Instructor's Manual
for

Algebra
Pure & Applied

Aigli Papantonopoulou
The College of New Jersey

First Printing Errors

Please make the indicated corrections in the following exercises:

Section 3.1: **Exercise 9**: $\mathbb{Z}_4 \times \mathbb{Z}_6$ find two subgroups H and K of order 4 such that H is not isomorphic to K, but $(\mathbb{Z}_4 \times \mathbb{Z}_6) / H \cong (\mathbb{Z}_4 \times \mathbb{Z}_6) / K$

Section 3.4: **Exercise 7**: $n = 36$

Section 4.1: line 8 . . . Let G act on X . . .

Exercise 18: Let $1 < i = [G : H]$ be the index of H in a finite group G .

Section 4.4: **Exercise 15**: Let G be a finite group . . .

Exercise 21: Explain why for any $g \in G$, the group G and the centralizer $C(g)$ are equal if and only if $g \in Z(G)$.

Section 5.1: **Exercise 12**: Let $K \lhd G$ with $|G|$ finite. Let H be a subgroup of G such that $[G : H]$ and $|K|$ are relatively prime . . .

Section 5.3: **Exercise 16**: Let H be a non trivial normal subgroup of A_n , $n \geq 6$. Assume that A_{n-1} is simple. Show that $G_i \leq H$, where $G_i = \{ \rho \in A_n \mid \rho(i) = i \}$, for some $1 \leq i \leq n$.

Exercise 19: Show that if G is a finite solvable group . . . .

Section 6.3: **Exercise 41**: . . . for every nonzero element $a \in R$ there exists . . .

Section 7.2: **Exercise 25** (d): If R is a commutative ring with unity . . .

Exercise 28 (b): If J is a maximal ideal in $\varphi(R)$ . . .

Section 8.8: **Exercise 8** and **Exercise 9**: Let R be a commutative ring with unity . . .

Section 10.3: **Exercise 13**: Prove Proposition 10.3.10,

Exercise 14 : . . . as in Example 10.3.11

Section 10.4: **Exercise 23** (b): Use (a) to show that if r divides n, then $p^r - 1$ divides $p^n - 1$.)

Section 11.1: **Exercise 20**: $f(x) = x^4 - x^2 + 1/8$,

Exercise 21: $f(x) = x^4 + 2x - 2$

Section 11.3: **Exercise 1** (b): By a substitution reduce $f(x) = 0$ to the form $g(y) = y^3 - 3y - \sqrt{7}/7 = 0$.

Section 11.4: **Exercise 12** (b) If $(q/2)^2 + (p/3)^3 < 0$ . . . ,

Exercise 13: . . . with square roots and angle trisections are those with three real zeros . . .

Section 12.5: **Exercise 5**: $x^5 - x^4 + x - 1$,

Exercise 17: $x^5 + x^4 + x^3 - 2x^2 - 2x - 2$

Exercise 18: Let $f(x) \in \mathbb{Q}[x]$ be an irreducible quintic over $\mathbb{Q}$ with exactly two nonreal zeros... (b) For any field $F \neq K$, $F \neq E$ with ...

Chapter 16: **Exercise 28**: . . . where B is an $(n - r) \times (n - k) = k \times r$ matrix . . .

Exercise 33: Show that a (6, 3) linear binary code could correct . . .

Chapter 0

Background

0.1 Sets and Maps

The notions of one to one, onto and invertible maps may be already in the background of many students. One of the aims of this section though is to make the introduction of permutations in Chapter 1 much easier. Theorem 0.1.15, Proposition 0.1.17, Theorem 0.1.20 and Theorem 0.1.24 allow us in Chapter 1 to immediately see that the set of permutations S_n is a group. The notion of cardinality of a set is also introduced here as an appropriate example and is used throughout the text.

Exercises 0.1

1. Yes. $5u + 3 = 5v + 3$ implies $5u = 5v$ and $u = v$ in $\mathbb{R}$.

2. Yes. $e^u = e^v$ implies $u = ln\, e^u = ln\, e^v = v$.

3. Yes. $u^3 = v^3$ implies $u = (u^3)^{1/3} = (v^3)^{1/3} = v$.

4. No. $(-2)^2 = (2)^2$.

5. Yes. If $m/n = u/v$ then $mv = un$ which implies $v/u = n/m$.

6. No. $(-2)^4 = (2)^4$.

7. No. $\phi(0,1) = 0 = \phi(0,2)$.

8. Yes. For $b \in \mathbb{R}$ consider $a = e^b$. Then $ln\, a = ln\, e^b = b$.

9. No. $\phi(x) \geq -4$.

10. Yes. ϕ is one to one and $\phi(1)$, $\phi(2)$, $\phi(3)$, $\phi(4)$ are all distinct.

11. (1) Let $\rho_0 : A \to A$ be the identity map. $\rho_0(u) = u$ and $\rho_0(v) = v$.
Therefore, $\rho_0(u) = \rho_0(v)$ implies $u = v$ and given any $b \in A$ we have $b = \rho_0(b)$.
(2) For any $a \in A$, we have $\phi \circ \rho_0 (a) = \phi (\rho_0 (a)) = \phi (a)$.
(3) For any $b \in B$, we have $\rho_0 \circ \phi(b) = \rho_0 (\phi(b)) = \phi (b)$.

