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

Scott Donaldson

Jun. - Jul. 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
- $\langle x^{15} \rangle = \{1, x^{15}, x^{30}\} \equiv \mathbb{Z}/3\mathbb{Z}$
- $\langle x^9 \rangle = \{1, x^9, x^{18}, x^{27}, x^{36}\} \equiv \mathbb{Z}/5\mathbb{Z}$
- $\langle x^5 \rangle = \{1, x^5, x^{10}, x^{15}, x^{20}, x^{25}, x^{30}, x^{35}, x^{40}\} \equiv \mathbb{Z}/9\mathbb{Z}$
- $\langle x^3 \rangle = \{1, x^3, x^6, ..., x^{39}, x^{42}\} \equiv \mathbb{Z}/15\mathbb{Z}$
- $\langle x \rangle = Z_{45}$ 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. $\square$

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. $\square$

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 $\mathbb{Z}/49000\mathbb{Z}$. $\square$

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 $\mathbb{Z}/48\mathbb{Z} \equiv Z_{48}$ 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

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

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 $(0, 0), (\pm x, \pm y), (\pm 2x, \pm 2y), (\pm 3x, \pm 3y), \ldots.$ 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. $\square$

18. (7/8/23)

Show that if H is any group and h is an element of H with $h^n = 1$, then there is a unique homomorphism from $Z_n = \langle x \rangle$ to H such that $x \mapsto h$.

Proof. Let φ be a map from $Z_n \Rightarrow H$ defined by $\varphi(x^k) = h^k$ for $k \in \{0, ..., n-1\}$. We will show first that φ is a homomorphism, and then that is the unique homomorphism from Z_n to H such that $\varphi(x) = h$.

Let x^a, x^b be arbitrary elements of Z_n. We have $\varphi(x^a)\varphi(x^b) = h^a h^b = h^{a+b} = \varphi(x^{a+b}) = \varphi(x^a x^b)$, so φ is a homomorphism.

Next, suppose that γ is a homomorphism from Z_n to H with $\gamma(x) = h$. Then, from Ch. 1.6, Ex. 1, we have:

$$\gamma(x^a) = \gamma(x)^a = h^a = \varphi(a),$$

and so $\gamma = \varphi$. Therefore φ is the only such homomorphism from Z_n to H with $\varphi(x) = h$. $\square$

19. (7/8/23)

Show that if H is any group and h is any element of H, then there is a unique homomorphism from $\mathbb{Z}$ to H such that $1 \mapsto h$.

Proof. The structure of this proof is nearly identical to that of the immediately preceding exercise. Let φ be a map from $\mathbb{Z} \Rightarrow H$ defined by $\varphi(k) = h^k$ for any $k \in \mathbb{Z}$. We will show first that φ is a homomorphism, and then that is the unique homomorphism from $\mathbb{Z}$ to H such that $\varphi(1) = h$.

For any $a, b \in \mathbb{Z}$, we have $\varphi(a)\varphi(b) = h^a h^b = h^{a+b} = \varphi(a+b)$, so φ is a homomorphism.

Next, suppose that γ is a homomorphism from $\mathbb{Z}$ to H with $\gamma(1) = h$. Then:

$$\gamma(a) = \gamma(\underbrace{1 + ... + 1}_{a \text{ times}}) = \underbrace{\gamma(1) \cdot ... \cdot \gamma(1)}_{a \text{ times}} = \underbrace{h \cdot ... \cdot h}_{a \text{ times}} = h^a = \varphi(a),$$

and so $\gamma = \varphi$. Therefore φ is the only such homomorphism from $\mathbb{Z}$ to H with $\varphi(1) = h$. $\square$

20. (7/8/23)

Let p be a prime and let n be a positive integer. Show that if x is an element of the group G such that $x^{p^n} = 1$ then $|x| = p^m$ for some $m \leq n$.

