Problem Set 2
Abstract Algebra I

Bennett Rennier
barennier@gmail.com

January 15, 2018

Lemma 1 Let $|x| = n$. Then $x^k = 1$ if and only if $n \mid k$

Proof. We see that if $k = n \cdot p$, then $x^k = x^{np} = (x^n)^p = 1^p = 1$.

Conversely, let $x^k = 1$. Then $k = qn + r$ where $0 \leq r < n$. Thus, $x^k = x^{qn+r} = x^{qn}x^r = (x^n)^q x^r = 1^q x^r = x^r$. This means that $x^r = 1$. However, $0 \leq r < n$ and n is the smallest integer greater than 0 such that $x^n = 1$. This must mean that $r = 0$. Thus, $x^k = x^r = x^0 = 1$. □

Section 1.1

Exercise 25. Prove that if $x^2 = 1$ for all $x \in G$, then G is abelian

Proof. Let $x, y \in G$. This means that $xy \in G$. Thus $(xy)^2 = xyxy = 1$. Multiplying on the left by $y^{-1}x^{-1}$, we get $xy = y^{-1}x^{-1}$. However, we know that if $g \in G$, then $g^2 = 1$, which means that if we multiply both sides by g^{-1}, we get that $g = g^{-1}$ for all $g \in G$. This means that $xy = y^{-1}x^{-1} = yx$. Thus, G is abelian. □

Exercise 33. Let x be an element of finite order n in G

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

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

Proof. a) Suppose that $|x| = n$ and that $x^i = x^{-i}$ for some $i \in \{1, 2, \dots, n-1\}$. Multiplying both sides by x^i, we get that $x^i x^i = x^{-i}x^i$. This simplifies to $x^{2i} = x^{i-i} = 1$. By lemma 1, we see that $n \mid 2i$. Since n is odd, this means that $n \mid i$. However, $i < n$. Thus, there is no such i.

b) Let $|x| = n = 2k$ and $1 \leq i < n$. We see that if $i = k$, then $x^{2i} = x^{2k} = x^n = 1$. Thus, multiplying both sides by x^{-1}, we get that $x^i = x^{-i}$. Conversely, if $x^i = x^{-i}$, we see that $x^{2i} = 1$. By lemma 1, this means that $n = 2k \mid 2i$. Thus $k \mid i$. Since $0 < i < n = 2k$, this must mean that $i = k$.

□

Section 1.2

Exercise 4. 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 that z is the only nonidentity element of D_{2n}, which commutes with all elements of D_{2n}.

Proof. Since $r^k \neq 1$, this means that $\left|r^k\right| > 1$. We see that $\left(r^k\right)^2 = r^{2k} = r^n = 1$. Thus, $\left|r^k\right| = 2$. Since $\left(r^k\right)^2 = 1$, this also means that $r^k r^k = 1$, which, after multiplying both sides by r^{-k}, shows that $r^k = r^{-k}$.

Since we know that $s, r \in D_{2n}$ generate D_{2n}, then let $d = s^i r^j$ be an arbitrary element in D_{2n}. We see that $r^k d = r^k s^i r^j = s^i r^{-k} r^j = s^i r^{-kj} = s^i r^j r^{-k} = dr^{-k} = dr^k$, as $r^{-k} = r^k$. Thus, r^k commutes with any element of D_{2n}.

Say that $g = s^i r^j \in D_{2n}$ commutes with every element of D_{2n}. Since $s^2 = 1$, we see that $i = 0$ or $i = 1$.

If $i = 0$, then $g = s^0 r^j = r^j$. Since g must commute with every element in D_{2n}, then it must commute with s. Thus, $gs = sg$, which means $r^j s = sr^j = r^{-j} s$. Multiplying on the left by $s^{-1} r^j$, we get $s^{-1} r^j r^j s = 1$. This means that $s^{-1} r^{2j} s = s^{-1} s r^{-2j} = r^{-2j} = 1$. Multiplying by r^j, we get that $r^{-j} = r^j$. By Sec 1.1 Ex 33, this means that if $j > 0$, then $j = k$. Thus, either $j = 0$ or $j = k$. This means that $g = r^k$ and $g = r^0 = 1$ are the only such g's that commute with s. We assumed that $z \neq 1$, so $g = r^k$. We already proved that $g = r^k$ commutes with everything.

