Dummit & Foote Ch. 2.3: Cyclic Groups and Cyclic Subgroups

Scott Donaldson

Jun. 2023

1. (6/18/23)

Find all subgroups of $Z_{45} = \langle x \rangle$, giving a generator for each. Describe the containments between these subgroups.

Proof. The subgroups of $Z_{45} = \langle x \rangle$ are those cyclic groups generated by x^n, where n divides 45. These are:

- $\langle 1 \rangle = \{1\}$, the trivial subgroup
- $\langle x^{15} \rangle = \{1, x^{15}, x^{30}\} \cong \mathbb{Z}/3\mathbb{Z}$
- $\langle x^9 \rangle = \{1, x^9, x^{18}, x^{27}, x^{36}\} \cong \mathbb{Z}/5\mathbb{Z}$
- $\langle x^5 \rangle = \{1, x^5, x^{10}, x^{15}, x^{20}, x^{25}, x^{30}, x^{35}, x^{40}\} \cong \mathbb{Z}/9\mathbb{Z}$
- $\langle x^3 \rangle = \{1, x^3, x^6, ..., x^{39}, x^{42}\} \cong \mathbb{Z}/15\mathbb{Z}$
- $\langle x \rangle = Z_{45}$ itself

Among these subgroups, we have $\langle 1 \rangle$ contained within every other subgroup, as well as $\langle x^{15} \rangle \leq \langle x^5 \rangle$, $\langle x^{15} \rangle \leq \langle x^3 \rangle$, and $\langle x^9 \rangle \leq \langle x^3 \rangle$. $\square$

2. (6/19/23)

If x is an element of the finite group G and $|x| = |G|$, prove that $G = \langle x \rangle$. Give an explicit example to show that this result need not be true if G is an infinite group.

Proof. Let $|x| = |G| = n < \infty$. By definition, G is closed, so it contains all powers of $x : 1, x, x^2, ..., x^{n-1}$. These are exactly n elements, so G contains no other elements. It is therefore generated by x, that is, $G = \langle x \rangle$.

However, if G is an infinite group and $x \in G$ with $|x| = \infty$, then this is not necessarily the case. For example, if $G = \mathbb{Z}$ and $x = 2$, then x generates all even integers in $\mathbb{Z}$, but does not generate the element 5. $\square$

3. (6/19/23)

Find all generators for $\mathbb{Z}/48\mathbb{Z}$.

Proof. From Proposition 6., the generators for $\mathbb{Z}/48\mathbb{Z}$ are those positive integers $n < 48$ for which n is relatively prime to 48. These are: 1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, and 47. □

4. (6/19/23)

Find all generators for $\mathbb{Z}/202\mathbb{Z}$.

Proof. As above, the generators for $\mathbb{Z}/202\mathbb{Z}$ are those positive integers $n < 202$ for which n is relatively prime to 202. The integer 202 only has two divisors greater than 1, namely 2 and 101. Therefore the generators of $\mathbb{Z}/202\mathbb{Z}$ are every odd positive integer less than 202 except for 101. □

5. (6/19/23)

Find the number of generators for $\mathbb{Z}/49000\mathbb{Z}$.

Proof. We are concerned with the number of integers n between 0 and 48999 for which n is relatively prime to 49000. It will be helpful to write 49000 uniquely as the product of primes: $2^3 \cdot 5^3 \cdot 7^2$.

Let us first consider the generators for $\mathbb{Z}/49000\mathbb{Z}$ between 0 and 69, that is, all the numbers that are relatively prime to 49000 between 0 and 69: 1, 3, 9, 11, 13, 17, 19, 23, 27, 29, 31, 33, 37, 39, 41, 43, 47, 51, 53, 57, 59, 61, 67, and 69. There are 24 such generators.

