

Answer key No.1 to selected homework problems: Math. 110B

7.1

2. A permutation f either fixes one number $1 \leq j \leq 3$ or two numbers or moves all. There are 3 elements fixing only one number (those interchanging the two numbers different from j). For such f , $f \circ f = I$. There is only one which fixes two numbers; so, it fixes actually all three numbers 1, 2, 3, that is, I . Take f which moves all. Then $f(1) = i$ and $i \neq 1$. If $f(i) = 1$, then f interchanges 1 and i ; so, f fixes the rest j with $j \neq 1$ and $j \neq i$. This is impossible because f moves all. Thus we conclude that $f(i) = j$ and $j \neq i$ and $j \neq 1$. In other words, $f = \begin{pmatrix} 1 & i & j \\ i & j & 1 \end{pmatrix}$. The choice of i and j are either $(i, j) = (2, 3)$ or $(i, j) = (3, 2)$; so, there are two elements with $f \circ f \circ f = I$ (which can be verified by the above shape of f). In conclusion, there are 3 elements $g \in S_3$ with $g \circ g = I$, and there are two elements f with $f \circ f \circ f = I$; the rest is I itself.
2. (a) $|\mathbb{Z}_{18}| = 18$;
 (b) $|D_4| = 8$, four rotations (including the identity), one flip after a rotation (see Example in page 164-167).
 (c) $4!$: number of 4-permutations;
 (d) $5!$: number of 5-permutations;
 (e) By Theorem 2.11, non-units of \mathbb{Z}_n are zero-divisors, which are multiples of proper divisors of $n = 0$ (here “proper divisor $d|n$ ” means $1 < d$). When $n = 18$, proper divisors are: 2, 3, 6, 9, 18. Remove all multiples of the above numbers out of integers 1 to 18 = 0, remaining ones are 1, 5, 7, 11, 13, 17; so, $|U_{18}| = 6$.
4. (a) Yes. Consider $\pi : \mathbb{Z}_{10} \rightarrow \mathbb{Z}_5$ given by $\pi(x) = x \pmod{5}$. Check this is a homomorphism of rings. Then $\pi : \{2, 4, 6, 8\} \rightarrow U_5$ is one-to-one and onto. The product is just a product of U_5 . Since we know that U_5 is a group; so, $\{2, 4, 6, 8\}$ is also a group.
 (b) Yes, because $2^{x+y} = 2^x 2^y$. Consider a function $f : \mathbb{Q} \rightarrow G$ given by $f(x) = 2^x$. Then f is one-to-one and onto. Moreover $f(x+y) = f(x) * f(y)$. Since \mathbb{Q} with addition $+$ is a group, $(G, *)$ is a group (the structure of $(G, *)$ is identical with $(\mathbb{Q}, +)$ via f).
 (c) No. $6 \in G$ does not have inverse in G .
 (d) Yes. Check associative law:

$$\begin{aligned} (a * b) * c &= (a + b - ab) * c = (a + b - ab + c) - (a + b - ab)c \\ &= (a + b + c - bc) - a(b + c - bc) = a * (b + c - bc) = a * (b * c). \end{aligned}$$

The identity exists:

$$a * b = b \Rightarrow a + b - ab = b \Rightarrow a(1 - b) = 0 \xrightarrow{b \neq 1} a = 0.$$

Thus $a = 0$ is the identity. Inverse exists:

$$a * b = 0 \Rightarrow a + b - ab = 0 \Rightarrow b = \frac{-a}{1 - a} \in G,$$

because $a \neq 1$. Actually defining $f : \mathbb{Q} \rightarrow \mathbb{Q}$ by $f(x) = 1 - x$, then $f(a * b) = 1 - (a + b - ab) = (1 - a)(1 - b) = f(a)f(b)$. $f(0) = 1$. This shows the group structure of G and $(\mathbb{R}^\times, \times)$ are identical by one-to-one onto function f . Here \mathbb{R}^\times is the number line 0 removed (the unit group of the ring \mathbb{R}).

(e) Yes. Consider $f : \mathbb{R} \rightarrow \mathbb{R}$ by $f(x) = x + 1$. Then $f(a * b) = f(a + b + ab) = a + b + ab + 1 = (a + 1)(b + 1) = f(a)f(b)$ and $f(-1) = 0$. Thus the group structure of $(G, *)$ and the group structure of $(\mathbb{R}^\times, \times)$ are identical via the one-to-one onto function f .

