $(xy)^{\text{lcm}(m,n)} = (xy)^{kl+r} = (xy)^{kl}(xy)^r = \left((xy)^l\right)^k (xy)^r = 1^k (xy)^r = (xy)^r$. Since r is nonzero and less than $l = |xy|$, $(xy)^r$ is not equal to the identity. Therefore $(xy)^{\text{lcm}(m,n)} \neq 1$ which contradicts the previous result. Therefore $|xy|$ must divide $\text{lcm}(m, n)$.

This result need not be true if the elements do not commute. In S_3, consider the elements $(1\ 2)$ and $(2\ 3)$. Both elements have order two, so the least common multiple of them is two. The product $(1\ 2) \circ (2\ 3) = (1\ 2\ 3)$ so the order of their product is three, which does not divide two.

Any two elements of a group with order two or higher that are inverses of one another commute, and the order of their product is one.

Section 2.4

7. Prove that the subgroup of S_4 generated by $(1\ 2)$ and $(1\ 3)(2\ 4)$ is isomorphic to the dihedral group of order 8.

We have that $(1\ 2)^2 = ((1\ 3)(2\ 4))^2 = 1$ and $(1\ 2) \circ (1\ 3)(2\ 4) = (1\ 3\ 2\ 4)$. The element $(1\ 3\ 2\ 4) = b$ has order 4 with $b^2 = (1\ 2)(3\ 4)$, $b^3 = (1\ 4\ 2\ 3)$. The inverse of $(1\ 3\ 2\ 4)$ is $(1\ 4\ 2\ 3)$ and $(1\ 2) \circ (1\ 3\ 2\ 4) = (1\ 3)(2\ 4) = (1\ 4\ 2\ 3) \circ (1\ 2)$.

Thus, there is an element $(1\ 2) = a$ with $a^2 = 1$ and an element $(1\ 3\ 2\ 4) = b$ such that $b^4 = 1$. The relation $ab = b^{-1}a$ is satisfied and thus the relations of D_8 are satisfied. Thus, there exists a

homomorphism from $\phi : D_8 \to \langle a, b\rangle$ defined by $\phi(r^x s^y) = b^x \circ a^y$. Since the powers of b are unique for $1, 2$, and 3, this homomorphism is injective. Hence, the subgroup generated by a and b is isomorphic to D_8.

11. Show that $SL_2(\mathbb{F}_3)$ and S_4 are two nonisomorphic groups of order 24.

We show that $SL_2(\mathbb{F}_3)$ contains an element that commutes with all other elements of $SL_2(\mathbb{F}_3)$. Consider the element $A = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$. This matrix is in $SL_2(\mathbb{F}_3)$ since the determinant is equal to 1 in $\mathbb{F}_3$. We have that for arbitrary element $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{F}_3)$,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 2a & 2b \\ 2c & 2d \end{pmatrix}$$
$$\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 2a & 2b \\ 2c & 2d \end{pmatrix}$$

Thus A is is a nontrival element of $SL_2(\mathbb{F}_3$ that commutes with all elements of $SL_2(\mathbb{F}_3$.

Consider S_4. Let $\sigma \in S_4$ be a permutation not equal to the identity. Then there exists an element a in the set $\{1, 2, 3, 4\}$ such that $\sigma(a) \neq a$. Let $b = \sigma(a)$ and let c be an element in $\{1, 2, 3, 4\}$ not equal to a or b. Consider the element $\sigma_0 = (b\ c)$. We have $\sigma_0 \circ \sigma(a) = \sigma_0(b) = c$ and $\sigma \circ \sigma_0(a) = \sigma(a) = b$. Thus $\sigma_0 \circ \sigma(a) \neq \sigma \circ \sigma_0(a)$ and σ_0 does not commute with σ. Since σ is arbitrary, for any nontrivial element in S_4, there exists an element of S_4 which does not commute with that element.

Suppose there exists an isomorphism $\phi : S_4 \to SL_2(\mathbb{F}_3)$. Let $\sigma \in S_4$ be such that $\phi(\sigma) = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = A$ and let σ_0 be an element of S_4 that does not commute with σ. Let $\phi(\sigma_0) = B$. Then $\phi(\sigma_0 \circ \sigma) = AB = BA = \phi(\sigma \circ \sigma_0)$. Since ϕ is injective, this implies that $\sigma \circ \sigma_0 = \sigma_0 \circ \sigma$, which is a contradiction.