MATH 343 · Group Theory

Chapter 4 Assigned Problems

Exercises 1, 8, 9, 23, 24, 31, and 61

The $\mathbb{Z}_8$ part of Exercise 1 is worked in the Chapter 4 lecture slides; nothing else on the list is.

Solutions based on Gallian, Contemporary Abstract Algebra, 10th edition

Exercise 1: Question

Question

Find all generators of the following groups.

$$\mathbb{Z}_6, \qquad \mathbb{Z}_8, \qquad \mathbb{Z}_{20}$$

Exercise 1: Solution

Find all generators of $\mathbb{Z}_6$, $\mathbb{Z}_8$, and $\mathbb{Z}_{20}$.

The criterion

$$k \text{ generates } \mathbb{Z}_n \Leftrightarrow \gcd(n,k) = 1 \qquad \text{(Corollary 4 of Theorem 4.2)}$$

Group	Number of generators	Generators
$\mathbb{Z}_6$	$\phi(6) = 2$	1, 5
$\mathbb{Z}_8$	$\phi(8) = 4$	1, 3, 5, 7
$\mathbb{Z}_{20}$	$\phi(20) = 8$	1, 3, 7, 9, 11, 13, 17, 19

A check in $\mathbb{Z}_{20}$: the multiples of 3, in order, are

$$3,6,9,12,15,18,1,4,7,10,13,16,19,2,5,8,11,14,17,0$$

all twenty elements, so $\langle 3 \rangle = \mathbb{Z}_{20}$. The $\mathbb{Z}_8$ case is the worked example on the lecture slides.

Exercise 8: Question

Question

Let a be an element of a group with |a| = 15. Compute the orders of the following elements.

(a) $a^3,\ a^6,\ a^9,\ a^{12}$

(b) $a^5,\ a^{10}$

(c) $a^2,\ a^4,\ a^8,\ a^{14}$

Exercise 8: Solution

Orders of the powers of a, given |a| = 15.

$$\left|a^k\right| = \frac{15}{\gcd(15, k)} \qquad \text{(Theorem 4.2)}$$

k	3	6	9	12	5	10	2	4	8	14
gcd(15, k)	3	3	3	3	5	5	1	1	1	1
$\|a^k\|$	5	5	5	5	3	3	15	15	15	15

(a) all four have order 5 (b) both have order 3 (c) all four have order 15

Equal gcds mean equal subgroups (Corollary 2 of Theorem 4.2):

$$\langle a^3\rangle = \langle a^6\rangle = \langle a^9\rangle = \langle a^{12}\rangle, \quad \langle a^5\rangle = \langle a^{10}\rangle, \quad \langle a^2\rangle = \langle a^4\rangle = \langle a^8\rangle = \langle a^{14}\rangle = \langle a\rangle$$

so a^2, a^4, a^8 and a^{14} are generators of ⟨a⟩.

Exercise 9: Question

Question

How many subgroups does $\mathbb{Z}_{20}$ have? List a generator for each of these subgroups.

Suppose that $G = \langle a \rangle$ and $|a| = 20$. How many subgroups does G have? List a generator for each of these subgroups.

Exercise 9: Solution

Count the subgroups of $\mathbb{Z}_{20}$ and of $G = \langle a \rangle$ with $|a| = 20$, and give a generator of each.

20 has six positive divisors — 1, 2, 4, 5, 10, 20 — so each group has exactly six subgroups, one per divisor (Theorem 4.3). The subgroup of order k is

$$\langle 20/k \rangle \text{ in } \mathbb{Z}_{20}, \qquad \langle a^{20/k} \rangle \text{ in } G = \langle a \rangle$$

Order	Subgroup of $\mathbb{Z}_{20}$	Elements	Subgroup of $G = \langle a \rangle$
1	$\langle 0 \rangle$	{0}	$\langle a^{20} \rangle = \{e\}$
2	$\langle 10 \rangle$	{0, 10}	$\langle a^{10} \rangle$
4	$\langle 5 \rangle$	{0, 5, 10, 15}	$\langle a^{5} \rangle$
5	$\langle 4 \rangle$	{0, 4, 8, 12, 16}	$\langle a^{4} \rangle$
10	$\langle 2 \rangle$	{0, 2, 4, …, 18}	$\langle a^{2} \rangle$
20	$\langle 1 \rangle$	$\mathbb{Z}_{20}$	$\langle a \rangle$

Exercise 23: Question

Question

Let a and b be elements of a finite group, and suppose that a and b commute.
Prove that

$$|ab| = |a|\,|b| \Leftrightarrow \gcd(|a|, |b|) = 1$$

Exercise 23: Solution (1 of 2)

Write $m = |a|$, $n = |b|$ and $k = |ab|$. Since $ab = ba$, $(ab)^t = a^t b^t$ for every integer t.