(f) Yes. By the condition $cd = 0$, the complex numbers in G are either real or purely imaginary (that is, $r\sqrt{-1}$ for real numbers r). Since $c + d \neq 0$, $0 \in \mathbb{C}$ is removed. Since product of real or purely imaginary numbers stay in real or purely imaginary, G is a group with identity 1.

There is another way to see that G is a group: Since every element of G can be written uniquely as $r\zeta$ with $\zeta \in \{\pm 1, \pm i\}$ for a positive real number r , we define $f : \mathbb{R}_+ \times \{\pm 1, \pm i\} \rightarrow G$ by $f(r, \zeta) = r\zeta$. Then verify $f((x, \zeta)(y, \xi)) = f(x, \zeta)f(y, \xi)$, $f(1, 1) = 1$ and f is one-to-one and onto. Here \mathbb{R}_+ is the set of positive real numbers (which is a group with identity 1 under multiplication). The four element set $\{\pm 1, \pm i\}$ is also a group under multiplication (see Example in page 169). Thus the set G with multiplication is identical to the group $\mathbb{R}_+ \times \{\pm 1, \pm i\}$ by f , and hence G is a group (see Theorem 7.4).

5. For every element $r \in R$, $r0_R = 0_R$. Since R is not a zero ring, $1_R \neq 0_R$; thus, 0_R does not have multiplicative inverse; so, (R, \times) is not a group.
6. Hint: Just proceed as in the solution of Problem 3 (e).
8. We add the zero matrix to G and form a set $R = G \cup \{0\}$. Then as seen in Examples in page 47-48, R is a commutative ring. Define $f : R \rightarrow \mathbb{C}$ by $f\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\right) = a - b\sqrt{-1}$. Then as seen in the example in page 69, f is an isomorphism of rings. In particular, f induces a one-to-one onto function from G to \mathbb{C}^\times . Since $f(AB) = f(A)f(B)$, $f(1_2) = 1$ for the 2×2 identity matrix 1_2 and $f(A^{-1}) = f(A)^{-1}$, the group G is identical to the group $(\mathbb{C}^\times, \times)$. Thus G is an abelian group.
10. Composition of functions are associative; so, we need to check the existence of inverse and the identity. The identity map I obviously satisfies $I \circ f = f \circ I = f$; so, it gives the identity of $A(T)$. Since f is a permutation; so, it is onto and one-to-one. Thus for each given $y \in T$, there is a unique $x \in T$ so that $f(x) = y$. Define $g(y) = x$. Then $g \circ f(x) = g(y) = x$ and $f \circ g(y) = f(x) = y$. This shows that g is the inverse of f .
11. (a) Group of order 30: D_{15} , $D_5 \times \mathbb{Z}_3$, $D_3 \times \mathbb{Z}_5$ (which is identical to $S_3 \times \mathbb{Z}_5$).
Group of order 48: $S_4 \times \mathbb{Z}_2$, $D_{24} \dots$
- (b) $\{\pm 1\} \times \{\pm 1\}$ (under multiplication), $\mathbb{Z}_2 \times \mathbb{Z}_2$ (under addition).
12. Let α be any rigid motion. Write S for the square. Suppose that one face of S is colored to be red and the other white. At the beginning, we assume that red side is shown (face up). If $\alpha(S)$ has white face, apply flip (reflection) d so that face of $d\alpha(S)$ is red. Suppose j is the number of the

left corner of $d\alpha(S)$. Then turn around $d\alpha(S)$ by a rotation r to bring j to 1. Then $rd\alpha(S)$ is at the original position; so, $rd\alpha = r_0$; in other words, $\alpha = d^{-1}r^{-1}r_0 = dr^{-1} \in D_4$. If the face of $\alpha(S)$ is red, just rotate back $\alpha(S)$ to the original position; so, $\alpha = r^{-1}$ for a rotation r . This shows D_4 are made of all rigid motions.

18. An element of S_n is determined by a sequence of numbers $1, 2, \dots, n$ without repetition. There are $n = n - 0$ choice to place number at the first spot. After filling the first spot, there remain $n - 1$ numbers; so, there are $n - 1 = n - (2 - 1)$ choices at 2nd spot. Repeating this process, there are $n - (j - 1)$ choice possible to fill j -th spot. In total $n \times (n - 1) \times \dots \times 1 = n!$ choices for such sequence. This tells us that $|S_n| = n!$.