Next, we show that, for any $n \in \{0, ..., 48999\}$, the greatest common divisor of n and 49000 is equal to the greatest common divisor of n mod 70 and 49000. This is because 70 is equal to the product of the bases of the prime factors of 49000: $70 = 2 \cdot 5 \cdot 7$. So for any n, we have $n = m + 70k = m + (2 \cdot 5 \cdot 7)k$, where $m \in \{0, ..., 69\}$ and $k \geq 0$. Suppose that m is *not* in the list of the above generators (that is, that the greatest common divisor of m and 49000 is greater than 1). Then either 2, 5, or 7 divides m (otherwise m would be relatively prime to 49000). Without loss of generality, suppose that 2 divides m, and write $m = 2p$. We can then rewrite n as:

$$n = m + (2 \cdot 5 \cdot 7)k = 2p + (2 \cdot 5 \cdot 7)k = 2\big(p + (5 \cdot 7)k\big),$$

that is, 2 divides n, so it is not relatively prime to 49000 (similarly, if 5 or 7 divide m, then 5 or 7 also divide n, respectively). It follows that the generators for $\mathbb{Z}/49000\mathbb{Z}$ between 0 and 69 repeat (mod 70) over the rest of 49000. Since $49000/70 = 700$, there are thus $700 \cdot 24 = 16800$ generators for $\mathbb{Z}/49000\mathbb{Z}$. □

6. (6/20/23)

In $\mathbb{Z}/48\mathbb{Z}$ write out all elements of $\langle \overline{a} \rangle$ for every $\overline{a}$. Find all inclusions between subgroups in $\mathbb{Z}/48\mathbb{Z}$.

- Subgroup of order 48: $\langle \overline{1} \rangle = \langle \overline{5} \rangle = \langle \overline{7} \rangle = \langle \overline{11} \rangle = \langle \overline{13} \rangle = \langle \overline{17} \rangle = \langle \overline{19} \rangle = \langle \overline{23} \rangle = \langle \overline{25} \rangle = \langle \overline{29} \rangle = \langle \overline{31} \rangle = \langle \overline{35} \rangle = \langle \overline{37} \rangle = \langle \overline{41} \rangle = \langle \overline{43} \rangle = \langle \overline{47} \rangle$.
- Subgroup of order 24: $\langle \overline{2} \rangle = \langle \overline{10} \rangle = \langle \overline{14} \rangle = \langle \overline{22} \rangle = \langle \overline{26} \rangle = \langle \overline{34} \rangle = \langle \overline{38} \rangle = \langle \overline{46} \rangle$.
- Subgroup of order 16: $\langle \overline{3} \rangle = \langle \overline{9} \rangle = \langle \overline{15} \rangle = \langle \overline{21} \rangle = \langle \overline{27} \rangle = \langle \overline{33} \rangle = \langle \overline{39} \rangle = \langle \overline{45} \rangle$.
- Subgroup of order 12: $\langle \overline{4} \rangle = \langle \overline{20} \rangle = \langle \overline{28} \rangle = \langle \overline{44} \rangle$.
- Subgroup of order 8: $\langle \overline{6} \rangle = \langle \overline{18} \rangle = \langle \overline{30} \rangle = \langle \overline{42} \rangle$.
- Subgroup of order 6: $\langle \overline{8} \rangle = \langle \overline{40} \rangle$.
- Subgroup of order 4: $\langle \overline{12} \rangle = \langle \overline{36} \rangle$.
- Subgroup of order 3: $\langle \overline{16} \rangle = \langle \overline{32} \rangle$.
- Subgroup of order 2: $\langle \overline{24} \rangle$.
- Subgroup of order 1, the trivial subgroup: $\{0\}$.

Among these subgroups, all contain the trivial subgroup. The subgroups of order 2 and 3 are distinct, but both are contained in the subgroup of order 6. The subgroup of order 2 is also contained in the subgroup of order 4. The subgroups of order 4 and 6 are both contained in the subgroup of order 12. The subgroup of order 4 is also contained in the subgroup of order 8. The subgroups of order 8 and 12 are both contained in the subgroup of order 24. The subgroup of order 8 is also contained in the subgroup of order 16.

7. (6/22/23)

Let $Z_{48} = \langle x \rangle$ and use the isomorphism $\mathbb{Z}/48\mathbb{Z} \cong Z_{48}$ given by $\overline{1} \mapsto x$ to list all subgroups of Z_{48} as computed in the preceding exercise.

