Math 620: §3.3 Constructing Examples

Due on Monday, October 19, 2015

Boynton 10:00

Kailee Gray

Exercise 3.3.6: Construct an abelian group of order 12 that is not cyclic.

Let G be the group we want to construct. If G is not cyclic, then there is no element in G with order 12. Since the order of the elements of G have to divide the order of G, the order of the elements of G must be $1, 2, 3, 4$, or 6. Note $|\mathbb{Z}_2 \times \mathbb{Z}_6| = 12$ and by commutativity of addition in $\mathbb{Z}$, $\mathbb{Z}_2 \times \mathbb{Z}_6$ is abelian. Note there is no element in $\mathbb{Z}_2 \times \mathbb{Z}_6$ has order 12 so $\mathbb{Z}_2 \times \mathbb{Z}_6$ is not cyclic:

$+$	$(0,0)$	$(0,1)$	$(0,2)$	$(0,3)$	$(0,4)$	$(0,5)$	$(1,0)$	$(1,1)$	$(1,2)$	$(1,3)$	$(1,4)$	$(1,5)$
order	1	6	3	2	3	6	2	6	6	2	6	6

Exercise 3.3.7: Construct a group of order 12 that is not abelian.

Consider S_4. Note $|S_4| = 24$ and S_4 is not abelian because $(12)(34)(123) = (243)$ and $(123)(12)(34) = (134)$. Let A_4 be the set of all permutations in S_4 that can be written as a product of an even number of transpositions. Then, $A_4 \subset S_4$ and $A_4 = \{(1)(1), (12)(34), (13)(24), (14)(23), (123), (124), (132), (134), (142), (143), (234), (243)\}$ and so $|A_4| = 12$. Consider $\sigma, \tau \in A_4$. Then, σ can be written as the product of even number of transpositions and τ can be written as the product of even number of transpositions. So $\sigma\tau$ can be written as the product of even number of transpositions which implies $\sigma\tau \in A_4$. Thus, by corollary 3.2.4, A_4 is a subgroup of S_4 so A_4 is a group. Also, $(12)(34)(123) = (243)$ and $(123)(12)(34) = (134)$ with $(12)(34), (123) \in A_4$ so A_4 is not abelian.

Exercise 3.3.9: Concerning subgroups of $\mathbb{Z} \times \mathbb{Z}$. (a) Let $C_1 = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a = b\}$. Show that C_1 is a subgroup of $\mathbb{Z} \times \mathbb{Z}$.

Proof. Since $(0,0) \in C_1$, C_1 is nonempty; note $(0,0)$ is the identity element of C_1 since $(a,b) + (0,0) = (a,b)$ for any $a, b \in \mathbb{Z}$. Also, $C_1 \subseteq \mathbb{Z} \times \mathbb{Z}$. Suppose $(a_1, a_2), (b_1, b_2) \in C_1$. Then, $a_1 = a_2$ and $b_1 = b_2$. Because $(b_1, b_2) + (-b_1, -b_2) = (0,0)$, $(b_1, b_2)^{-1} = (-b_1, -b_2)$. If $b_1 = b_2$, $-b_1 = -b_2$ so $(b_1, b_2)^{-1} \in C_1$. Also, $(a_1, a_2) + (-b_1, -b_2) = (a_1 - b_1, a_2 - b_2)$. Since $a_1 = a_2$ and $-b_1 = -b_2$, $a_1 - b_1 = a_2 - b_2$. Thus, $(a_1, a_2) + (b_1, b_2)^{-1} \in C_1$. By corollary 3.2.3, C_1 is a subgroup of $\mathbb{Z} \times \mathbb{Z}$. □

(b) For each positive integer $n \geq 2$, let $C_n = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a \equiv b \pmod{n}\}$. Show that C_n is a subgroup of $\mathbb{Z} \times \mathbb{Z}$.