7.2

7. (b) 7 because if we renumber $(7, 6, 4, 5)$ into $(4, 5, 6, 7)$, then the permutation brings $1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 5 \rightarrow 6 \rightarrow 7 \rightarrow 1$ just circling around 1 to 7; so, it returns to the identity after 7 operations.
11. Consider $n + 1$ elements a^0, a, a^1, \dots, a^n of G . Since there are only n distinct elements, at least two have to overlap; so, we find two integers i and j with $0 \leq i < j \leq n$ such that $a^j = a^i$. Then by exponent law (Theorem 7.7), for $m = j - i \leq n$, we have $a^m = e$.
12. The group of Exercise 11(b) in Section 7.1 has 4 elements but all elements has order ≤ 2 ; so, false.
13. (a) Let m be the order of a ; so, m is the smallest positive integer such that $a^m = e$. Then by DAG (division algorithm), $12 = mq + r$ with remainder $0 \leq r < m$. Then $e = a^{12} = a^{mq+r} = (a^m)^q a^r = ea^r = a^r$. Thus $a^r = e$. By the minimality of m and $0 \leq r < m$, we conclude $r = 0$ and hence $m|12$.
- (b) Let $m = |b|$. In the above argument, replacing 12 by p , we conclude $m|p$. Since p is a prime, we see that $|b| = 1$ or $|b| = p$. If $|b| = 1$, then $b = b^1 = e$, which is impossible since $b \neq e$. Thus $|b| = p$.
14. Let $b = a^m$ and $\ell = |b|$. Since $e = b^\ell = (a^m)^\ell = a^{m\ell}$. By DAG, $m\ell = 12q + r$ for $0 \leq r < 12$. Then $e = a^{m\ell} = a^{12q+r} = (a^{12})^q a^r = a^r$. By the minimality of $|a| = 12$, we find $r = 0$. Thus $12|m\ell$. Thus ℓ is the least number such that $12|m\ell$. In other words, $m\ell$ is the least common multiple (LCM) $[m, 12]$ of m and 12. Thus $|a^m| = \ell = \frac{[m, 12]}{m}$. In general, $|a^m| = \frac{[m, |a|]}{m}$. Here is the table of the values $|a^m|$:

m	1	2	3	4	5	6	7	8	9	10	11
$ a^m $	12	6	4	3	12	2	12	3	4	6	12

15. (a) Multiplying $ax = b$ by a^{-1} from the left, we get

$$x = ex = (a^{-1}a)x \stackrel{ASS}{=} a^{-1}(ax) = a^{-1}b.$$

Multiplying $ya = b$ by a^{-1} from the right, we get

$$y = ye = y(aa^{-1}) \stackrel{ASS}{=} (ya)a^{-1} = ba^{-1}.$$

Thus the solution to each equation is unique as determined above.

(b) Let $G = S_3$ and $a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ and $b = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$. Then $a^{-1} = a$ and

$$x = a^{-1}b = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = ba^{-1} = y.$$

19. Suppose first m and n both positive. Then

$$a^{m+n} = \overbrace{aa \cdots a}^{m+n} = \overbrace{aa \cdots a}^m \cdot \overbrace{aa \cdots a}^n = a^m a^n.$$

If m and n both negative, replacing a by a^{-1} , the above argument proves the result. If $m > 0$ and $n < 0$ with $m > |n|$, then the right $|n|$ of a^{-1} in

$$\underbrace{\overbrace{aa \cdots a}^m}_{m-|n|} \cdot \overbrace{a^{-1}a^{-1} \cdots a^{-1}}^{|n|}$$

is canceled out by the left $|n|$ of a , which yield $a^{m-|n|} = a^{m+n}$. When $m < |n|$, left m of a canceled out by right $|n|$ of a^{-1} , getting $(a^{-1})^{|n|-m} = a^{m+n}$. The assertion $(a^m)^n = a^{mn}$ can be similarly proven; so, do it yourself.