12. No. $\phi(0) = 1 = \phi(-2)$.

13. Yes and $\phi^{-1}(x) = (2x - 3)/5$.

14. Yes and $\phi^{-1}(i) = i - 2$ for $3 \le i \le n$, $\phi^{-1}(2) = n$ and $\phi^{-1}(1) = n - 1$.

15. (a) Suppose $\chi \circ \phi$ is onto. Then for any $c \in C$ there exists an $a \in A$ such that $c = \chi(\phi(a))$. Let $b = \phi(a) \in B$, then $c = \chi(b)$.
(b) Suppose $\phi(u) = \phi(v)$. Then $\chi(\phi(u)) = \chi(\phi(v))$ and this implies $u = v$ when $\chi \circ \phi$ is one to one.

Exercises 16, 17 and 18 illustrate the fact that if two maps ϕ and ψ are one to one and onto then so is the map (ϕ,ψ) on the Cartesian products. One may add this as a separate exercise.

16. Let ϕ: $\mathbb{Z} \to 2\mathbb{Z}$ be the one to one and onto map defined by $\phi(x) = 2x$ and let $\chi : \mathbb{Z} \times \mathbb{Z} \to 2\mathbb{Z} \times 2\mathbb{Z}$ be the map defined by $\chi(a, b) = (\phi(a), \phi(b)) = (2a, 2b)$. Then χ is one to one because if $\chi(a, b) = \chi(u, v)$, then $\phi(a) = \phi(u)$, $\phi(b) = \phi(v)$ and $a = u$, $b = v$ since ϕ is one to one. Finally, χ is onto because for any $(2k,2l)$ in $2\mathbb{Z} \times 2\mathbb{Z}$ we have $\chi(k,l) = (2k,2l)$.

17. If $|A| = n$ then there exists a one to one and onto map $\phi : \{1,2,3,...,n\} \to A$. So let $A = \{a_1, a_2, a_3,..., a_n\}$, where $a_i = \phi(i)$ and let $X = \{ (i, j) \mid 1 \le i, j \le n\}$. Then $|X| = n^2$ and $\chi : X \to A \times A$ defined by $\chi(i, j) = (\phi(i), \phi(j)) = (a_i, a_j)$ is one to one and onto since ϕ is .

18. If $|A| = |B|$ and $|C| = |D|$, then there exist one to one and onto maps $\phi : A \to B$ and $\psi : C \to D$. Hence $\chi : A \times C \to B \times D$, defined by $\chi(a, c) = (\phi(a), \psi(c))$, is one to one and onto.

0.2 Equivalence Relations and Partitions

Equivalence relations and equivalence classes are fundamental notions that play an important role throughout the text. For many students the notions of quotient groups and quotient rings are very difficult to work with. Theorem 0.2.4 is used in Chapter 2 where cosets are seen as equivalence classes and in this way the proof of Lagrange's theorem becomes easier. In Chapter 7 again where quotient rings are introduced Theorem 0.2.4 is needed.

Exercises 0.2

1. Yes. (1) $|a| = |a|$, (2) $|a| = |b|$ implies $|b| = |a|$, (3) $|a| = |b|$ and $|b| = |c|$ implies $|a| = |c|$. The equivalence classes are $\{a,- a\}$ for all $a \in \mathbb{R}$.

2. No. For example, $1 \sim 2$ holds but $2 \sim 1$ is false.

3. Yes. (1) $a - a$ is even , (2) if $a - b$ is even, so is $b - a$, (3) if $a - b = 2k$ and $b - c = 2l$ for some integers k and l, then $a - c = (a - b) + (b - c) = 2(k + l)$. There are two equivalence classes, namely $2\mathbb{Z}$ = the even integers and $1 + 2\mathbb{Z}$ = the odd integers.

4. No. $|2 - 3| \le 1$ and $|3 - 4| \le 1$ but $|2 - 4| > 1$.

5. Yes. (1) $a - a$ is a multiple of 3, (2) if $a - b$ is a multiple of 3, so is $b - a$, (3) if $a - b = 3k$ and $b - c = 3l$ for some integers k and l, then $a - c = 3(k + l)$. In this case there are three equivalence classes, namely $3\mathbb{Z}$ = {all multiples of 3}, $1 + 3\mathbb{Z}$ = {1 + any multiple of 3} and $2 + 3\mathbb{Z}$ = {2 + any multiple of 3}.

Exercise 6 should be assigned together with Exercise 11 for students to realize the difference between the two examples.

6. Yes. (3) Suppose $x_1y_2 = x_2y_1$ and $x_2y_3 = x_3y_2$. If $x_1 = 0$, then $y_1 \neq 0$ and the first equation implies $x_2 = 0$. In this case $y_2 \neq 0$ and the second equation implies $x_3 = 0$. Thus if $x_1 = 0$, we obtain $x_1y_3 = x_3y_1$. If $x_1 \neq 0$, then $x_2 \neq 0$ and $x_3 \neq 0$, the two equations imply $y_1 / x_1 = y_2 / x_2 = y_3 / x_3$ and $x_1y_3 = x_3y_1$. The equivalence classes are all the straight lines through the origin with the origin removed.

7. Yes. $(x_1,y_1) \sim (x_2,y_2)$ if and only if they are on the same circle centered at the origin.

8. Yes. The equivalence classes are all the parallel lines with slope 5/3.

9. (3) if $x \sim y$, then $x \in [n]$ and $y \in [n]$ for some integer n and if $y \sim z$ then $y \in [m]$ and $z \in [m]$ for some integer m. Since $y \in [n] \cap [m] \neq \varnothing$, the two equivalence classes are equal. Hence $n = m$ and $x \sim z$.

