Chapter 04

Mostafa Touny

September 25, 2023

Contents

Problems

1

By *corollary 4* (page 80).

Generators of $\mathcal{Z}_6$ are $1, 5$ since $gcd(1, 6) = gcd(5, 6) = 1$.

Generators of $\mathcal{Z}_8$ are $1, 3, 5, 7$ since $gcd(1, 8) = gcd(3, 8) = gcd(5, 8) = gcd(7, 8) = 1$.

Generators of $\mathcal{Z}_{20}$ are $1, 3, 7, 9, 11, 13, 17, 19$ since $gcd(1, 20) = gcd(3, 20) = gcd(7, 20) = gcd(9, 20) = gcd(11, 20) = gcd(13, 20) = gcd(17, 20) = gcd(19, 20) = 1$.

5

$\langle 3 \rangle = \{3^0, 3^1, 3^2, 3^3, 3^4, 3^5, \dots\} \cup \{3^{-1}, 3^{-2}, 3^{-3}, 3^{-4}, 3^{-5}, \dots\} = \{0, 3, 9, 7, 1, 3, \dots\} \cup \{-3, 9, -7, 1, -3, \dots\} = \{0, 3, 9, 7, 1, 3\} \cup \{17, 9, 13, 1, 17\} = \{0, 1, 3, 7, 9, 13, 17\}$.

$\langle 7 \rangle = \{7^0, 7^1, 7^2, 7^3, 7^4, 7^5, \dots\} \cup \{7^{-1}, 7^{-2}, 7^{-3}, 7^{-4}, 7^{-5}, \dots\} = \{0, 7, 9, 3, 1, 7, \dots\} \cup \{-7, 9, -3, 1, -7, \dots\} = \{0, 7, 9, 3, 1\} \cup \{13, 1, 17, 1\} = \{0, 1, 3, 7, 9, 13, 17\}$

10

By corollary (page 82). One generator is $\langle 24/8 \rangle = \langle 3 \rangle = \{3^0, 3^1, 3^2, 3^3, 3^4, 3^5, 3^6, 3^7, 3^8, 3^9\} \cup \{3^{-1}, 3^{-2}, 3^{-3}, 3^{-4}, 3^{-5}, 3^{-6}, 3^{-7}, 3^{-8}, 3^{-9}\} = \{0, 3, 6, 9, 12, 15, 18, 21, 0\} \cup \{21, 6, 15, 12, 9, 18, 3, 0, 21\} = \{0, 3, 6, 9, 12, 15, 18, 21\}$

Note any generator of that subgroup must be contained in it as $a = a^1 \in \langle a \rangle$.

By corollary 3 (page 80). Generators are $3^5 = 15$ and $3^7 = 21$, as $gcd(24, 5) = gcd(24, 7) = 1$.

By corollary 3 (page 80). Generators of arbitrary G are $1, 5, 7, 11, 13, 17, 19, 23$ since $gcd(24, i) = 1$. Observe since G is generated by a, Any candidate must be of the form a^i. So we covered all of them.

11

Follows trivially by corollary 3 (page 80), as $gcd(n, -1) = 1$.

27

We know given a positive integer n, there is a complex z such that $z^n = 1$. Then $S_n = \{z^0, z^1, z^2, \dots\} = \{z^0, z^1, \dots, z^{n-1}\}$. Clearly it is a group.

For z^{-i} observe $-i = n(m) + r$ where $0 \leq r < n$. Then $-i - r$ is divisable by n, and by *theorem 4.1* (page 76), $z^{-i} = z^r$. Then $\{z^{-1}, z^{-2}, \dots\}$ is contained in S_n.

Thus we conclude $S_n = \langle z \rangle$ is a subgroup of order n.

30

We call a subgroup *new* if it is not $\{e\}$ or G. Observe constructing it contradicts a given hypothesis.

Select $a \neq e$. If $\langle a \rangle$ is of infinite order, then $\langle a^2 \rangle$ is a *new* subgroup. So $\langle a \rangle$ is of finite order n.

If $\langle a \rangle \neq G$ then $\langle a \rangle$ is a *new* subgroup. So $\langle a \rangle = G$.

If n is not prime, i.e composite, then by *theorem 4.3* (page 81), we can take divisor k such that $\langle a^{n/k} \rangle$ is a *new* subgroup of order k. Note by divisibility $1 < k < n$.

It follows G is a finite cyclic group of prime order n.

36

	4	8	12	16
4	16	12	8	4
8	12	4	16	8
12	8	16	4	12
16	4	8	12	16

All entries are contained in $\{4, 8, 12, 16\}$, So closed. 16 is the identity. Every row has an 16 entry showing inverses existince. The group is cyclic.

Its generators are all its elements, $4, 8, 12$ and 16. To see why you can trace the table. For example $8^1 = 8$, $8^2 = 4$, $8^3 = 8^2 \cdot 8 = 4 \cdot 8 = 12$, $8^4 = 8^3 \cdot 8 = 12 \cdot 8 = 16$.

48

H is a subgroup by *Theorem 3.2* (page 63). Given $a = 10k_0 = 8k_1$ and $b = 10k_2 = 8k_3$, Trivially $a + b = 10(k_0 + k_2) = 8(k_1 + k_3) \in H$. Also $-a = 10(-k_0) = 8(-k_1) \in H$.

H is not a subgroup in case of "OR". Consider the counter-example $10 + 8 = 18$ as 18 is neither divisible by 10 nor 8, Violating closeness property.

59

*** Partially Solved**.

Let G be a group with only a and b elements of order 2. We try to come-up with a contradiction.

By definition $a^2 = b^2 = e$, so $a^{-1} = a$ and $b^{-1} = b$. Clearly $ab \neq a, b$, or e. For example if $ab = e$ then $b = a^{-1} = a$ which is not true as a and b are given as distinct elements.

Case $ab = ba$. Then $(ab)^2 = (ab)(ba) = aea = a^2 = e$. Contradiction.

Case $ab \neq ba$. No solution found for that case.

61

Let $x \in \langle a \rangle \cap \langle b \rangle$. Then by *corollary 1* (page 79), $|x|$ divides both 10 and 21. Since they are coprime, $|x| = 1$ and $x^1 = x = e$.