Proof. Since $x^{p^n} = 1$, x has finite order, so let $|x| = a < \infty$. Then we must have $a \leq p^n$, and $a \mid p^n$. Written as a product of its factors, $p^n = \underbrace{p \cdot ... \cdot p}_{n \text{ times}}$. From the Fundamental Theorem of Arithmetic, any divisor of this product must be a product of its factors, which consist only of the prime p. Thus, it follows that a is likewise a product of p, and so $|x| = p^m$ for some $m \leq n$. $\square$

21. (7/9/23)

Let p be an odd prime and let n be a positive integer. Use the Binomial Theorem to show that $(1+p)^{p^{n-1}} \equiv 1 \pmod{p^n}$ but $(1+p)^{p^{n-2}} \not\equiv 1 \pmod{p^n}$. Deduce that $1 + p$ is an element of order p^{n-1} in the multiplicative group $(\mathbb{Z}/p^n\mathbb{Z})^\times$.

Proof. The Binomial Theorem states that $(x+y)^n = \binom{n}{0}x^n y^0 + \binom{n}{1}x^{n-1}y^1 + ... + \binom{n}{n}x^0 y^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$.

Then for $(1+p)^{p^{n-1}}$, we have:

$$\begin{aligned}
(1+p)^{p^{n-1}} &= \sum_{k=0}^{p^{n-1}} \binom{p^{n-1}}{k} p^{p^{n-1}-k} \\
&= 1 + \sum_{k=1}^{p^{n-1}} \binom{p^{n-1}}{k} p^n p^{(p^{n-1}-k-n)} \\
&= 1 + p^n \sum_{k=1}^{p^{n-1}} \binom{p^{n-1}}{k} p^{(p^{n-1}-k-n)}.
\end{aligned}$$

Notice that, by factoring out the constant p^n from the sum, the entire equation will be equal to 1 (mod p^n) if the exponent within the sum, $p^{n-1} - k - n$, remains a non-negative integer for each summand. Now k ranges from 1 to n, so $p^{n-1} - k - n \geq p^{n-1} - n - n = p^{n-1} - 2n$. We will that $p^{n-1} - 2n \geq 0$ for all primes p, with $n > 0$.

First, let's consider the case $n \geq 3$ (we will consider $n = 1$ and 2 separately). By induction, with the base case $n = 3$, we have $p^{n-1} - 2n = p^2 - 6$, which is positive for all primes $p \geq 3$. Suppose then that $p^{n-1} - 2n \geq 0$ for some fixed n. This implies that $p^{n-1} \geq 2n$. Now since we are only considering odd prime numbers p, we must have $p > 2$. Then if we multiply the left side of the inequality by p, and add 2 to the right side, the inequality holds because we have added more to the left side than the right side. This results in $p \cdot p^{n-1} \geq 2n+2 \Rightarrow p^{(n+1)-1} \geq 2(n+1)$, which satisfies the induction step. This shows that the exponent in the above sum is indeed a non-negative integer, and so the entire sum reduces to an integer, which proves that $(1+p)^{p^{n-1}} \equiv 1$ (mod p^n) for $n \geq 3$.

The final cases $n = 1$ and $n = 2$ are simple enough to solve algebraically. For $n = 1$, we have $(1+p)^{p^0} = 1 + p \equiv 1 \pmod{p}$. Then, for $n = 2$, we have $(1+p)^{p^1} = (1+p)^p$. Again using the Binomial Theorem, we have:

$$
\begin{aligned}
(1+p)^p &= \sum_{k=0}^{p} \binom{p}{k} p^{p-k} = \underbrace{\sum_{k=0}^{p} \binom{p}{k} p^k}_{\text{(alternate form)}} \\
&= 1 + \sum_{k=1}^{p} \binom{p}{k} p^k = 1 + p^2 \sum_{k=1}^{p} \binom{p}{k} p^{k-2} \\
&= 1 + p^2 \left(\binom{p}{1} p^{-1} + \binom{p}{2} p^0 + \binom{p}{3} p^1 + ... + \binom{p}{p} p^{p-2} \right).
\end{aligned}
$$

Of the summands within the parentheses, only one — $\binom{p}{1} p^{-1}$ is not obviously an integer, because may be a fraction with p in the denominator. However, it reduces to $\frac{p!}{1 \cdot (p-1)!} p^{-1} = p \cdot p^{-1} = 1$. Therefore the sum remains a whole number, and so the entire expansion is equivalent to 1 mod p^2.

This completes the proof that $(1+p)^{p^{n-1}} \equiv 1$ (mod p^n) for odd primes p and $n > 0$.