If $i = 1$, then $g = sr^j$. Since g must commute with every element in D_{2n}, then it must commute with r. Thus, $rg = gr$, which means that $rsr^j = sr^j r$. Since $sr^k = r^{-k} s$ for all k, we see that this means that $sr^{-1} r^j = sr^j r$. Canceling the s and grouping the r's, we get $r^{j-1} = r^{j+1}$. Multiplying both sides by r^{1-j}, we get that $r^{j+1+1-j} = r^2 = 1$. But since $n \geq 4$, tis means $|r| = n \geq 4$. This is contradiction and thus no such element g of this form commutes with everything in D_{2n}.

This proves that $z = r^k$ is the only nonidentity element that commutes with all elements of D_{2n}, where $n \geq 4$ and $n = 2k$. □

Exercise 5. If n is odd and $n \geq 3$, show that the identity is the only element of D_{2n} which commutes with all elements of D_{2n}.

Proof. The identity commutes with everything trivally so we must only prove that no other element of D_{2n} commutes with everything. Let $g = s^i r^j$ be an arbitrary element of D_{2n}, where $i \in \{0, 1\}$ and $j \in \{0, 1, \ldots, n-1\}$.

If $i = 0$, then $g = s^0 r^j = r^j$. Since g must commute with every element in D_{2n}, then it must commute with s. Thus, $gs = sg$, which means $r^j s = sr^j = r^{-j} s$. Multiplying on the left by $s^{-1} r^j$, we get $s^{-1} r^j r^j s = 1$. This means that $s^{-1} r^{2j} s = s^{-1} s r^{-2j} = r^{-2j} = 1$. Multiplying by r^j, we get that $r^{-j} = r^j$. However, by Sec 1.1 Ex 33, since $|r| = n$ and n is assumed to be odd, this equation fails for all $j > 1$. If $j = 0$, then $r^{-0} = 1 = r^0$, which is true. Thus, g must be the identity, which we know commutes with everything.

If $i = 1$, then $g = sr^j$. Since g must commute with every element in D_{2n}, then it must commute with r. Thus, $rg = gr$, which means that $rsr^j = sr^j r$. Since $sr^k = r^{-k} s$ for all k, we see that this means that $sr^{-1} r^j = sr^j r$. Canceling the s and grouping the r's, we get $r^{j-1} = r^{j+1}$. Multiplying both sides by r^{1-j}, we get that $r^{j+1+1-j} = r^2 = 1$. But since $n \geq 3$, tis means $|r| = n \geq 3$. This is contradiction and thus no such element g of this form commutes with everything in D_{2n}.

This proves that if n is odd and $n \geq 3$ that the identity is the only element of D_{2n} that commutes with everything. □

Exercise 8. Find the order of the cyclic subgroup of D_{2n} generated by r.

Proof. By the additional problem (A), we see that the order of a cyclic subgroup is equal to the order of the element that generated it. Thus, we only need to find the order of r. According to the standard presentation of D_{2n}, though, we know that the order of r is n. Thus, the order of the cyclic subgroup generated by r is n as well. □

Section 1.6

Exercise 8. Prove that if $n \neq m$, S_n and S_m are not isomorphic.

Proof. We know that $|S_n| = n!$ and that $|S_m| = m!$. We also know that an isomorphism is a homomorphism that's bijective. However, since $|S_n| \neq |S_m|$, we know that there is no bijection between them. Thus, S_n and S_m are not isomorphic. □

Exercise 16. Let A and B be groups and let G be their direct product, $A \times B$. Prove that the maps $\pi_1 : G \to A$ and $\pi_2 : G \to B$ defined by $\pi_1((a, b)) = a$ and $\pi_2((a, b)) = b$ are homomorphisms and find their kernels.