Proof. Since $0 \equiv 0 \pmod{n}$ for any n, $(0, 0) \in C_n$, C_n is nonempty. Also, $C_n \subseteq \mathbb{Z} \times \mathbb{Z}$. Consider any $(a_1, a_2), (b_1, b_2) \in C_n$. Then, $a_1 \equiv a_2 \pmod{n}$ and $b_1 \equiv b_2 \pmod{n}$. Therefore, $a_1 + b_1 \equiv a_2 + b_2 \pmod{n}$ so $(a_1, a_2) + (b_1, b_2) \in C_n$. Because $(b_1, b_2) + (-b_1, -b_2) = (0, 0)$, $(b_1, b_2)^{-1} = (-b_1, -b_2)$. If $b_1 \equiv b_2 \pmod{n}$, $-b_1 \equiv -b_2 \pmod{n}$ so $(b_1, b_2)^{-1} \in C_n$. By proposition 3.2.2, C_n is a subgroup of $\mathbb{Z} \times \mathbb{Z}$. □

(c) Show that every subgroup of $\mathbb{Z} \times \mathbb{Z}$ that contains C_1 has the form C_n, for some positive integer n.

Proof. Suppose H is a subgroup of $\mathbb{Z} \times \mathbb{Z}$ such that $C_1 \subseteq H$. If for all $(a, b) \in H$, $a = b$, then $a \equiv b \pmod{1}$ so $H = C_1$ and H is in the form C_n.
Suppose there exist $(a, b) \in H$ such that $a \neq b$. Since H is a group, it must be closed under addition and have inverses, so $(-a, -a), (-b, -b) \in H$ and $(a, b) + (-a, -a) = (0, b - a) \in H$. Thus, elements of the form $(0, n) \in H$. If $n < 0$, elements in H have inverses so $(0, -n) \in H$. Since $(a, b), a \neq b$ there exists one such n, so by the Well-Ordering Principle, we can let $n = |n|$ be the smallest positive integer such that $(0, n)$ or $(0, -n)$ is in H.
We will show $H = C_n$. First, we will show $H \subseteq C_n$. Let $(a, b) \in H$. We want to show that $(a, b) \in C_n$ which is equivalent to showing $a \equiv b \pmod{n}$. From above, we know $(a, b) \in H$ implies $(0, b - a) \in H$. By the division algorithm there exists $0 \leq r < n$ and $q \in \mathbb{Z}$ such that $b - a = qn + r$. We want to show $r = 0$. Notice $(0, b - a) = (0, qn) + (0, r)$ and $(0, r) = (0, b - a) - (0, qn)$. Since $(0, b - a), (0, n) \in H$, $(0, qn) \in H$ and therefore $(0, r) \in H$. Thus, we have $r < n$ such that $(0, r) \in H$. But, n was selected as the least possible positive integer with $(0, n) \in H$ so $(0, r) = (0, 0)$ and so $r = 0$. Since $r = 0$, $b - a = nq$ which implies $a \equiv b \pmod{n}$ and so $(a, b) \in C_n$.
Next, show $C_n \subseteq H$. Let $(a, b) \in C_n$. Then, $a \equiv b \pmod{n}$ implies $b - a = nk$ and so $b = a + nk$ for some integer k. Since $C_1 \subset H$, we know $(a, a) \in H$. Also, from above, we know $(0, n) \in H$. Thus, $(a, b) = (a, a) + k(0, n)$. H is closed under addition so $k(0, n) \in H$ and so $(a, b) \in H$. Thus, $C_n = H$. □

Exercise 3.3.10: Let $n > 2$ be an integer, and let $X \subseteq S_n \times S_n$ be the set $X = \{(\sigma, \tau) \mid \sigma(1) = \tau(1)\}$. Show that X is not a subgroup of $S_n \times S_n$.

Proof. Consider $X \subseteq S_3 \times S_3$. Then, $(\sigma_1, \tau_1) = ((12), (123))$ and $(\sigma_2, \tau_2) = ((13), (132))$ are in X since $\sigma_1(1) = 2 = \tau_1(1)$ and $\sigma_2(1) = 3 = \tau_2(1)$. If X is a subgroup of $S_3 \times S_3$, $(\sigma_1, \tau_1) \circ (\sigma_2, \tau_2) \in X$. Notice $(\sigma_1, \tau_1) \circ (\sigma_2, \tau_2) = ((12)(13), (123)(132)) = ((132), (1))$. Let, $\sigma = (132)$ and $\tau = (1)$. Notice $\sigma(1) = 3$ but $\tau(1) = 1$. Thus, $((132), (1)) \notin X$. Since X is not closed, X is not a subgroup of $S_3 \times S_3$ □

Exercise 3.3.13: Let p, q be distinct prime numbers, and $n = pq$. Show $HK = \mathbb{Z}_n^\times$.