10. $[n + 2] = (n, n + 2] = \{x \in \mathbb{R} \mid 0 < x - n \le 2\}$. For any $x \in \mathbb{R}$ we have $x \in [n + 2]$, where n is the greatest even integer such that $n < x$ and $[n + 2] \cap [m + 2] = \varnothing$ is equivalent to $n = m$.

11. $(1, 2) \sim (0, 0)$ and $(1, 3) \sim (0, 0)$ even though $(1, 2)$ and $(1, 3)$ are not equivalent. The origin would belong to every equivalence class and this contradicts Theorem 0.2.4 .

12. (1) $n \mid a - a = 0$, (2) if $n \mid a - b$, then $n \mid -(a - b) = b - a$, (3) if $a - b = kn$ and $b - c = ln$ for some integers k and l, then $a - c = (k + l)\, n$.

13. (1) $\phi(a) = \phi(a)$, (2) $\phi(a) = \phi(b)$ is equivalent to $\phi(b) = \phi(a)$, (3) $\phi(a) = \phi(b)$ and $\phi(b) = \phi(c)$ imply $\phi(a) = \phi(c)$.

0.3 Properties of $\mathbb{Z}$

The Binomial theorem, Theorem 0.3.8, is used repeatedly and students should be familiar with it. The Division Algorithm and the Euclidean Algorithm for $\mathbb{Z}$, Theorem 0.3.11 and Proposition 0.3.18, are used as models in Chapter 8 for the corresponding theorems for $F[x]$. The last part of this section on integers mod n does all the necessary ground work for the introduction in Chapter 1of the groups $\mathbb{Z}_n$ and $U(n)$, the group of units mod n .

Exercises 0.3

1. For $n = 1$, the LHS = 1 and the RHS = 1 (1 + 1) / 2 = 1. Assume true for $n = k$. Then $1 + 2 + ...+ k + (k + 1) = [k(k + 1) / 2] + (k + 1) = (k + 1)(k + 2) / 2$.

2. For $n = 1$, the LHS = 1 and the RHS = $1(1 + 1)(2 + 1 / 6 = 1$. Assume true for $n = k$. Then $1^2 + 2^2 + ... + k^2 + (k + 1)^2 = [k(k + 1)(2k + 1) / 6] + (k + 1)^2 = (k + 1)[k(2k + 1) + 6(k + 1)] / 6 = (k + 1)(k + 2)(2k + 3) /6$.

3. For $n = 1$, the LHS = 1 and the RHS = $1^2(1 + 1)^2 / 4 = 1$. Assume true for $n = k$. Then $1^3 + ... + k^3 + (k + 1)^3 = [k^2(k + 1)^2 /4] + (k + 1)^3 = (k + 1)^2[k^2 + 4(k + 1)] / 4 = (k + 1)^2(k + 2)^2 / 4$.

4. For $n = 0$ the inequality holds. Assume true for $n = k$. Then $x^k \le y^k$ and since $0 \le x \le y$ we have $x^{k+1} = x^k . x \le y^k . x \le y^k . y = y^{k+1}$.

5. For $n = 0$, we have LHS = $0 < 1$ = RHS and for $n = 1$, LHS = $1 < 2$ = RHS. Assume true for $n = k \ge 1$. Then $k + 1 \le k + k = 2k < 2 . 2^k = 2^{k+1}$.

6. For $n = 1$, the LHS = $1^2 - (1 . 2) = -1$ and the RHS = -1. Assume true for $n = k$. Then $(F_{k+2})^2 - F_{k+1}F_{k+3} = (F_{k+2})^2 - (F_{k+1})^2 - F_{k+1}F_{k+2} = (F_{k+2})^2 - (-1)^k - F_kF_{k+2} - F_{k+1}F_{k+2} = -(-1)^k = (-1)^{k+1}$.

7. $F_{n+1}F_{n+2} - F_nF_{n+3} = F_{n+1}(F_{n+1} + F_n) - F_n(F_{n+2} + F_{n+1}) = (F_{n+1})^2 - F_nF_{n+2} = (-1)^n$.

8. For $n = 1$ we have LHS = $1 < 2$ = RHS. Assume true for all i such that $1 \le i \le k$. Then $F_{k+1} = F_k + F_{k-1} < 2^k + 2^{k-1} < 2^k + 2^k = 2^{k+1}$.

9. For $n = 1$, the LHS = $a(1 + r)$ and the RHS = $a(1- r^2) /(1 - r) = a(1 + r)$.

Assume true for $n = k$. Then $a + ar + ... + ar^k + ar^{k+1} = a(1 - r^{k+1})/(1 - r) + ar^{k+1} = a[1 - r^{k+1} + r^{k+1} - r^{k+2}] / (1 - r) = a(1 - r^{k+2}) / (1 - r)$.

10. Suppose there exists a positive integer $n \geq n_0$ for which $P(n)$ is false. Then the set S of all positive integers $n \geq n_0$, for which $P(n)$ is false, is nonempty. Therefore, S has a least element m. Then for any k such that $n_0 \leq k < m$, we have $k \notin S$ and hence $P(k)$ is true but then (2) leads us to a contradiction.