Proof. We see that $\pi_1((a, b)(c, d)) = \pi_1((ac, bd)) = ac = \pi_1((a, b))\pi_1((c, d))$, where $(a, b), (c, d) \in A \times B$. Thus, π_1 is a homomorphism. The kernel of this homomorphism is all the elements $g \in A \times B$, such that $\pi_1((a, b)) = 1_A$. Thus, $\pi_1((a, b)) = a = 1_A$. Thus, the kernel of this homomorphism is $\{(1_A, b) \mid b \in B\}$. The symmetrical argument can be applied to π_2. □

Exercise 20. Let G be a group and let $\mathrm{Aut}(G)$ be the set of all isomorphisms from G onto G. Prove that $\mathrm{Aut}(G)$ is a group under function composition.

Proof. Let φ, ψ be two isomorphisms from $G \to G$. We see that since φ and ψ are bijective, that $\varphi \circ \psi$ is a bijection. We also see that $(\varphi \circ \psi)(gh) = \varphi(\psi(gh)) = \varphi(\psi(g)\psi(h)) = \varphi(\psi(g))\varphi(\psi(h)) = (\varphi \circ \psi)(g)(\varphi \circ \psi)(h)$, as φ and ψ are homomorphisms. Thus, $\varphi \circ \psi$ is a homomorphism. This proves that the binary operation is well defined.

We've already proven that function composition is associative.

The identity function $\varphi : G \to G$, is obviously a bijection. Also, $\varphi(gh) = gh = \varphi(g)\varphi(h)$, so it's also a homomorphism. Thus, $\varphi \in \mathrm{Aut}(G)$.

Let φ be an isomorphism and let $g, h \in G$. Since φ is a bijection, then there exists φ^{-1}, and since φ is a surjection, there exists $u, v \in G$ such that $\varphi(u) = g$ and $\varphi(v) = h$. We see that $\varphi^{-1}(gh) = \varphi^{-1}(\varphi(u)\varphi(v)) = \varphi^{-1}(\varphi(uv)) = uv = \varphi^{-1}(g)\varphi^{-1}(h)$, as φ is a homomorphism. This proves that φ^{-1} is a homomorphism. Since φ is a bijection, than φ^{-1} is a bijection. Thus, $\varphi^{-1} \in \mathrm{Aut}(G)$. This proves closure under inverses. And thus $\mathrm{Aut}(G)$ is a group under function composition. □

Section 1.7

Exercise 2. Show that the additive group $\mathbb{Z}$ acts on itself by $z \cdot a = z + a$ for all $z, a \in \mathbb{Z}$.

Proof. We see that $0 \cdot a = 0 + a = a$. This satisfies the first axiom of a group action. We also see that $z_1 \cdot (z_2 \cdot a) = z_1 \cdot (z_2 + a) = z_1 + (z_2 + a) = (z_1 + z_2) + a = (z_1 + z_2) \cdot a$. This means that this operation satisfies the second axiom as well and is thus a group action. $\square$

Exercise 3. Show that the additive group $\mathbb{R}$ acts on the x, y plane $\mathbb{R} \times \mathbb{R}$ by $r \cdot (x, y) = (x + ry, y)$.

Proof. We see that $0 \cdot (x, y) = (x + 0y, y) = (x, y)$. This satisfies the first axiom of a group action. We also see that $r_1 \cdot (r_2 \cdot (x, y)) = r_1 \cdot (x + r_2 y, y) = ((x + r_2 y) + r_1 y, y) = (x + (r_1 + r_2) y, y) = (r_1 + r_2) \cdot (x, y)$. This means that this operation satisfies the second axiom as well and is thus a group action. $\square$

Exercise 5. Prove that the kernel of an action of the group G on the set A is the same as the kernel of the corresponding permutation representation $G \to S_A$.