Proof. Let p, q be distinct prime numbers, and let $n = pq$ and consider the subgroups $H = \{[x] \in \mathbb{Z}_n^\times \mid x \equiv 1 \pmod{p}\}$ and $K = \{[y] \in \mathbb{Z}_n^\times \mid y \equiv 1 \pmod{q}\}$ of $\mathbb{Z}_n^\times$. By proposition 3.3.2, since $\mathbb{Z}_n^\times$ is abelian, HK is a subgroup of $\mathbb{Z}_n^\times$
From page 41 of Beachy, $|\mathbb{Z}_n^\times| = \varphi(n) = \varphi(pq) = (p-1)(q-1)$. We will show $|HK| = (p-1)(q-1)$.
Since $n = pq$, all elements $h, k \in H, K \subseteq \mathbb{Z}_n^\times$ must satisfy $1 \leq h, k \leq pq - 1$. Also, $h \in H \subseteq \mathbb{Z}_n^\times$ implies $h = 1 + mp$ and $k \in K \subseteq \mathbb{Z}_n^\times$ implies $k = 1 + nq$ with $m, n \in \mathbb{Z}_n$. Since $1 \leq h, k \leq pq - 1$, $0 \leq m < q$ and $0 \leq n < p$. Thus, H contains at most $1, 1 + p, 1 + 2p, \ldots, 1 + (q-1)p$ and K contains at most $1, 1 + q, 1 + 2q, \ldots, 1 + (p-1)q$. We need to check to ensure these elements are in $\mathbb{Z}_n^\times$. Notice if $x \in H$, $x \equiv 1 \pmod{p}$. If $x \notin \mathbb{Z}_n^\times$, x is not relatively prime to n. Since $x \equiv 1 \pmod{p}$ and p, q are the only divisors of n, $x \in 1, 1 + p, 1 + 2p, \ldots, 1 + (q-1)p$ but $x \notin \mathbb{Z}_n^\times$ implies $q \mid x$ so $x \equiv 0 \pmod{q}$. Since $\gcd(p, q) = 1$, the Chinese Remainder Theorem implies there exists a unique $x \bmod pq$ with $x \equiv 0 \pmod{q}$ and $x \equiv 1 \pmod{p}$. Thus, there is exactly one element in $1, 1 + p, 1 + 2p, \ldots, 1 + (q-1)p$ that is not in $H \subseteq \mathbb{Z}_n^\times$. Since $1, 1 + p, 1 + 2p, \ldots, 1 + (q-1)p$ contains q elements, $|H| = q - 1$.
Similarly, if $x \in K$, $x \equiv 1 \pmod{q}$. If $1 \leq x \leq n - 1$ and $x \notin \mathbb{Z}_n^\times$, x is not relatively prime to n. Since $x \equiv 1 \pmod{q}$ and p, q are the only divisors of n, $x \in 1, 1 + q, 1 + 2q, \ldots, 1 + (p-1)q$ but $x \notin \mathbb{Z}_n^\times$ implies $p \mid x$ so $x \equiv 0 \pmod{p}$. Since

$\gcd(p,q) = 1$, the Chinese Remainder Theorem implies there exists a unique $x \bmod pq$ with $x \equiv 0 \pmod{p}$ and $x \equiv 1 \pmod{q}$. Thus, there is exactly one element in $1, 1+q, 1+2q, \ldots, 1+(p-1)q$ that is not in $\mathbb{Z}_n^\times$. Since $1, 1+q, 1+2q, \ldots, 1+(p-1)q$ contains p elements, $|K| = p-1$.