Now if we consider $(1+p)^{p^{n-2}}$, the Binomial Theorem expansion shows that:

$$
\begin{aligned}
(1+p)^{p^{n-2}} &= \sum_{k=0}^{p^{n-2}} \binom{p^{n-2}}{k} p^{p^{n-2}-k} \\
&= 1 + p^{n-2}p + \frac{p^{n-2}(p^{n-2}-1)}{2} p^2 + \frac{p^{n-2}(p^{n-2}-1)(p^{n-2}-2)}{6} p^3 \\
&\quad + ... + p^{p^{n-2}} \\
&= 1 + p^{n-1} + p^n (...)
\end{aligned}
$$

Where the omitted elements within the parenthesis reduce to an integer by similar proof to above. However, the whole expansion is equivalent to $(1+p^{n-1}) \mod p^n$, not 1.

Finally, we note that, since p^{n-1} is the smallest power a of $1+p$ such that $(1+p)^a \equiv 1 \pmod{p^n}$, this implies that $1+p$ is an element of order p^{n-1} in the multiplicative group $\mathbb{Z}/2^n\mathbb{Z}^\times$. $\square$

22. (7/9/23)

Let n be an integer $n \geq 3$. Use the Binomial Theorem to show that $(1+2^2)^{2^{n-2}} \equiv 1 \pmod{2^n}$ but $(1+2^2)^{2^{n-3}} \not\equiv 1 \pmod{2^n}$. Deduce that 5 is an element of order 2^{n-2} in the multiplicative group $(\mathbb{Z}/2^n\mathbb{Z})^\times$.

Proof. Now:

$$\begin{aligned}(1+2^2)^{2^{n-2}} &= 1 + 2^{n-2}\cdot 2^2 + \frac{2^{n-2}(2^{n-2}-1)}{2}\cdot(2^2)^2 + \\ &\quad \frac{2^{n-2}(2^{n-2}-1)(2^{n-2}-2)}{6}\cdot(2^2)^3 + ... + (2^2)^{2^{n-2}} \\ &= 1 + 2^n + 2^n\frac{2^2(2^{n-2}-1)}{2} + 2^n\frac{(2^2)^2(2^{n-2}-1)(2^{n-2}-2)}{6} + \\ &\quad ... + 2^n(2^{2^{n-1}-n}),\end{aligned}$$

and as with Exercise 21, every summand after 1 is the product of 2^n with a whole number, which implies that the entire sum is equivalent to $1 \pmod{2^n}$.

Meanwhile:

$$\begin{aligned}(1+2^2)^{2^{n-3}} &= 1 + 2^{n-3}\cdot 2^2 + \frac{2^{n-3}(2^{n-3}-1)}{2}\cdot(2^2)^2 + \\ &\quad \frac{2^{n-3}(2^{n-3}-1)(2^{n-3}-2)}{6}\cdot(2^2)^3 + ... + (2^2)^{2^{n-3}} \\ &= 1 + 2^{n-1} + 2^n(2^{n-3}-1) + 2^n\frac{2^3(2^{n-3}-1)(2^{n-3}-2)}{6} + \\ &\quad ... + 2^n(2^{2^{n-2}-n}),\end{aligned}$$

which is not equivalent to $1 \pmod{2^n}$. It follows that the order of 5 in $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is 2^{n-2}. $\square$

23. (7/9/23)

Show that $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is not cyclic for any $n \geq 3$. [Find two distinct subgroups of order 2.]

Proof. Recall that the multiplicative group $(\mathbb{Z}/2^n\mathbb{Z})^\times$ consists of all integers between 1 and 2^n with a multiplicative inverse in $\mathbb{Z}/2^n\mathbb{Z}$, that is, all integers relatively prime to 2^n, or all positive odd integers less than 2^n.

Note that, in $\mathbb{Z}/2^n\mathbb{Z}$:

$$(2^n-1)^2 = (2^n)^2 - 2\cdot 2^n + 1 = 2^{2n} - 2^{n+1} + 1 = 2^n(2^n-2) + 1 = 1, \text{ and}$$
$$(2^{n-1}-1)^2 = (2^{n-1})^2 - 2\cdot 2^{n-1} + 1 = 2^{2n-2} - 2^n + 1 = 2^n(2^{n-2}-1) + 1 = 1.$$

So $2^n - 1$ and $2^{n-1} - 1$ are two distinct elements in $(\mathbb{Z}/2^n\mathbb{Z})^\times$ of order 2. From Theorem 7.(3), a cyclic group has only one unique subgroup of order 2. However, $(\mathbb{Z}/2^n\mathbb{Z})^\times$ contains the two distinct subgroups $\{1, 2^n-1\}$ and $\{1, 2^{n-1}-1\}$. Thus $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is *not* a cyclic group. □

24. (7/11/23)

Let G be a finite group and let $x \in G$.