Proof. Let A be a G-set. The kernel of the action is the set $H = \{g \in G \mid g.a = a, \forall a \in A\}$. The corresponding permutation is a group homomorphism $\varphi : G \to S_A$ given by $\varphi(g)(a) = g.a$. Let $h \in H$. Then for all $a \in A$, we see that $\varphi(h)(a) = h.a = a$. This means that $\varphi(h) = \mathrm{id}_A = 1$. Thus, $h \in \ker \varphi$. This shows that $H \subseteq \ker \varphi$. Let $k \in \ker \varphi$. This means for all $a \in A$, that $\varphi(k)(a) = \mathrm{id}_A(a) = a$. Thus, $\varphi(k)(a) = k.a = a$. This means that $k \in H$. This proves that $\ker \varphi \subseteq H$. Thus, $\ker \varphi = H$. $\square$

Exercise 8. 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 (12 3) act on the six 2-element subsets of $\{1, 2, 3, 4\}$.

Proof. a) Let σ be the identity permutation. Then $\sigma \cdot \{a_1, \ldots, a_k\} = \{\sigma(a_1), \ldots, \sigma(a_k)\} = \{a_1, \ldots, a_k\}$. This proves the first group action axiom. Now, let $\sigma, \rho \in S_A$. Then $\sigma \cdot (\rho \cdot \{a_1, \ldots, a_k\}) = \sigma \cdot \{\rho(a_1), \ldots, \rho(a_k)\} = \{\sigma(\rho(a_1)), \ldots, \sigma(\rho(a_k))\}$. Remember that the operation in S_A is function composition, thus this is equivalent to the set $\{(\sigma \circ \rho)(a_1), \ldots, (\sigma \circ \rho)(a_k)\} = (\sigma \circ \rho) \cdot \{a_1, \ldots, a_k\}$. This proves the second group action axiom. Thus, this is a group action.

b) We see that the six elements of B are $\{\{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}\}$. If we apply (12) to each element, we get $\{1, 2\}, \{2, 3\}, \{2, 4\}, \{1, 3\}, \{1, 4\}, \{3, 4\}$ respectively. If we apply (123) to each element, we get $\{2, 3\}, \{1, 2\}, \{2, 4\}, \{1, 3\}, \{3, 4\}, \{1, 4\}$ respectively.

$\square$

Exercise 13. Find the kernel of the left regular action.

Proof. Recall that the left regular action is the action from $G \times G \to G$, where $g.h = gh$. The kernel of this is the set $K = \{g \in G \mid g.h = gh = h\}$. After cancelling the h's, we see that this is the set $\{g \in G \mid g = 1\} = \{1_G\}$. Thus, the kernel is just the trival group. $\square$

Exercise 14. Let G be a group and let $A = G$. Show that if G is non-abelian then the maps defined by $g \cdot a = ag$ for all $g, a \in G$ do *not* satisfy the axioms of a (left) group action of G on itself.

Proof. Let $g, h \in G$. One of the axioms of a group action is that $h(g \cdot a) = (hg) \cdot a$. However, this means that $h(g \cdot a) = h \cdot ag = agh$, while $(hg) \cdot a = ahg$. This means that for this to be a group action it is necessary that $agh = ahg$, and after cancelling the a's, that $gh = hg$. This is not necessarily true for a non-abelian group. Thus, we cannot guarantee this axiom of a group action. $\square$

Additional Problems

Exercise A. Let G be a group and fix an element $x \in G$. Let $\langle x \rangle = \{e, x, x^2, x^3, \dots\} \subseteq G$. Prove that $\langle x \rangle$ is a subgroup of G. Prove that $|x| = |\langle x \rangle|$. That is, the order of the element x equals the order of the group $\langle x \rangle$.

