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 $\mathbb{Z}/48\mathbb{Z}$.

Proof. 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: $\langle \overline{24} \rangle$.

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. $\square$