11. (a) $\Rightarrow$ (b) This is Theorem 0.3.2
(b) $\Rightarrow$ (c) This is Theorem 0.3.6
(c) $\Rightarrow$ (a) Suppose there exists a set U of positive integers with no least element. Let $P(n)$ be the statement " $n \notin U$ ". $P(1)$ is true because $1 \notin U$ since U has no least element. Assume $P(k)$ true for all k, $1 \leq k < m$. Then $k \notin U$ for all k, $1 \leq k < m$ and $m \notin U$ since U has no least element. Hence $P(m)$ is true. Therefore $P(n)$ is true for all $n \geq 1$ and U is the empty set.

12. 1 10 45 120 210 252 210 120 45 10 1

13. $n! / r!(n - r)! = n! / (n - r)!r!$

14. For this exercise it is important to first point out that the binomial coefficients are always integers. This follows immediately from Pascal's identity and induction on n.
$c_r = p! / r! (p - r)! \in \mathbb{Z}$, where $r < p$ and $p - r < p$. Therefore, the prime number p does not appear in the prime factorization of $r!$ or of $(p - r)!$. Hence since p divides $p! = c_r r! (p - r)!$ and p does not divide $r! (p - r)!$, we have that p must divide c_r.

15. $c_1 = 11 = c_{10}$, $c_2 = 55 = c_9$, $c_4 = 330$, $c_6 = 462$

16. $135 = 2 (52) + 31$
$52 = 31 + 21$
$31 = 21 + 10$
$21 = 2(10) + 1$
$1 = 21 - 2(10) = 21 - 2(31 - 21) = 3(21) - 2(31) = 3(52 - 31) - 2(31) = 3(52) - 5(31)$
$= 3(52) - 5(135 - 2(52)) = 13(52) - 5(135)$.

17. $\gcd(a,b) = 1 = ua + vb$. Therefore $n = (nu)a + (nv)b$.

18. Let $1 \leq u = \gcd(a',b')$. Then ud is a common divisor of a and b. Hence ud divides d and $u = 1$.

19. Let $d = p_1^{c_1} ... p_k^{c_k}$. Since $c_i \leq a_i$, d divides n and since $c_i \leq b_i$, d divides m. If $l \mid n$ and $l \mid m$ then $l = p_1^{r_1} ... p_k^{r_k}$, where $r_i \leq a_i$ and $r_i \leq b_i$. Hence $r_i \leq \min(a_i,b_i) = c_i$ and $l \mid d$.

20. Let $f = p_1^{d_1} \ldots p_k^{d_k}$. Since $a_i \le d_i$, n divides f and since $b_i \le d_i$, m divides f. If $g = p_1^{s_1} \ldots p_k^{s_k}$ and $n \mid g$ and $m \mid g$ then $a_i \le s_i$ and $b_i \le s_i$. Hence $\max(a_i,b_i) \le s_i$ and $f \mid g$.

21. Let $e_i = \min(a_i,b_i) + \max(a_i,b_i) = a_i + b_i$. Then $\text{lcm}(n,m)\gcd(n,m) = p_1^{e_1} \ldots p_k^{e_k}$.

22. From Exercise 21 we obtain $\text{lcm}(n,m) = nm$ if and only if $\gcd(n,m) = 1$.

23. $\gcd(9750,59400) = 2 \cdot 3 \cdot 5^2$ and $\text{lcm}(9750,59400) = 2^3 \cdot 3^3 \cdot 5^3 \cdot 11 \cdot 13$

24. $n^3 - n = n(n^2 - 1) = n(n + 1)(n - 1)$. Since $2 \mid n$ or $2 \mid n + 1$, we have $2 \mid n^3 - n$. Furthermore $n \equiv 0 \bmod 3$ in which case $3 \mid n$, or $n \equiv 1 \bmod 3$ in which case $3 \mid n - 1$, or $n \equiv 2 \bmod 3$ in which case $3 \mid n + 1$. Hence $3 \mid n^3 - n$.

25. $n \equiv 1 \bmod 5 \Rightarrow n^4 \equiv 1 \bmod 5$, $n \equiv 2 \bmod 5 \Rightarrow n^4 \equiv 16 \equiv 1 \bmod 5$, $n \equiv 3 \bmod 5 \Rightarrow n^4 \equiv 81 \equiv 1 \bmod 5$ and $n \equiv 4 \bmod 5 \Rightarrow n^4 \equiv (-1)^4 \bmod 5 \equiv 1 \bmod 5$.

26. $n^5 - n = n(n^4 - 1)$. If $n \equiv 0 \bmod 5$ then $n^5 \equiv n \bmod 5$. Otherwise by Exercise 25 $n^4 \equiv 1 \bmod 5$ and hence $n^5 \equiv n \bmod 5$.

27. $[r] + [s] = [r + s] = [s + r] = [s] + [r]$ and $[r][s] = [rs] = [sr] = [s][r]$.

28. $[r] + ([s] + [t]) = [r] + [s + t] = [r + (s + t)] = [(r + s) + t] = ([r + s]) + [t] = ([r] + [s]) + [t]$ and $[r]([s][t]) = [r][st] = [r(st)] = [(rs)t] = [rs][t] = ([r][s])[t]$.

29. $[r]([s] + [t]) = [r][s + t] = [r(s + t)] = [rs + rt] = [rs] + [rt] = [r][s] + [r][t]$.

30. $[0] + [r] = [0 + r] = [r] = [r + 0] = [r] + [0]$ and $[1][r] = [1 \cdot r] = [r] = [r \cdot 1] = [r][1]$.