If gcd(m, n) = 1, then k = mn

k divides mn

$$(ab)^{mn} = (a^m)^n (b^n)^m = e \;\Rightarrow\; k \mid mn$$

mn divides k

$$(ab)^k = e \;\Rightarrow\; a^k = b^{-k}$$

Call this element c. Then $c^m = (a^m)^k = e$ and $c^n = (b^n)^{-k} = e$, so |c| divides both m and n, hence divides gcd(m, n) = 1. So c = e, giving

$$a^k = e \text{ and } b^k = e \;\Rightarrow\; m \mid k \text{ and } n \mid k \;\Rightarrow\; mn \mid k$$

the last step because m and n are relatively prime.

Both divisibilities give k = mn, that is, |ab| = |a| |b|.

Exercise 23: Solution (2 of 2)

Conversely, suppose |ab| = mn, where m = |a| and n = |b|.

If k = mn, then gcd(m, n) = 1

Let d = gcd(m, n). Both m and n divide mn/d, so

$$(ab)^{mn/d} = (a^m)^{n/d}(b^n)^{m/d} = e$$

Hence mn = |ab| divides mn/d, which forces d = 1.

So |ab| = |a| |b| holds exactly when |a| and |b| are relatively prime.

Commutativity is essential: in S_3 the elements (12) and (123) have orders 2 and 3, with gcd 1, but their product is a transposition, of order 2 — not 6.

Exercise 24: Question

Question

Suppose that G is a group with more than one element and that G has no proper, nontrivial subgroups. Prove that $|G|$ is prime.

Do not assume at the outset that G is finite.

Exercise 24: Solution

G has more than one element and only the subgroups {e} and G. Show that |G| is prime.

G is cyclic

$$a \neq e \;\Rightarrow\; \langle a\rangle \neq \{e\} \;\Rightarrow\; \langle a\rangle = G$$

a has finite order

If |a| were infinite, $\langle a^2\rangle$ would be proper and nontrivial: $a^2 \neq e$, and $a \notin \langle a^2\rangle$.

and that order is prime

So $|G| = |\langle a\rangle| = n = |a| > 1$ (Corollary 1, Theorem 4.1). If $n = st$ with $1 < s < n$, Theorem 4.2 gives

$$|\langle a^s\rangle| = \frac{n}{\gcd(n,s)} = \frac{n}{s} = t, \qquad 1 < t < n$$

— again a proper nontrivial subgroup.

No divisor of n lies strictly between 1 and n, so |G| = n is prime.

Exercise 31: Question

Question

Let $\mathbb{Z}$ denote the group of integers under addition. Is every subgroup of $\mathbb{Z}$ cyclic? Why?

Describe all the subgroups of $\mathbb{Z}$.

Let a be a group element with infinite order. Describe all subgroups of $\langle a \rangle$.

Exercise 31: Solution

Are the subgroups of $\mathbb{Z}$ cyclic, and what are they? Same question for $\langle a \rangle$ when $|a|$ is infinite.

Yes. $\mathbb{Z} = \langle 1 \rangle$ is cyclic, and every subgroup of a cyclic group is cyclic (Theorem 4.3).

The argument, in $\mathbb{Z}$

Let $H \leq \mathbb{Z}$ with $H \neq \{0\}$. With $h \in H$ also $-h \in H$, so H has a least positive element m. For $h \in H$ write $h = mq + r$ with $0 \leq r < m$; then $r = h - mq \in H$, so $r = 0$ by minimality.

$$H = \langle m \rangle = m\mathbb{Z} = \{0, \pm m, \pm 2m, \pm 3m, \dots\}$$

All of them

$$\langle m \rangle \ \ (m = 0,1,2,3, \dots) \ \text{ in } \mathbb{Z}; \qquad \langle a^m \rangle \ \ (m = 0,1,2,3, \dots) \ \text{ in } \langle a \rangle$$

These are distinct for distinct m, since $a^i = a^j$ only when $i = j$ (Theorem 4.1). An infinite cyclic group therefore has infinitely many subgroups, while a finite one has exactly one per divisor of its order.

Exercise 61: Question

Question

List all the elements of $\mathbb{Z}_{40}$ that have order 10.

Let $|x| = 40$. List all the elements of $\langle x \rangle$ that have order 10.

Exercise 61: Solution

Find the elements of order 10 in $\mathbb{Z}_{40}$, and in $\langle x \rangle$ with $|x| = 40$.

$$|k| = \frac{40}{\gcd(40, k)} = 10 \Leftrightarrow \gcd(40, k) = 4$$

So k = 4j with gcd(j, 10) = 1, that is j = 1, 3, 7, 9:

$$k = 4,\ 12,\ 28,\ 36 \qquad \text{in } \mathbb{Z}_{40}; \qquad x^4,\ x^{12},\ x^{28},\ x^{36} \qquad \text{in } \langle x \rangle$$

There are $\phi(10) = 4$ of them, as Theorem 4.4 predicts. All four lie in $\langle 4 \rangle = \{0, 4, 8, \ldots, 36\}$, the unique subgroup of order 10, and they are exactly its generators.

$\mathbb{Z}_{40}$: 4, 12, 28, 36. $\langle x \rangle$: x^4, x^{12}, x^{28}, x^{36}.