Next, consider $H \cap K$. If $x \in H \cap K$, then $x \equiv 1 \pmod{p}$ and $x \equiv 1 \pmod{q}$. Since $\gcd(p,q) = 1$ the Chinese Remainder Theorem implies there exists a unique $x \bmod pq$ such that $x \equiv 1 \pmod{p}$ and $x \equiv 1 \pmod{q}$. Thus, $|H \cap K| = 1$.

Thus, by exercise 3.3.14,

$|HK| = \frac{|H||K|}{|H \cap K|} = \frac{(q-1)(p-1)}{1} = (p-1)(q-1) = \varphi(pq) = \varphi(n) = |\mathbb{Z}_n^\times|$. So HK and $\mathbb{Z}_n^\times$ are finite groups of the same cardinality with $HK \leq \mathbb{Z}_n^\times$ implies $HK = \mathbb{Z}_n^\times$. □

Exercise 3.3.15: Let G be a group of order 6. Show that G must contain an element of order 2. Show that it cannot be true that every element different from e has order 2.

Proof. Let G be a group of order 6. Then, G is a finite group with an even number of elements, so by exercise 24 in §3.1, there must exist an element $a \in G$ such that $a^2 = e$ with $a \neq e$. Thus, $o(a) = 2$ and so G must have at least one element of order 2.

Suppose all elements in G have order 2. Let $a, b \in G$. Then, since all elements of G have order 2, $a^2 = e, b^2 = e$. Then, $\langle a \rangle = \{e, a\}$ and $\langle b \rangle = \{e, b\}$. By proposition 3.2.6(a), $\langle a \rangle$ and $\langle b \rangle$ are subgroups of G. Consider the product of these cyclic groups: HK where $H = \langle a \rangle, K = \langle b \rangle$. Then, $HK \neq \emptyset$ since HK contains at least $\{e, a, b, ab\}$. Consider any $h \in \langle a \rangle$ and $k \in \langle b \rangle$. Then, $h = e$ or a and $k = e$ or b, so we consider the following cases:

If $h = e, k = e, h^{-1} = e$ then $h^{-1}kh = eee = e \in K$. If $h = e$ and $k = b$ then $h^{-1}kh = ebe = b \in K$. Suppose $k = e$ and $h = a$. Because a has order 2, $a^{-1} = a$. Thus, $h^{-1}kh = aea = aa = e \in K$.

Suppose $h = a$ and $k = b$. Then, $h^{-1}kh = aba$. Since G is a group and $a, b \in G$, so $ab \in G$. Then, from our assumption above ab has order 2. So $(ab)(ab) = e$. $b^{-1} = b$, so $(ab)(ab) = abab = e$ and $ababb = eb$. Hence, $aba = b \in K$.

Since $h^{-1}kh \in K$ for all $h \in \langle a \rangle$ and $k \in \langle b \rangle$, HK is a subgroup of G. Notice $|H| = 2$, $|K| = 2$ and $H \cap K = \{e\}$, so $|H \cap K| = 1$. By exercise 14 in §3.3,

$$|HK| = \frac{|H||K|}{|H \cap K|} = \frac{2 \cdot 2}{1} = 4$$

However, 4 does not divide 6, the order of G. But, by Lagrange's Theorem, the order of any subgroup of G must divide 6. Hence, no such HK exists and so it is not the case that all elements of G have order 2. □

Exercise 3.3.16: Let G be a group of order 6, and suppose that $a, b \in G$ with a of order 3 and b of order 2. Show that either G is cyclic or $ab \neq ba$.

Proof. Let G be a group of order 6, and suppose that $a, b \in G$ with a of order 3 and b of order 2. Assume that $ba = ab$. By exercise 25 in §3.2, since $\gcd(o(a), o(b)) = 1$ and $ba = ab$, $o(ab) = o(a)o(b)$ so $o(ab) = 2 \cdot 3 = 6$. Thus, G contains an element of order 6 which implies G is cyclic. We have proved the statement "Let G be a group of order 6, if $a, b \in G$ with a of order 3 and b of order 2 and $ab = ba$, then G is cyclic." Note this is logically equivalent to the desired statement. □

Exercise 3.3.17: Let G be any group of order 6. Show that if G is not cyclic, then its multiplication table must look like that of S_3.