31. Addition mod 6 in $\mathbb{Z}_6$

	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Multiplication mod 6 in $\mathbb{Z}_6$

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Addition mod 7 in $\mathbb{Z}_7$

	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Multiplication mod 7 in $\mathbb{Z}_7$

	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

32. Suppose p is prime. Then $[r][s] = [rs] = [0]$ implies p divides rs in $\mathbb{Z}$. Hence p divides r and $[r] = [0]$ or p divides s and $[s] = [0]$. Suppose p is not prime and $p = rs$ with $r < p$ and $s < p$. Then $[r] \neq [0]$ and $[s] \neq [0]$ in $\mathbb{Z}_p$ with $[r][s] = [0]$.

33. $\gcd(n,r) = 1 = un + vr$ for some integers u and v. Therefore, $\gcd(n,v) = 1$ and $vr \equiv 1 \bmod n$.

34. Multiplication mod 7 in $U(7)$ is as in $\mathbb{Z}_7$ with the row and column of zeros removed (see Exercise 31).

Mult. mod 8 in $U(8)$

	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

35. $\gcd(m,n) = 1 = um + vn$ for some integers u and v. Then $a = aum + avn$, hence $a \equiv avn \bmod m$ and $b = bum + bvn$, hence $b \equiv bum \bmod n$. Let $x = avn + bum$.

36. (a) We will use induction on s. For $s = 1$ let $x = a_1$. Assume true for $s - 1$ and let $y \equiv a_i \bmod m_i$ for $1 \leq i \leq s - 1$. Let $N = m_1 \ldots m_{s-1}$. Then $\gcd(N,m_s) = 1$ and by Exercise 35 there exists x such that $x \equiv y \bmod N$ and $x \equiv a_s \bmod m_s$. Note that $y = a_i + k_i m_i$, $1 \leq i \leq s - 1$ for some k_i and $x = y + k(m_1 \ldots m_{s-1})$ for some k. Hence $x = a_i + k_i m_i + k(m_1 \ldots m_{s-1})$ and $x \equiv a_i \bmod m_i$ for all i , $1 \leq i \leq s$.
(b) If $s = 1$ there is nothing to prove. Assume true for $1 \leq i \leq s - 1$ and let N be as in part (a) . Then $x = x' + kN$ and $x = x' + lm_s$ for some integers k and l and $kN = lm_s$. By Proposition 0.3.22 since $\gcd(N,m_s) = 1$ we have m_s divides k. Hence $x \equiv x' \bmod M$.

0.4 Complex Numbers

De Moivre's formula is used freely throughout the text. The cyclic group of the nth roots of unity is introduced in Chapter 1 using the polar representation of a complex number. Examples 0.4.18, 0.4.19 and 0.4.20 illustrate the type of calculations students should become comfortable with. For this purpose Exercises 23 through 28 are strongly recommended. It is especially important in Chapter 8 and later chapters for students to be at ease with finding solutions of polynomial equations.

Exercises 0.4

1. $10 - 3i$ **2.** $-2 + 2i$ **3.** $1 + i$

4. i **5.** -1 **6.** $-i$

7. 1 **8.** -1 **9.** $-i$

10. $-4 + 19i$ **11.** $23 + 14i$ **12.** $8 - 8i$

13. $1 - i$ **14.** $3/2 - i/2$ **15.** $-1/2 + i/2$

16. $\sqrt{13}$, $\sqrt{2}$, $\sqrt{5}$ **17.** $\sqrt{2}\,(\cos 7\pi/4 + i \sin 7\pi/4)$

18. $\sqrt{2}\,(\cos 5\pi/4 + i \sin 5\pi/4)$ **19.** $2(\cos 2\pi/3 + i \sin 2\pi/3)$

20. $z_1z_2 = r_1r_2[(\cos\theta_1\cos\theta_2 - \sin\theta_1\sin\theta_2) + i\,(\sin\theta_1\cos\theta_2 + \cos\theta_1\sin\theta_2) =$
$r_1r_2\,(\cos(\theta_1+\theta_2) + i \sin(\theta_1+\theta_2))$.

21. Apply Proposition 0.4.15 with $\theta = \theta_1 = \theta_2$.

22. For $n = 1$ there is nothing to prove. Assume true for $n = k$. Then

$$z^k = r^k(\cos k\theta + i \sin k\theta)$$

Using now Proposition 0.4.15 with $\theta_1 = k\theta$ and $\theta_2 = \theta$ we obtain

$$z^{k+1} = z^k \,.\, z = r^{k+1}(\cos(k+1)\theta + i \sin(k+1)\theta).$$

23. $z_1 = 1$, $z_2 = \omega = (-1 + \sqrt{3}i)/2$, $z_3 = \omega^2 = (-1 - \sqrt{3}i)/2$.

24. $z_1 = 1$, $z_2 = i$, $z_3 = -1$, $z_4 = -i$.

25. $z^4 = r^4(\cos 4\theta + i \sin 4\theta) = \cos\pi + i \sin\pi$. Thus $r = 1$ and $\theta = \pi/4 + k\pi/2$ with $k = 0, 1, 2$ or 3. Hence the four solutions are $z = (\pm\sqrt{2} \pm \sqrt{2}\,i)/2$.