Proof. By the definition of $\langle x \rangle$, we see that $e \in \langle x \rangle$. Thus, it's not empty. Now, let $g, h \in \langle x \rangle$. Then $g = x^k$ and $h = x^j$ for some $k, j \in \mathbb{Z}$. Thus, $gh^{-1} = \left(x^k\right)\left(x^j\right)^{-1} = x^k x^{-j} = x^{k-j} \in \langle x \rangle$. Thus, by the two step subgroup criteria that I proved in the last problem set, we see that $\langle x \rangle$ is a subgroup of G.

Let $|x| = n < \infty$. We see that x^k are distinct for $0 \leq k < n$. Otherwise, this would contradict the definition of order. However, we know that for $k \geq n$, then $k = qn + r$ for some $0 \leq r < n$, which means $x^k = x^{qn+r} = (x^n)^q x^r = x^r$. Thus, every element x^k where $k \geq n$ is equal to a number x^r where $0 \geq r < n$. Thus, there are only n distinct elements of the form x^k, which means $|\langle x \rangle| = n$. Thus, $|x| = |\langle x \rangle|$.

Let $|x| = \infty$. Say $x^k = x^j$ for some $j, k \in \mathbb{Z}$. Then this means $x^{k-j} = 1$. This is a contradiction, as $|x| = \infty$. Thus, x^k is distinct for all $k \in \mathbb{Z}$. This means that $|\langle x \rangle| = \infty$. Thus, $|x| = |\langle x \rangle|$.

$\square$

Exercise B. 1) Prove that $x \in [x]$

2) Let I be an index set and let $\{E_i \mid i \in I\}$ be a collection of subsets of X which satisfy the following two axioms:

   i) $X = \cup_{i \in I} E_i$

   ii) If $E_i \cap E_j \neq \varnothing$, then $E_i = E_j$

   Such a collection of subsets of a set X is called a partition of the set X. Prove that for any equivalence relation on the set X, the collection of equivalence classes provides a partition of X.

3) Let $\{E_i \mid i \in I\}$ be a partition of X. Given elements $x, y \in X$, we have that $x \in E_i$ and $y \in E_j$ for some $i, j \in I$. We declare $x \sim y$ to hold if and only if $i = j$. Prove that this rule for $\sim$ is well-defined. Also prove that $\sim$ is an equivalence relation on X and that the partitioning sets are precisly the equivalence classes of this equivalence relation.

Proof. 1) We know that $[x] = \{y \in X \mid y \sim x\}$. Since $\sim$ is an equivalence relation, it's reflexive. Thus $x \sim x$. This shows that $x \in [x]$.

2) Let E_x be the set $\{y \in X \mid x \sim y\} \subseteq X$. We see that $X = \cup_{x \in X} E_x$, as $x \in E_x$ for all $x \in X$. Suppose $E_x \cap E_q \neq \varnothing$. Then let $w \in E_x \cap E_y$. This means $w \in E_x$, so $w \sim x$. Also, $w \in E_y$, so $w \sim y$. Thus, $x \sim y$. This means that if $w \in E_x$, then $w \sim x \sim y$, which means $w \in E_y$. Thus $E_x \subseteq E_y$. By similar argument, $E_y \subseteq E_x$. Thus, $E_x = E_y$. This proves that the equivalence classes form a partition.

3) Since $x, y \in X = \cup_{i \in I} E_i$, we know that x, y have to each be in at least one partitioning set. Suppose $x \in E_i$ and $x \in E_j$. This means that $x \in E_i \cap E_j$. As $\{E_i\}$ form a partition, this means that $i = j$. Thus, each $x \in X$ belong to exactly one such set E_i. This proves that $\sim$ is well-defined.