- Subgroup of order 48: $\{1, x, x^2, ..., x^{47}\}$.
- Subgroup of order 24: $\{1, x^2, x^4, ..., x^{46}\}$.
- Subgroup of order 16: $\{1, x^3, x^6, ..., x^{45}\}$.
- Subgroup of order 12: $\{1, x^4, x^8, ..., x^{44}\}$.
- Subgroup of order 8: $\{1, x^6, x^{12}, x^{18}, x^{24}, x^{30}, x^{36}, x^{42}\}$.
- Subgroup of order 6: $\{1, x^8, x^{16}, x^{24}, x^{32}, x^{40}\}$.
- Subgroup of order 4: $\{1, x^{12}, x^{24}, x^{36}\}$.
- Subgroup of order 3: $\{1, x^{16}, x^{32}\}$.
- Subgroup of order 2: $\{1, x^{24}\}$.
- Subgroup of order 1, the trivial subgroup: $\{1\}$.

8. (6/23/23)

Let $Z_{48} = \langle x \rangle$. For which integers a does the map φ_a defined by $\varphi_a : \overline{1} \mapsto x^a$ extend to an *isomorphism* from $\mathbb{Z}/48\mathbb{Z}$ onto Z_{48}?

Proof. We will show that φ_a is an isomorphism from $\mathbb{Z}/48\mathbb{Z}$ onto Z_{48} if and only if $a \in \mathbb{Z}$ is relatively prime to 48.

First, let $m, n \in \mathbb{Z}/48\mathbb{Z}$. Then $\varphi_a(m)\varphi_a(n) = (x^a)^m(x^a)^n = (x^a)^{m+n} = \varphi_a(m+n)$. So φ_a is a homomorphism.

Next, φ_a is one-to-one. Let $\varphi_a(n) = \varphi_a(m)$ for $m, n \in \mathbb{Z}/48\mathbb{Z}$. Then $(x^a)^m = (x^a)^n \Rightarrow x^{am} = x^{an}$, and so $am = an \pmod{48}$. Since a is relatively prime to 48, we must therefore have $m = n$, and it follows that φ_a is injective. (Note, however, that if $k > 1$ divides both a and 48, then $am = an$ does not imply that $m = n$, and φ_a is therefore not injective. For example, if $a = 14$, then $\varphi_a(7) = (x^14)^7 = x^{98} = x^2$ and $\varphi_a(31) = (x^14)^31 = x^{434} = x^2$).

Finally, φ_a is onto. Let $x^b \in Z_{48}$. Suppose there exists some $n \in \mathbb{Z}/48\mathbb{Z}$ such that $\varphi_a(n) = x^b$, that is, $(x^a)^n = x^b$. Then we must have $an = b \pmod{48}$. Since a is relatively prime to 48, any integer between 0 and 47 can be written as an for some $n \in \mathbb{Z}/48\mathbb{Z}$, and so φ_a is onto.

Thus for a relatively prime to 48, $\varphi_a : \overline{1} \mapsto x^a$ is an isomorphism from $\mathbb{Z}/48\mathbb{Z}$ onto Z_{48}. □

9. (7/2/23)

Let $Z_{36} = \langle x \rangle$. For which integers a does the map φ_a defined by $\varphi_a : \overline{1} \mapsto x^a$ extend to a *well defined homomorphism* from $\mathbb{Z}/48\mathbb{Z}$ onto Z_{36}? Can φ_a ever be a surjective homomorphism?

Proof. We will show that $\varphi_a : \mathbb{Z}/48\mathbb{Z} \to Z_{36}$ is a well defined homomorphism if and only if a is a multiple of 3.

For φ_a to be a homomorphism, we must have $\varphi_a(b)\varphi_a(c) = \varphi_a(b+c)$ for all $b, c \in \mathbb{Z}/48\mathbb{Z}$. Now $\varphi_a(b)\varphi_a(c) = (x^a)^b(x^a)^c = (x^a)^{b+c} = x^{a(b+c)}$ and $\varphi_a(b+c) = (x^a)^{b+c} = x^{a(b+c)}$. Superficially these appear identical already. However, note that in $\varphi_a(b)\varphi_a(c)$ we compute $ab + ac$ mod 36, while in $\varphi_a(b+c)$ we first take $b + c$ mod 48 before then computing $a(b + c)$. That is, a must satisfy

$$a(b + c \bmod 48) \bmod 36 = a(b + c) \bmod 36$$

for all $b, c \in \mathbb{Z}/48\mathbb{Z}$. If $b + c < 48$, then the two are equal for all $a \in \mathbb{Z}$. So suppose that $b + c \geq 48$. Then $b + c \bmod 48 = b + c - 48$, so we must have