26. The three solutions are -2 , $1 - \sqrt{3}\,i$ and $1 + \sqrt{3}\,i$

27. The three solutions are i , $(-\sqrt{3} - i) / 2$ and $(\sqrt{3} - i) / 2$.

28. The three solutions are $5i$, $5(-\sqrt{3} - i) / 2$ and $5(\sqrt{3} - i) / 2$.

29. Using from calculus the power series expansions of the exponential function as well as that of the cosine and the sine functions we obtain

$$e^{i\theta} = \sum_{n=0}^{\infty} (i\theta)^n / n! = \sum_{k=0}^{\infty} [\theta^{4k} /(4k)! + i\,\theta^{4k+1} /(4k + 1)! - \theta^{4k+2} /(4k+2)! - i\,\theta^{4k+3} /(4k + 3)!] =$$

$$\sum_{n=0}^{\infty} (-1)^n\,\theta^{2n} / (2n)! \; + \; i \sum_{n=0}^{\infty} (-1)^n\,\theta^{2n+1} / (2n + 1)! = \cos\theta + i \sin\theta .$$

30. Let $z = r(\cos\theta + i \sin\theta)$. Then $z = re^{i\theta}$ and $z^n = r^n e^{in\theta} = r^n(\cos n\theta + i \sin n\theta)$.

0.5 Matrices

In order to introduce the general linear groups and the special linear groups of 2x2 matrices in Chapter 1 a brief review on 2x2 matrices and their determinant is done in this section. The examples and the exercises illustrate matrices with entries not necessarily from $\mathbb{R}$.

Exercises 0.5

1.
$$\begin{bmatrix} 2 & 6 \\ 3 & 5 \\ 0 & 5 \end{bmatrix}$$

2.
$$\begin{bmatrix} 1 + i & 3 + 2\,i \\ 1 + i & 1 \end{bmatrix}$$

3.
$$\begin{bmatrix} 1 + 2\,i & 4 \\ i & 4 + 2\,i \end{bmatrix}$$

4.
$$\begin{bmatrix} 1 + i & 3 + 2\,i \\ 1 + i & 1 \end{bmatrix}$$

5.
$$\begin{bmatrix} -\,i & 1 + i \\ -\,1 + i & -\,1 \end{bmatrix}$$

6.
$$\begin{bmatrix} 1 & 4 \\ 3 & 2 \end{bmatrix}$$

7.
$$\begin{bmatrix} 4 & 2 \\ 4 & 2 \end{bmatrix}$$

8.
$$\begin{bmatrix} 1 + 2\,i & 2\,i \\ -\,2 + i & -\,2 \end{bmatrix}$$

9.
$$\begin{bmatrix} i & 0 \\ 0 & i \end{bmatrix}$$

10.
$$\begin{bmatrix} 8 & 8\,i \\ -\,8\,i & 8 \end{bmatrix}$$

11. $1 - (1 + i)(2i) = 3 - 2i$ **12.** 2 **13.** 1 **14.** 0

15. $\det A = -2 \neq 0$ and $A^{-1} = 1/2\ A$

16. $\det A = 1 \neq 0$ and $A^{-1} = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix}$

17. $\det A = 2 \neq 0$ and $A^{-1} = -1/2\ A$

18. $\det A = 1 \neq 0$ and $A^{-1} = \begin{bmatrix} 2 & -1 \\ 3 & 4 \end{bmatrix}$

19. $\det AB = \det A \det B \neq 0$

20. $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

21. $\det A = ad - bc = 1$ in $\mathbb{Z}_3$ .We will break up the counting into five cases.
(1) $a = 0$, $d = 0$, 1 or 2 and $b = 1$, $c = 2$ or $b = 2$, $c = 1$
(2) $d = 0$, $a = 1$ or 2 and $b = 1$, $c = 2$ or $b = 2$, $c = 1$
(3) $b = 0$, $c = 0$, 1 or 2 and $a = d = 1$ or $a = d = 2$
(4) $c = 0$, $b = 1$ or 2 and $a = d = 1$ or $a = d = 2$
(5) $b = c = 1$ or $b = c = 2$ and $a = 2$, $d = 1$ or $a = 1$, $d = 2$

Chapter 1

Groups

1.1 Examples and basic concepts

All the examples of groups the students will be working on in the rest of the text are introduced in this first section. Familiarity with the finite groups $\mathbb{Z}_n$, $U(n)$, S_3, D_n , the Klein 4-group, the quaternion group as well as the matrix groups $GL(2,R)$ and $SL(2,R)$ right at the beginning is very important. In this section students also get to practice developing finite group tables. The first examples help them see the difference between a specific group of a given order and the underlying group structure.

Exercises 1.1

1. (1) If $a, b \in 2\mathbb{Z}$, then $a = 2k$ and $b = 2m$ for some integers k and m. Therefore, $a + b = 2(k + m) \in 2\mathbb{Z}$, (2) addition in $\mathbb{Z}$ is associative, (3) $0 \in 2\mathbb{Z}$ and (4) $a = 2k$ implies $-a = 2(-k) \in 2\mathbb{Z}$.