Let $x \in X$. This means that $x \in E_i$ for some $i \in I$. Since $x \in E_i$ and itself is in E_i, this means that $x \sim x$. Suppose $x \sim y$. This means that $y \in E_i$. Since $i = i$, this means that $y \sim x$. Let $x \sim y$ and $y \sim w$. Since $x \sim y$, this means $y \in E_i$. Since $y \sim w$, this means $w \in E_i$. Thus, since $x, w \in E_i$, we see that $x \sim w$. This proves that $\sim$ is an equivalence relation. If we look at $[x]$, we see that this is the set $\{y \in X \mid y \in E_i\}$, which means $[x] = \{y \in X \mid y \in E_i\} = E_i$.

□

Exercise C. 1) Let G be a group and let X be a G-set. Given $g \in G$ define a function $f_g : X \to X$ be the rule $f_g(x) = g.x$. Prove that f_g is bijective and hence we can define a function $\varphi : G \to \operatorname{Perm}(X)$ by $\varphi(g) = f_g$.

2) Prove that φ is a group homomorphism.

3) We now consider the converse to part (1) and part (2). Let a set X and a group homomorphism $\psi : G \to S_X$ be given. For $g \in G$ and $x \in X$, define $g * x = \psi(g)(x)$. Prove that this rule makes X into a G-set with $*$ as its operation.

4) Prove the two constructions given above are each other's inverse. That is, if X is a G-set with operation ., then you can construction the group homomorphism φ, and in turn, use this homomorphism to construction a G-set action $*$. Prove that $g.x = g * x$ for all $g \in G$ and all $x \in X$. Similarily, if ψ is a group homomorphism, then you can construct a G-set structure on X and, in turn, use this to define a group homomorphism $\varphi : G \to \operatorname{Perm}(X)$. Show that $\psi = \varphi$. This proves that there's a bijection between the collection of all possible G-set structures on X and the collection of all group homomorphisms $G \to \operatorname{Perm}(X)$.

Proof. 1) Consider $f_{g^{-1}}$. We see that $f_{g^{-1}}(f_g(x)) = g^{-1}.(g.x) = (g^{-1}g).x = x$. We see that the same argument applies for $f_g(f_{g^{-1}}(x))$. Thus, f_g and $f_{g^{-1}}$ are inverses. This proves that f_g is a bijection and is thus a permutation of X.

2) We see that $f_{gh}(x) = gh.x = g.h.x = g.f_h(x) = f_g(f_h(x)) = (f_g \circ f_h)(x)$. Thus, $f_{gh} = f_g \circ f_h$. This means that $\varphi(gh) = f_{gh} = f_g \circ f_h = \varphi(g) \circ \varphi(h)$. This proves that φ is a homomorphism.

3) We see that $e * x = \psi(e)(x) = \mathrm{id}_X(x) = x$, as $\psi(e)$ must map to the identity of S_x since ψ is a homomorphism. This proves the first axiom of a group action. We see that $g * (h * x) = g * \psi(h)(x) = \psi(g)(\psi(h)(g)) = (\psi(g) \circ \psi(h))(x) = \psi(gh)(x) = (gh) * x$, as ψ is a homomorphism. This proves the second axiom of a group action. Thus, $*$ is a group action.

4) Let X be a G-set with operation .. By (1) and (2), we can construct a homomorphism $\varphi : G \to S_X$ by $\varphi(g) = f_g$, where $f_g(x) = g.x$. By (3), this homomorphism φ can be made into a group action $*$, where $g * x = \varphi(g)(x)$. Let $x \in X$ and $g \in G$. We see that $g.x = f_g(x) = \varphi(g)(x) = g * x$.

   Let $\psi : G \to S_X$ be a group homomorphism. Then by (3), we can construct a group action by defining $g * x = \psi(g)(x)$. By (1) and (2), we can construct a homomorphism from this group action by defining $\varphi(g)(x) = f_g(x) = g * x$. We see that for all $x \in X$ and $g \in G$, that $\psi(g)(x) = g * x = f_g(x) = \varphi(g)(x)$. Thus, $\psi = \varphi$. This proves that the processes of part (1,2) and part (3) are inverses of each other.

$\square$