25. Take $a, b \in G$. Then multiplying $a^2 = e$ by a^{-1} , we get $a = a^2 a^{-1} = ea^{-1} = a^{-1}$. Similarly, $b = b^{-1}$. Then multiplying $abab = e$ by $ba = b^{-1}a^{-1}$ from the right, we get

$$ab = ab(abb^{-1}a^{-1}) = (abab)b^{-1}a^{-1} = e(b^{-1}a^{-1}) = ba.$$

27. The x is given by $a^{-1}cb^{-1}$.

29. (a) We have

$$\begin{aligned} (ab)^{|a||b|} &= \overbrace{abab \cdots ab}^{|a||b|} \stackrel{\text{comm}}{=} \overbrace{aa \cdots a}^{|a||b|} \cdot \overbrace{bb \cdots b}^{|a||b|} \\ &= a^{|a||b|} b^{|b||a|} = (a^{|a|})^{|b|} (b^{|b|})^{|a|} = e^{|b|} e^{|a|} = e. \end{aligned}$$

(b) Take $G = S_3$, $a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ and $b = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$. Then $ab = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, and $|a| = |b| = 2$ but $|ab| = 3$ as seen in Exercise 2 in Section 7.1.

31. We claim

$$\text{For } x \in G, \text{ if } x^n = e, \text{ then } |x| \mid n. \quad (*)$$

To see this, by DAG, $n = |x|q + r$ with $0 \leq r < |x|$. Then we see

$$e = x^n = x^{|x|q+r} = (x^{|x|})^q x^r = x^r.$$

By the minimality of $|x|$, $r = 0$. Thus $(*)$ holds.

Let $m = |ab|$. By $(*)$ applied to $x = ab$ and $n = |a||b|$, m is a factor of $|a||b|$ by Exercise 29 (a). Thus $m \leq |a||b|$. Since $e = (ab)^m = a^m b^m$, we find that $a^m = b^{-m}$. Thus

$$(a^m)^{|b|} = (b^{-m})^{|b|} = (b^{|b|})^{-m} = e,$$

which implies by $(*)$ (applied to $x = a^m$ and $n = |b|$) that $|a^m|$ is a factor of $|b|$. Similarly $(a^m)^{|a|} = e$, and hence $|a^m|$ is a factor of $|a|$. Thus $|a^m|$ is

a common divisor of $|a|$ and $|b|$, which has to be equal to 1, because $|a|$ and $|b|$ are relatively prime. Thus $a^m = e$ and hence $b^{-m} = e \Rightarrow b^m = e$. This implies m is divisible $|b|$. Similarly, $a^m = e$ implies that m is divisible by $|a|$. Thus m is divisible by $|a||b|$ because $|a|$ and $|b|$ are relatively prime. In particular, $|a||b| \leq m$. This combined with $m \leq |a||b|$ already shown, we conclude that $m = |a||b|$.

33. $|a^{-1}xa| = |x|$ because

$$(a^{-1}xa)^m = \overbrace{a^{-1}xaa^{-1}xa \cdots a^{-1}xa}^m = a^{-1} \overbrace{xxe \cdots ex}^m a = a^{-1}x^m a.$$

Thus $|b| = |a^{-1}b^4a| = |b^4| = \frac{[6,4]}{4} = 3$ by the argument in the solution of Exercise 14. Thus $b^3 = e$ and $b^4 = b^{3+1} = b$ and $ab = b^4a = ba$ as desired.

7.3

2. Consider $G = \mathbb{Z} \times \mathbb{Z}$. Then $H = \{(x, 0) | x \in \mathbb{Z}\}$ is a subring of G with identity $e_H = (1, 0)$, but e_H is a zero-divisor in G , because $e_H(0, 1) = (0, 0) = 0_G$. The identity of G is given by $(1, 1) = 1_G$.
4. (a) Take $G = \mathbb{Z}_2 \times \mathbb{Z}_2$. Then

$$H = \{(x, 0) | x \in \mathbb{Z}_2\} \text{ and } K = \{(0, x) | x \in \mathbb{Z}_2\}$$

are subgroups. But $H \cup K = \{(x, y) | x = 0 \text{ or } y = 0\}$ is not a subgroup, because $(1, 0) + (0, 1) = (1, 1) \notin H \cup K$.

- (b) If $H \subset K$, then $H \cup K = K$, which is a subgroup. Conversely, suppose that $x \in H - K$ and $y \in K - H$. If $xy \in H \cup K$, either $xy \in H$ or $xy \in K$. If $xy = h \in H$, then $y = x^{-1}h \in H$ contradicting $y \notin H$. If $xy = k \in K$, then $x = ky^{-1} \in K$ contradicting $x \notin K$. In any case, we find something wrong; so, this never happens; in other words, the product xy get out of $H \cup K$; so, it is not a group.