2. By Proposition 0.3.31 and Proposition 0.3.34 .

3. Use Table 5.

4. (1) If $x, y \in \mathbb{C}^*$ then $x = a + bi$ and $y = c + di$ where a, b and c, d are pairs of real numbers which are not the 0, 0 pair. Hence $xy = (ac - bd) + (bc + ad)i$ and $xy = 0$ only when $ac = bd$ and $bc = -ad$. If $a = 0$ then $d = 0$ and this contradicts the second equation. If $a \neq 0$ then $d \neq 0$ and from the second equation we obtain $b^2 = -a^2$ which is impossible since b is a real number and $a \neq 0$. Hence $xy \in \mathbb{C}^*$,
(2) $(a + bi)[(c + di)(u + vi)] = a(cu - dv) - b(cv + du) + [b(cu - dv) + a(cv + du)]i =$
$(ac - bd)u - (ad + bc)v + [(ac-bd)v + (ad +bc)u]i = [(a + bi)(c + di)](u + vi)$,
(3)$1 \in \mathbb{C}^*$ and (4) $x = a + bi \in \mathbb{C}^*$ implies $a^2 + b^2 \neq 0$ and $x^{-1} = (a - bi)/a^2 + b^2 \in \mathbb{C}^*$.

5. (1) $\det A \neq 0$ and $\det B \neq 0$ implies $\det AB = \det A \det B \neq 0$, (2) multiplication is associative in $\mathbb{Q}$ hence in G, (3) $\det I_2 = 1$ hence $I_2 \in G$ and (4) $\det A \neq 0$ hence A^{-1} exists and $\det A^{-1} = (1 / \det A) \neq 0$.

Constructing the group tables in Exercises 6 through 9 help students understand how the tables give us a "picture " of these groups, and at the same time they get more familiar with these important finite groups that will appear very often in the text.

6. The group table of S_3

	ρ_0	ρ	ρ^2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ	ρ^2	μ_1	μ_2	μ_3
ρ	ρ	ρ^2	ρ_0	μ_3	μ_1	μ_2
ρ^2	ρ^2	ρ_0	ρ	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ	ρ^2
μ_2	μ_2	μ_3	μ_1	ρ^2	ρ_0	ρ
μ_3	μ_3	μ_1	μ_2	ρ	ρ^2	ρ_0

Not Abelian since for example $\mu_1\rho \neq \rho\mu_1$

7. The group table of D_4

	ρ_0	ρ	ρ^2	ρ^3	τ	$\rho\tau$	$\rho^2\tau$	$\rho^3\tau$
ρ_0	ρ_0	ρ	ρ^2	ρ^3	τ	$\rho\tau$	$\rho^2\tau$	$\rho^3\tau$
ρ	ρ	ρ^2	ρ^3	ρ_0	$\rho\tau$	$\rho^2\tau$	$\rho^3\tau$	τ
ρ^2	ρ^2	ρ^3	ρ_0	ρ	$\rho^2\tau$	$\rho^3\tau$	τ	$\rho\tau$
ρ^3	ρ^3	ρ_0	ρ	ρ^2	$\rho^3\tau$	τ	$\rho\tau$	$\rho^2\tau$
τ	τ	$\rho^3\tau$	$\rho^2\tau$	$\rho\tau$	ρ_0	ρ^3	ρ^2	ρ
$\rho\tau$	$\rho\tau$	τ	$\rho^3\tau$	$\rho^2\tau$	ρ	ρ_0	ρ^3	ρ^2
$\rho^2\tau$	$\rho^2\tau$	$\rho\tau$	τ	$\rho^3\tau$	ρ^2	ρ	ρ_0	ρ^3
$\rho^3\tau$	$\rho^3\tau$	$\rho^2\tau$	$\rho\tau$	τ	ρ^3	ρ^2	ρ	ρ_0

Not Abelian since for example $\rho\tau \neq \tau\rho$.

8. Let $a = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$ $b = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ and $c = ab = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$

Then we obtain the following group table and the group is Abelian

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

9. The group table of Q_8

	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	$-j$	j	$-i$	i	-1	1
$-k$	$-k$	k	j	$-j$	i	$-i$	1	-1

10.

$$\begin{bmatrix}1 & 1\\ 1 & 0\end{bmatrix}\begin{bmatrix}0 & 1\\ 1 & 1\end{bmatrix} = \begin{bmatrix}1 & 2\\ 0 & 1\end{bmatrix} \quad \text{while}$$

$$\begin{bmatrix}0 & 1\\ 1 & 1\end{bmatrix}\begin{bmatrix}1 & 1\\ 1 & 0\end{bmatrix} = \begin{bmatrix}1 & 0\\ 2 & 1\end{bmatrix}$$

11. If $n = 0$ or 1 nothing to prove since the group is Abelian. Assume true for all $k \geq 0$, then $(ab)^{k+1} = (ab)^k(ab) = (a^kb^k)(ab) = a^k(b^ka)b = a^k(ab^k)b = a^{k+1}b^{k+1}$ and if $n = -s < 0$ then $(ab)^n = (ab)^{-s} = (b^{-1}a^{-1})^s = (a^{-1}b^{-1})^s = a^{-s}b^{-s} = a^nb^n$.

12. $(\rho\mu_1)^2 = \rho_0$ while $\rho^2\mu_1^2 = \rho^2 \neq \rho_0$.

13. $a^2 = \rho_0$ if $a = \rho_0, \mu_1, \mu_2$ or μ_3 and $b^3 = \rho_0$ if $b = \rho$ or ρ^2.

14. In $U(10)$ $3^{-1} = 7$, $7^{-1} = 3$ and $9^{-1} = 9$.
In $U(15)$ $2^{-1} = 8$, $4^{-1} = 4$, $7^{-1} = 13$, $11^{-1} = 11$ and $14^{-1} = 14$.