(a) Prove that if $g \in N_G(\langle x\rangle)$ then $gxg^{-1} = x^a$ for some $a \in \mathbb{Z}$.

Proof. Recall that $N_G(\langle x\rangle) = \{g \in G \mid g\langle x\rangle g^{-1} = \langle x\rangle\}$.

Let $g \in G$ be in the normalizer of $\langle x\rangle$. Then for each $x^k \in \langle x\rangle$, $gx^kg^{-1} \in \langle x\rangle$, and specifically $gxg^{-1} \in \langle x\rangle$. Since $\langle x\rangle$ consists of all powers of x, this implies in turn that $gxg^{-1} = x^a$ for some $a \in \mathbb{Z}$. □

(b) Prove conversely that if $gxg^{-1} = x^a$ for some $a \in \mathbb{Z}$ then $g \in N_G(\langle x\rangle)$.

Proof. Suppose that, for some $g \in G$, $gxg^{-1} = x^a$ for some $a \in \mathbb{Z}$. It can be shown by induction that $(gxg^{-1})^k = gx^kg^{-1}$ for all integers k. It follows that, for all elements $x^k \in \langle x\rangle$, we have $gx^kg^{-1} = (gxg^{-1})^k = x^{ak}$, a power of x which is therefore also in $\langle x\rangle$. This implies that $g\langle x\rangle g^{-1} = \langle x\rangle$, and thus $g \in N_G(\langle x\rangle)$. □

25. (7/11/23)

Let G be a cyclic group of order n and let k be an integer relatively prime to n. Prove that the map $x \mapsto x^k$ is surjective. Use Lagrange's Theorem (Ch. 1.7, Exercise 19) to prove the same is true for any finite group of order n.

Proof. Let $G = \langle x\rangle, |G| = n$, and let k be relatively prime to n. Define a map $\varphi : G \to G$ by $\varphi(x) = x^k$.

From Proposition 6., the generators of G are those x^k for which k is relatively prime to n, so $G = \langle x\rangle = \langle x^k\rangle$; that is, $\langle x^k\rangle$ has n distinct elements. Now $\varphi(\langle x\rangle) = \{1, x^k, x^{2k}, ..., x^{(n-1)k}\} = \langle x^k\rangle$. Thus φ maps onto every element of $G = \langle x^k\rangle$, and so is surjective.

Now let H be an arbitrary finite group of order n and define φ as above. Let $x \in H$ and suppose that $|x| = a$. Now $\langle x\rangle$ is a subgroup of H of order a, so by Lagrange's Theorem, a divides n. Next, again consider $\varphi(\langle x\rangle) =$

$\{1, x^k, x^{2k}, ..., x^{(n-1)k}\} = \langle x^k \rangle$. Since k is relatively prime to n, it is also relatively prime to every divisor of n, including a. So the order of $\langle x^k \rangle$ can be no less than a, since for no integer $b < a$ do we have $x^{bk} = 1$. However, since $x^a = 1 \Rightarrow x^{ak} = 1$, it can also be no greater than a. It follows that $|\langle x^k \rangle| = a$. And, since $x^k \in \langle x^k \rangle$ and $x^k \in \langle x \rangle$, we must have $\langle x \rangle = \langle x^k \rangle$. Thus, every element $x \in H$, x is included in $\varphi(\langle x \rangle)$, that is, there is some power of x whose image under φ is x, and therefore φ is a surjective map. $\square$

26. (7/11/23)

Let Z_n be a cyclic group of order n and for each integer a let

$$\sigma_a : Z_n \to Z_n \qquad \text{by} \qquad \sigma_a(x) = x^a \text{ for all } x \in Z_n.$$

(a) Prove that σ_a is an automorphism of Z_n if and only if a and n are relatively prime.