Proof. Let G be any group of order 6. Assume that G is not cyclic. By proposition 3.2.11, the order of any element in G must divide 6. So the order of any element in G must be 1, 2, 3, 6. Since G is not cyclic, no element in G has order 6. Thus, elements of G must have order 1, 2, or 3. Also, by exercise 3.3.15, G must contain an element of order 2. Let $b \in G$ have order 2. Also by exercise 3.3.15, there must be an element of G, other than e, that does not have order 2. Therefore there must be an element $a \in G$ that has order 3. Since G is a non-cyclic group of order 6 with $o(a) = 3, o(b) = 2$, exercise 3.3.16 implies $ab \neq ba$.

element(s) in G	justification
e, b, a, a^2	order of b is 2, order of a is 3 and G is a group
ab, ba, a^2b, ba^2	because G is closed and $ab \neq ba$

Notice we've listed 8 elements of G. But G has 6 elements, so there must be two pairs of elements that are equivalent. Since $o(a) = 3, o(b) = 2$, and $b \neq a$, so the elements e, a, a^2, b must be distinct. Notice $ab \neq ba$, so we will test the following equivalencies:

$=$	ab, ba
e	If $ab = e, ab^2 = b$ implies $a = b$, but $o(a) \neq o(b)$. Thus, $ab \neq e$. Similarly, $ba \neq e$.
a	If $ab = a$, cancellation implies $b = e$, but $o(b) \neq 1$. Thus, $ab \neq a$. Similarly, $ba \neq a$.
b	If $ab = b$, cancellation implies $a = e$, but $o(a) \neq 1$. Thus, $ab \neq b$. Similarly, $ba \neq b$.
a^2	If $ab = a^2$, cancellation implies $b = a$, but $o(a) \neq o(b)$. Thus, $ab \neq a^2$. Similarly, $ba \neq a^2$.
a^2b	If $ab = a^2b$, cancellation implies $a = a^2$, but $o(a) \neq 1$. Thus, $ab \neq a^2b$.
ba^2	If $ba = ba^2$, cancellation implies $a = a^2$, but $o(a) \neq 1$. Thus, $ba \neq ba^2$.

Thus, $ab = ba^2$ and $ba = a^2b$ so we can conclude $G = \{e, a, a^2, b, ab, a^2b\}$. Additionally, if $ba = a^2b$ then $aba = a^3b = b$ and $bab = a^2b^2$ implies $bab = a^2$. Using these equalities and the associative property of G, we can simplify the following products: $a^2ba = a(aba) = ab$, $a^2ba^2 = a(aba)a = a(b)a = b$, $aba^2 = (aba)a = ba = a^2b$, $aba^2 = (aba)a = ba$, $(aba)b = bb = e$, $a^2bab = a^2(bab) = a^2a^2 = a$, $a^2a^2b = a(a^3)b = ab$, $ba^2b = (ba^2)b = abb = a$, $a^2ba^2b = a^2(ba^2b) = a^2a = e$, $aba^2b = a(ba^2b) = aa = a^2$ and $a^2ba^2b = a^2(ba^2b) = a^2a = e$. Now, we can construct the multiplication table of G:

	e	a	a^2	b	ab	a^2b
e	e	a	a^2	b	ab	a^2b
a	a	a^2	e	ab	a^2	$a^3b = b$
a^2	a^2	e	a	a^2b	$a^2ab = b$	$a^2a^2b = ab$
b	b	$ba = a^2b$	$ba^2 = ab$	e	$bab = a^2$	$ba^2b = a$
ab	ab	$aba = b$	$aba^2 = a^2b$	a	$abab = e$	$aba^2b = a^2$
a^2b	a^2b	$a^2ba = ab$	$a^2ba^2 = b$	$a^2b^2 = a^2$	$a^2bab = a$	e

Notice this multiplication table looks like the multiplication table of S_3 listed on page 116 of Beachy. Thus, if G is not cyclic and has order 6, G has a multiplication that looks like the multiplication table of S_3.

□