6. Since G is abelian, if $x, y \in H$, then $(xy)^k = x^k y^k = e$. Thus $|xy| |k|$ by (*) in the solution of Exercise 31 in Section 7.2. Since $|x^{-1}| = |x|$, $x \in H \iff x^{-1} \in H$. Also $|e| = 1$ implies $e \in H$. Thus H is a subgroup by Theorem 7.10.
9. (a) False. Look at D_4 . By Example in page 183, $Z(D_4) = \{r_0, r_2\}$. Then for $a = b = r_1 d$ and $ab = r_1 d r_1 d = r_1 r_1^{-1} d^2 = r_0 \in Z(D_4)$ but $a \notin Z(D_4)$.
- (b) Since $ab \in Z(G)$, $aba = (ab)a = a(ab) = aab$. Multiplying $aba = aab$ by a^{-1} from the left, we get

$$ba = eba = a^{-1}aba = a^{-1}aab = eab = ab.$$

10. Since $|x^{-1}ax| = |a| = 2$ (see Exercise 33 in Section 7.2), we have $x^{-1}ax = a$ by the uniqueness of order 2 element. Multiplying the equation $x^{-1}ax = a$ by x from the left, we get

$$ax = eax = xx^{-1}ax = xa.$$

Thus a commutes with all $x \in G$; so, $a \in Z(G)$.

12. (a) Order 2 cyclic subgroups: $\{r_0, r_2\}$, $\{r_0, d\}$, $\{r_0, t\}$, $\{r_0, h\}$, $\{r_0, v\}$.
Order 4 cyclic subgroups: $\{r_0, r_1, r_3, r_4\}$.
(b) The subgroup $\{r_0, d, dr_2, r_2\}$ is order 4 but $|d| = |r_2| = |dr_2| = 2$; so, non-cyclic.
15. False. Any proper subgroup of D_3 is cyclic of order 2 or 3, but D_3 is non-abelian; in particular, non-cyclic.
18. Need to show that 1 generates \mathbb{Z} and 2 generates \mathbb{Z}_7 . Since any integer is a multiple of 1, the first claim is plain. Since 2 and 7 are relatively prime, for any given integer b , $2x \equiv b \pmod{7}$ has solution (LET); in other words, every $b \in \mathbb{Z}_7$ is a multiple of 2; so, 2 generates \mathbb{Z}_7 .
19. If x is a generator of \mathbb{Z} , then any integer $b \in \mathbb{Z}$ is a multiple of x ; so, in particular $11 = xy$ for some $y \in \mathbb{Z}$. In other words, x is a unit in \mathbb{Z} ; thus, $x \in \{\pm 1\}$.
21. We see

m	0	1	2	3	4	5
$m(1,1)$	(0,0)	(1,1)	(0,2)	(1,0)	(0,1)	(1,2)

Thus $m(1, 1)$ exhaust all elements of $\mathbb{Z}_2 \times \mathbb{Z}_3$; so, the group is cyclic.

There is another way of showing this: $a = (1, 0)$ has order 2, and $b = (0, 1)$ has order 3; so, by the solution of Exercise 31 in Section 7.2, $a + b = (1, 1)$ has order $|a||b| = 6$, and hence the group is cyclic.

25. We use the criterion in Exercise 23. If $x, y \in C(a)$, then $xa = ax \iff ax^{-1} = x^{-1}a$ and $ya = ay \iff ay^{-1} = y^{-1}a$. We then see $xy^{-1}a = xay^{-1} = axy^{-1}$. Thus $xy^{-1} \in C(a)$, and hence $C(a)$ is a subgroup.
33. If $x \in H$, then for any $h \in H$; so, $x^{-1}hx \in H$ (H is closed under group operation). Thus $x^{-1}Hx \subset H$. Replacing x by x^{-1} which is still in H , we find $xHx^{-1} \subset H$. Multiplying the equation $xHx^{-1} \subset H$ by x^{-1} from the left and x from the right, we get $H \subset x^{-1}Hx$. This combined with $x^{-1}Hx \subset H$ we have seen at the beginning, we conclude $H = x^{-1}Hx$; and hence $x \in N_H$ for all $x \in H$. Thus $H \subset N_H$.