$$\begin{aligned} a(b + c - 48) \bmod 36 &= a(b + c) \bmod 36 \\ ab + ac - 48a \bmod 36 &= ab + ac \bmod 36 \\ -48a \bmod 36 &= 0 \bmod 36 \\ -48a &\cong 36 \Rightarrow 48a \cong 36, \end{aligned}$$

that is, a is some integer which, when multiplied by 48, results in a multiple of 36. Writing 48 as the product of its prime factors gives $2^4 \cdot 3$, while $36 = 2^2 \cdot 3^2$. Note that 36 has one more factor of 3, and so when a is a multiple of 3, $48a$ will be a multiple of 36. Only these values satisfy the exponents in the equation above, and thus φ_a is a homomorphism if and only if a is a multiple of 3.

It is not possible for φ_a to be a surjective homomorphism. Because a must be a multiple of 3, we have $\varphi_a(1) = x^a = x^{3n} = (x^3)^n$ for some $n \in \mathbb{Z}$. In turn, φ_a generates only the values $\varphi_a(2) = (x^6)^n, \varphi_a(3) = (x^9)^n$, ..., that is, it only generates powers of x^3 in Z_{36}. By counterexample, there is no value in $\mathbb{Z}/48\mathbb{Z}$ whose image under φ_a is x, and so φ_a cannot be surjective. $\square$

10. (7/2/23)

What is the order of $\overline{30}$ in $\mathbb{Z}/54\mathbb{Z}$? Write out all the elements and their orders in $\langle\overline{30}\rangle$.

Proof. First, the group $\langle\overline{30}\rangle$ (ordered by multiples of $\overline{30}$ consists of the elements $\{0, 30, 6, 36, 12, 42, 18, 48, 24\}$. This implies that the order of $\overline{30} = |\langle\overline{30}\rangle| = 9$.

The orders of each of the elements of $\langle\overline{30}\rangle$ are:

- 0: 1
- 6: 9
- 12: 9
- 18: 3
- 24: 9
- 30: 9
- 36: 3
- 42: 9
- 48: 9

$\square$

11. (7/2/23)

Find all cyclic subgroups of D_8 Find a proper subgroup of D_8 which is not cyclic.

Proof. Recall that $D_8 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$. A cyclic subgroup of D_8 must be generated by one element, so it cannot contain both s and a multiple of r. Therefore the cyclic subgroups of D_8 are:

- $\langle 1\rangle = \{1\}$
- $\langle r\rangle = \langle r^3\rangle = \{1, r, r^2, r^3\}$

- $\langle r^2 \rangle = \{1, r^2\}$
- $\langle s \rangle = \{1, s\}$

The group D_8 also contains as a subgroup $\{1, r^2, s, sr^2\}$, which is generated by the two elements r^2 and s, and is therefore not cyclic. $\square$

12. (7/2/23)

Prove that the following groups are *not* cyclic:

(a) $Z_2 \times Z_2$

Proof. This group consists of the elements $\{(0,0),(0,1),(1,0),(1,1)\}$. So each non-identity element has order 2, and there is no element of order 4 (the size of the group). Therefore it is not generated by any single element, and so it is not a cyclic group. $\square$

(b) $Z_2 \times \mathbb{Z}$

Proof. Now $Z_2 \times \mathbb{Z} = \{(a,b) \mid a = 0 \text{ or } 1, b \in \mathbb{Z}\}$. So a generating element must be of the form $(0,b)$ or $(1,b)$. Elements of the form $(0,b)$ can only generate $(0,2b),(0,3b),...$ but never $(1,nb)$, so a generating element must be of the form $(1,b)$. Multiples of $(1,b)$ include $(0,2b),(1,3b),(0,4b),...$, that is, $(0,nb)$ and $(1,mb)$ for even n and odd m, respectively. However, then this element cannot generate $(1,nb)$, and so it is not a generating element. Since both candidates fail to generate the group, it is not cyclic. $\square$

(c) $\mathbb{Z} \times \mathbb{Z}$

Proof. Similar to $Z_2 \times \mathbb{Z}$, consider a generating element of $\mathbb{Z} \times \mathbb{Z}$, (a,b). Multiples of this element include $(2a,2b),(3a,3b),...$, that is, (na,nb) for $n \in \mathbb{Z}$. However, this element cannot generate (a,nb) (where $n \neq 1$), and so it is not a generating element. Since all elements of $\mathbb{Z} \times \mathbb{Z}$ are of this form, there is no generating element, and so the group is not cyclic. $\square$