Proof. First, let a and n be relatively prime. From Proposition 6., $\langle x^a \rangle = Z_n$, and from Exercise 25., σ_a is surjective. To show that it is one-to-one, let $x^b, x^c \in Z_n$. If $\sigma_a(x^b) = \sigma_a(x^c)$, then it follows that $(x^b)^a = (x^c)^a \Rightarrow (x^a)^b = (x^a)^c$. For all $b \in \{0, ..., n-1\}$, $(x^a)^b$ is unique (otherwise we would not have $\langle x^a \rangle = Z_n$), so $(x^a)^b = (x^a)^c$ implies that $b = c$, and therefore σ_a is injective.

This shows that σ_a is a bijection from Z_n to Z_n, but not yet that is an isomorphism. However, the fact that it is a homomorphism follows simply enough From

$$\sigma_a(x^b)\sigma_a(x^c) = (x^b)^a = (x^c)^a = (x^b x^c)^a = \sigma_a(x^b x^c),$$

and so σ_a is an automorphism of Z_n.

Next, suppose that σ_a is an automorphism of Z_n (to show that a is relatively prime to n). Suppose that d is a common divisor of a and n. Let $a = cd$ and $n = bd$. Now $\sigma_a(x^b) = x^{ab} = x^{bcd} = x^{cn} = (x^n)^c = 1$. And $\sigma_a(x^{2b}) = x^{2ab} = x^{2bcd} = x^{2cn} = (x^n)^{2c} = 1$. Since σ_a is an automorphism, $\sigma_a(x^b) = \sigma_a(x^{2b})$ implies that $b = 2b$ (mod n). Therefore b can be no less than n, and so b must equal n, which implies that $d = 1$. Therefore a and n are relatively prime. $\square$

(b) Prove that $\sigma_a = \sigma_b$ if and only if $a \equiv b$ (mod n).

Proof. First, let $a \equiv b$ (mod n). Let $a = qn + b \Rightarrow b = a - qn$. Then $\sigma_b(x) = x^{a-qn} = x^a x^{-qn} = x^a x^0 = x^a = \sigma_a(x)$, and so $\sigma_a = \sigma_b$.

Next, let $\sigma_a = \sigma_b$ (to show that $a \equiv b$ (mod n)). Then for each $x^k \in Z_n$, $\sigma_a(x^k) = \sigma_b(x^k)$. This implies that $x^{ak} = x^{bk}$, and so $ak \equiv bk$ (mod n) for each $k \in \mathbb{Z}$. For k relatively prime to n, this in turn implies that $a \equiv b$. $\square$

(c) Prove that *every* automorphism of Z_n is equal to σ_a for some integer a.

Proof. Let $\varphi : Z_n \to Z_n$ be an automorphism. With $Z_n = \langle x \rangle$, suppose that for the generating element x, $\varphi(x) = x^a$, where $0 \leq a < n$. Consider an arbitrary element x^k. Since φ is an automorphism, we have $\varphi(x^k) = \varphi(x)^k = (x^a)^k = (x^k)^a$. Then for every element x^k, $\varphi(x^k) = (x^k)^a = \sigma_a(x^k)$ as defined above. $\square$

(d) Prove that $\sigma_a \circ \sigma_b = \sigma_{ab}$. Deduce that the map $\overline{a} \mapsto \sigma_a$ is an isomorphism of $(\mathbb{Z}/n\mathbb{Z})^\times$ onto the automorphism group of Z_n (so $\mathrm{Aut}(Z_n)$ is an abelian group of order $\varphi(n)$, where φ is the Euler totient function).

Proof. Clearly:

$$(\sigma_a \circ \sigma_b)(x) = \sigma_a(\sigma_b(x)) = \sigma_a(x^b) = (x^b)^a = x^{ab} = \sigma_{ab}(x),$$

and so $\sigma_a \circ \sigma_b = \sigma_{ab}$.

Now let $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$ and define $\pi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Aut}(Z_n)$ by $\pi(a) = \sigma_a$. We can see that $\pi(a)\pi(b) = \sigma_a \circ \sigma_b = \sigma_{ab} = \pi(ab)$, so π is a homomorphism. Further, from b) and c), π is one-to-one and onto (respectively), and is therefore an isomorphism. Thus the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ is isomorphic to $\mathrm{Aut}(Z_n)$, and so the latter is an abelian group of order $\varphi(n)$. $\square$