We are going to see that N_H is a subgroup of G . We shall apply the criterion of Exercise 23. If $x \in N_H$, then $x^{-1}Hx = H$. Multiplying the equation $x^{-1}Hx = H$ by x from the left and x^{-1} from the right, we get $H = xHx^{-1}$; so, $x^{-1} \in N_H$. If $y \in N_H$, then $y^{-1}Hy = H$. Multiplying the equation $y^{-1}Hy = H$ by x from the left and x^{-1} from the right, we get $H = xy^{-1}Hyx^{-1} = (yx^{-1})^{-1}Hyx^{-1}$ (note that $(ab)^{-1} = b^{-1}a^{-1}$); so, $yx^{-1} \in N_H$; thus, N_H is a subgroup containing H .

37. If $G = \langle g \rangle$ is a cyclic group of order m , then for any divisor $d|m$, $|g^{m/d}| = d$; thus, it has a unique (cyclic) subgroup of order d . The generator of \mathbb{Z}_{20} is 1; so,

d :divisor of 20	cyclic subgroup of order d
1	$\{0\}$
2	$\{0, 10\}$
4	$\{0, 5, 10, 15\}$
5	$\{0, 4, 8, 12, 16\}$
10	$\{0, 2, 4, 6, 8, 10, 12, 14, 16, 18\}$
20	\mathbb{Z}_{20}

For \mathbb{Z}_{12} , one can list in the same way all subgroups (do it yourself).

7.4

3. (b) See the back of the book for a hint.

Here we give another argument. 2×2 matrices with non-zero determinant permutes non-zero column vectors $v = \begin{pmatrix} x \\ y \end{pmatrix}$ by matrix multiplication:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax+by \\ cx+dy \end{pmatrix}.$$

There are three non-zero column vectors with entries in \mathbb{Z}_2 : $v_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $v_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ and $v_3 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$. For each matrix $\alpha \in GL(2, \mathbb{Z}_2)$, define a permutation $f(\alpha)$ by $\begin{pmatrix} 1 & 2 & 3 \\ i & j & k \end{pmatrix}$ if $\alpha v_1 = v_i$, $\alpha v_2 = v_j$ and $\alpha v_3 = v_k$. Check yourself that $f(\alpha\beta) = f(\alpha)f(\beta)$ in S_3 . If $f(\alpha) = f(\beta)$, noting the fact that $(\alpha v_1, \alpha v_2) = \alpha$ as 2×2 matrices, we know that $\alpha = \beta$; so, f is an injective homomorphism. Since $|S_3| = |GL(2, \mathbb{Z}_2)| = 6$, f has to be onto; so, it is an isomorphism.

4. $U_5 = \langle 2 \rangle$ is cyclic of order 4; so, define $f : U_5 \rightarrow \mathbb{Z}_4$ taking 2^i to i , we find f is a surjective homomorphism (check yourself that f is a homomorphism). Since the target and source have the same number of elements 4, f has to be an isomorphism.
5. Note that $U_{10} = \{1, 3, 7, 9\} = \langle 3 \rangle$ because $3^2 \equiv 9 \pmod{10}$ and $3^3 \equiv 7 \pmod{10}$. Then again define $f : U_{10} \rightarrow \mathbb{Z}_4$ by $f(3^i) = i$. Check yourself that f is an isomorphism of groups.
26. U_7 is a cyclic group with generator 3, because $3^2 \equiv 2 \pmod{7}$, $3^3 \equiv 6 \pmod{7}$, $3^4 = 81 \equiv 4 \pmod{7}$ and $3^5 \equiv 4 \cdot 3 \equiv 5 \pmod{7}$ and $3^6 \equiv 1 \pmod{7}$. Then $f : U_7 \rightarrow \mathbb{Z}_6$ given by $f(3^i) = i$ gives rise to an isomorphism (check yourself).
7. See the solution of Exercise 4(d) for the isomorphism.
8. See the solution of Exercise 4(e) for the isomorphism.
9. Easy. Prove for yourself.
10. For each $x, y \in H$, take $a, b \in G$ so that $f(a) = x$ and $f(b) = y$. Then we see

$$xy = f(a)f(b) = f(ab) = f(ba) = f(b)f(a) = yx.$$

Thus H is abelian.