13. (7/5/23)

Prove that the following groups are *not* isomorphic:

(a) $\mathbb{Z} \times Z_2$ and $\mathbb{Z}$

Proof. The group of the integers under addition contains no elements of finite order other than the identity, 0. However, the group $\mathbb{Z} \times Z_2$ contains the element $(0,1)$, which has order 2. Since there is no corresponding element of order 2 in $\mathbb{Z}$, the groups are not isomorphic. $\square$

(b) $\mathbb{Q} \times Z_2$ and $\mathbb{Q}$

Proof. The proof that $\mathbb{Q} \times Z_2$ and $\mathbb{Q}$ are not isomorphic is identical to the proof that $\mathbb{Z} \times Z_2$ and $\mathbb{Z}$ are not isomorphic. $\square$

14. (7/5/23)

Let $\sigma = (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12)$. For each of the following integers a compute σ^a:

- $a = 13$: $\sigma^{13} = \sigma$
- $a = 65$: $\sigma^{65} = \sigma^5 = (1, 6, 11, 4, 9, 2, 7, 12, 5, 10, 3, 8)$
- $a = 626$: $\sigma^{626} = \sigma^2 = (1, 3, 5, 7, 9, 11)(2, 4, 6, 8, 10, 12)$
- $a = 1195$: $\sigma^{1195} = \sigma^7 = (1, 8, 3, 10, 5, 12, 7, 2, 9, 4, 11, 6)$
- $a = -6$: $\sigma^{-6} = \sigma^6 = (1, 7)(2, 8)(3, 9)(4, 10)(5, 11)(6, 12)$
- $a = -81$: $\sigma^{-81} = \sigma^3 = (1, 4, 7, 10)(2, 5, 8, 11)(3, 6, 9, 12)$
- $a = -570$: $\sigma^{-570} = \sigma^6$
- $a = -1211$: $\sigma^{-1211} = \sigma^{-11} = \sigma$

15. (7/5/23)

Prove that $\mathbb{Q} \times \mathbb{Q}$ is not cyclic.

Proof. If $\mathbb{Q} \times \mathbb{Q}$ were cyclic, then it could be generated from a single element. Suppose toward contradiction that some element (x, y) generates $\mathbb{Q} \times \mathbb{Q}$. Under addition in $\mathbb{Q}$ for each element of the ordered pair, we can generate elements of the form $(0, 0), (\pm x, \pm y), (\pm 2x, \pm 2y), (\pm 3x, \pm 3y), ...$ However, we cannot generate the element $(x/2, y/2)$, which is an element of $\mathbb{Q} \times \mathbb{Q}$. Therefore an arbitrary element (x, y) cannot generate $\mathbb{Q} \times \mathbb{Q}$, and so there is no generator. Thus $\mathbb{Q} \times \mathbb{Q}$ is not a cyclic group. $\square$

16. (7/8/23)

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

Proof. Given $|x| = n, |y| = m$, note that $x^n = y^m = 1$ implies that $x^{mn}y^{mn} = (xy)^{mn} = 1$. So xy has finite order. Suppose that $|xy| = k < \infty$. Then, from Ch. 1, Ex. 24., $(xy)^k = x^k y^k = 1$.

First, consider that if $x^k = a \neq 1$, then $y^k = a^{-1}$. It follows that $x^k = (y^k)^{-1}$, and so $x = y^{-1}$. Then $|xy| = |1| = 1$, which trivially divides the least common multiple of m and n.

In the other case, we must have $x^k = y^k = 1$. Since the orders of x and y are n and m, respectively, the orders of both elements divide k, that is, k is a multiple of both n and m. It follows that k must be the least common multiple of m and n.

If x and y do not commute, then the above does not hold. For example, in D_8, $|r^3| = |r^7| = 8$. However, $|(r^3r^7)| = |r^{10}| = |r^2| = 4$, which is not equal to the least common multiple of 8 and 8. $\square$

17. (7/8/23)

Find a presentation for Z_n with one generator.

Proof. Let Z_n be the cyclic group of order n. A presentation for Z_n is:

$$\langle x \mid x^n = 1 \rangle.$$

This generates the n elements $\{x, x^2, ..., x^{n-1}, 1\}$, which is equal to Z_n. $\square$