13. (a) We see $(a^{-1}ga)^{-1} = a^{-1}g^{-1}a$ (note that $(xy)^{-1} = y^{-1}x^{-1}$). Thus if $x, y \in a^{-1}Ha$, we can write $x = a^{-1}ha$ and $y = a^{-1}ga$ for $h, g \in H$. Then $xy^{-1} = a^{-1}haa^{-1}g^{-1}a = a^{-1}hg^{-1}a$. Since H is a subgroup, $hg^{-1} \in H$; so, $xy^{-1} \in a^{-1}Ha$. This shows that $a^{-1}Ha$ is a subgroup.
- (b) Define a function $f : H \rightarrow a^{-1}Ha$ by $f(x) = a^{-1}xa$. Show that f is one-to-one and onto; so, $|H| = |a^{-1}Ha|$.
15. The direction: (\Rightarrow) is easy; so, prove it yourself. We suppose that $f : G \rightarrow G$ with $f(x) = x^{-1}$ is a homomorphism. Since $f(x^{-1}) = (x^{-1})^{-1} = x$, f is surjective. Then we have

$$xy = f(x^{-1})f(y^{-1}) = f(x^{-1}y^{-1}) = f((yx)^{-1}) = yx.$$

This shows that G is abelian. If $f(x) = f(y)$, then $x = f(f(x)) = f(f(y)) = y$; so, f is injective. Thus f is an isomorphism.

18. Need to show that all $h \in H$ is a power of $f(a)$. Since f is surjective, $h = f(g)$ for $g \in G$. Since G is cyclic, $g = a^n$. Then $h = f(g) = f(a^n) = f(a)^n$ by Exercise 11.
19. Since every $g \in G$ is a power of b ; so, $g = b^i = f(a^i)$; therefore, f is surjective. If G is finite, then surjectivity implies injectivity. If G is infinite, then $b^i = b^j$ implies $i = j$. In particular, if $f(g) = f(h)$ for $g = a^i$ and $h = a^j$, then $b^i = f(g) = f(h) = b^j$, and hence $i = j$. This shows that f is injective. To show f is a homomorphism, we compute $f(gh) = f(a^i a^j) = f(a^{i+j}) = b^{i+j} = b^i b^j = f(g)f(h)$ by the exponent law (EL: Theorem 7.7). Thus f is an automorphism.
20. Label elements in T as $1, 2, \dots, n$. Then any $f : T \rightarrow T \in A(T)$ induces a permutation $i(f) = \begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix}$. The permutation $i(f)$ determines f because it contains all the information on the value of f ; so, $i : A(T) \rightarrow S_n$ is injective. For any given permutation $\alpha = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$, defining $f(j) = i_j$, we get $f \in A(T)$ such that $i(f) = \alpha$; so, i is surjective. The verification that i is a homomorphism is left to you.
22. We need to check that f^{-1} is a homomorphism. By definition $f^{-1}(f(x)) = x$. Then $f(xy) = f(x)f(y)$ implies $xy = f^{-1}(f(x)f(y))$. Writing $x' = f(x)$ and $y' = f(y)$, we have $f^{-1}(x') = x$ and $f^{-1}(y') = y$; so, the above identity means that $f^{-1}(x'y') = xy = f^{-1}(x')f^{-1}(y')$. Thus f^{-1} is a homomorphism on the image of f . Since f is surjective, the image is actually the entire H ; so, it is done.
24. By Exercise 9, composition of two automorphisms is a homomorphism. Check yourself that composition of surjections is surjection and that composition of injections is injection. So composition of two automorphisms is an automorphism. By Exercise 22, f^{-1} is again automorphism; so, $f \circ f^{-1} = f^{-1} \circ f$ is the identity map 1_G which does not move any element of G . Note that $f \circ 1_G(x) = f(x)$ and $1_G \circ f(x) = 1_G(f(x)) = f(x)$; so, 1_G gives the identity of $\text{Aut}(G)$ and f^{-1} gives the inverse of $\text{Aut}(G)$. Since composition of functions is associative, $\text{Aut}(G)$ is a group.
25. Conjugation $f_g(x) = g^{-1}xg$ is a homomorphism, because

$$f_g(x)f_g(y) = g^{-1}xgg^{-1}yg = g^{-1}xeyg = g^{-1}xyg = f_g(xy).$$

It is a surjection because $x = f_g(gxg^{-1})$. It is an injection because $f_g(x) = f_g(y) \Rightarrow g^{-1}xg = g^{-1}yg \Rightarrow x = y$ by multiplying g from the left and g^{-1} from the right. Thus f_g is an element in $\text{Aut}(G)$. Check yourself that $f_g \circ f_h = f_{gh}$. Thus $g \mapsto f_g$ gives rise to a homomorphism: $G \rightarrow \text{Aut}(G)$. The image is $\text{Inn}(G)$. Image of a homomorphism is a subgroup (see Theorem 7.19 (3)).

28. (a) \mathbb{Z}_6 is abelian but S_3 is non-abelian (give a concrete example of two elements in S_3 which do not commute).
- (b) $\mathbb{Z}_4 \times \mathbb{Z}_2$ is abelian but D_4 is not.
- (c) $\mathbb{Z}_4 \times \mathbb{Z}_2$ has an element of order 4 (that is, $(1, 0)$), but all elements of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ is killed by 2; so, their order is ≤ 2 .

- (d) Any number in \mathbb{R} is a twice of a real number, but it is not the case for \mathbb{Z} (for example, 1 is not $2x$ for $x \in \mathbb{Z}$).
35. (b) We check that $\theta_c \circ \theta_d(x) = \theta_c(xd^{-1}) = xd^{-1}c^{-1} = x(cd)^{-1} = \theta_{cd}(x)$. Thus $c \mapsto \theta_c$ is a homomorphism of G into $A(G)$ (θ_c is one-to-one and onto as verified in (a)). Thus G is isomorphic to its image in $A(G)$.

7.5

2. (a) $\{r_0, v\}, \{r_0, v\}d = \{d, r_1\}, \{r_0, v\}h = \{h, r_2\}, \{r_0, v\}t = \{t, r_3\}$.
 (c) $K, K \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \{ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \}, K \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \{ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \}$.
3. Hint: Index $[G : H] = \frac{|G|}{|H|}$.
4. $|a^3| = 5$; thus $|H| = 5$. This shows $[G : H] = \frac{15}{5} = 3$; so, there are three cosets: $H, Ha = \{a, a^4, a^7, a^{10}, a^{13}\}, Ha^2 = \{a^2, a^5, a^8, a^{11}, a^{14}\}$.
7. For a prime power p^m , the cyclic group \mathbb{Z}_{p^m} of order p^m has a (unique) cyclic subgroup of order p^j (for $j = 0, 2, \dots, m$) and it has no other subgroups. Thus \mathbb{Z}_{p^m} is the smallest group having subgroups of order p^j for all $j = 0, 1, \dots, m$ (because if there are more than one subgroup of such order, group has to get bigger). To have subgroup of all order between 1 to 12, we therefore list maximal prime powers from 1 to 12: that is, $8 = 2^3, 9 = 3^2, 5, 7, 11$. Thus the desired group is $\mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \times \mathbb{Z}_7 \times \mathbb{Z}_{11}$, which has order $27720 = 8 \cdot 9 \cdot 5 \cdot 7 \cdot 11$. For example, the subgroup of order 12 is given by $(2\mathbb{Z}_8) \times (3\mathbb{Z}_9)$, where $2\mathbb{Z}_8$ is the subgroup of order 4 in \mathbb{Z}_8 generated by 2, and similarly $3\mathbb{Z}_9$ is the subgroup of order 3 in \mathbb{Z}_9 generated by 3.
8. The smallest of such group has to be cyclic by the argument in the solution of Exercise 7. In that case, the order has to be divisible by 10 and 25, the smallest is the LCM $50 = [10, 25]$. Thus it is the cyclic group of order 50, that is, \mathbb{Z}_{50} . It has subgroup of order 25 generated by 2 and the subgroup of order 10 generated by 5.
10. $H \cap K$ is a subgroup of H and also of K by Exercise 3 of Section 7.3. Then by Lagrange's theorem, the assertion follows.
11. If an element a has composite order mn ($m > 1$ and $n > 1$), then the cyclic subgroup $\langle a \rangle$ has to have a subgroup of order m and n (Theorem 7.8 (4)). This is impossible by the assumption; so, all elements of G has prime order. If we have two distinct elements with different prime order p and q , G has to have two distinct subgroups of order p and q respectively. So all elements other than the identity has prime order p . One such element a generates G ; otherwise, G has two distinct subgroup of order p . Then G is cyclic of order p . Thus by Theorem 7.28, G is isomorphic to \mathbb{Z}_p . The isomorphism is given by $\mathbb{Z}_p \ni i \mapsto a^i \in G$.
13. Hint. Compute $|a^4|$ (see the solution of Exercise 14 of Section 7.2).