15. $a^{-1} = a^{n-1}$.

16. $\rho^{-1} = \rho^3$, $\tau^{-1} = \tau$ and $(\rho\tau)^{-1} = \rho\tau$.

17. The elements of V can be written as I_2, A, $-A$ and $-I_2$ and
$I_2^2 = A^2 = (-A)^2 = (-I_2)^2 = I_2$.

18. Let $a, b \in G$, then $(ab)^{-1} = ab$ and $(ab)^{-1} = b^{-1}a^{-1} = ba$.

Exercises 19 and 20 may seem to students at first long and complex with too many cases. The hint though in Exercise 20 should help them take a short cut.

19. Let $G = \{e, a, b, c\}$. Case 1: Assume $a^2 \neq e$. Then a^2 is one of the remaining two elements, let's say $a^2 = b$. Then ac can not be equal to a, b or c. Therefore, $ac = e$, $ab = c = a^3$, $a^4 = ac = e$ and $G = \{e, a, a^2, a^3\}$. Case 2 : Assume $a^2 = e$. Then $ab = c$ and $ac = b$. Furthermore, this gives us $ba = c$ and $ca = b$. If $b^2 = a$ then $c = ba = b^3$ and $G = \{e, b, b^2, b^3\}$ and we get the same table as in Case 1. If $b^2 = e$ then we obtain

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

20. If there exists $a \neq e$ in G such that $a^2 = e$, then let e, a, b, c, d be the five distinct elements of G with $c = ab$. Then $b = a^2b = ac$ and $ad = d$ which is impossible. Thus for all elements $a \neq e$ in G we have $a^2 \neq e$. If there exists an element $a \neq e$ in G such that $a^3 = e$, then $G = \{e, a, a^2, b, c\}$ with $ab = c$ and $ac = b$. In this case $a^2b = ac = b$ which is impossible. Thus for all elements $a \neq e$ in G we have $a^3 \neq e$. Finally if there exists an element $a \neq e$ in G with $a^4 = e$ then $G = \{e, a, a^2, a^3, b\}$, and $ab = b$ which is impossible.Thus $G = \{e, a, a^2, a^3, a^4\}$ and $a^5 = e$.

21. 6 , as in Exercise 20 in Section 0.5.

22. $a^2 = e$ means $a = a^{-1}$. Since $|G - \{e\}|$ is odd , if we pair every element of $G - \{e\}$ with its inverse, $\{b, b^{-1}\}$, then in at least one of these pairs $b = b^{-1}$.

23. $\rho\tau(1) = \rho(1) = 2$ and $\rho\tau(2) = \rho(n) = 1$,
also $\tau\rho^{-1}(1) = \tau(n) = 2$ and $\tau\rho^{-1}(2) = \tau(1) = 1$.

24. Let $G = \{a_1, a_2, ..., a_i, .., a_n\}$ and $A = \{a_ia_j\}$ the matrix that gives its group table. Then G is Abelian if and only if $a_ia_j = a_ja_i$ for all $1 \leq i, j \leq n$.

25. $\gcd(m, n) = 1 = um + vn$ for some integers u and v by Theorem 0.3.16.
Hence $a = (a^m)^u(a^v)^n = (a^v)^n$.

26. Since $a^2 \neq e$ for all $a \neq e$ in G and G is Abelian , we have
$a_1a_2...a_n = \prod_i (a_ia_i^{-1}) = e$.

27. Since G is finite and closed under the given operation, for any element a of G there exist positive integers $i < j$ such that $a^i = a^j$. Hence, using the cancellation laws we obtain $a^{j-i+1} = a$ where $j - i + 1 > 1$. For any other element b in G we have $a^{j-i+1}b = ab$ and by the left cancellation law $a^{j-i}b = b$. Similarly, using the right cancellation law we obtain $ba^{j-i} = b$ Therefore a^{j-i} is the identity element in G. Furthermore, a^{j-i-1} is the inverse of a in G.

28. By Proposition 0.3.37, $\mathbb{Z}_p - \{0\} = U(p)$ is closed under multiplication mod p. By Proposition 0.3.34 the operation is associative. Furthermore, if $a, b, c \in U(p)$ and $ab = ac$, then $a(b - c) = 0$, that is $p \mid a(b - c)$ in $\mathbb{Z}$. Since p does not divide a, by Euclid's Lemma, Corollary 0.3.23, $p \mid b - c$ and $b = c$ in $U(p)$. Similarly, right cancellation holds and $\mathbb{Z}_p - \{0\}$ is a group by Exercise 27.

29. For any prime p and any integer y such that $0 \leq y \leq p$, $p \mid y$ implies $y = 0$ or $y = p$. For any $x \in U(p)$ such that $x^2 = 1$ we must have $p \mid (x + 1)(x - 1)$ which implies $x + 1 = p$ or $x - 1 = 0$. Thus $x = x^{-1}$ in $U(p)$ only if $x = 1$ or $x = p-1$. Therefore, $(p - 2)! \equiv 1 \bmod p$ and $(p - 1)! \equiv -1 \bmod p$.

1.2 Subgroups

The subgroup test , Theorem 1.2.10, introduced in this section is used very frequently throughout the text . Similar theorems based on the subgroup test are given in Chapter 6 for subrings, subdomains and subfields. The order of an element a and the cyclic subgroup $< a >$ it generates are notions introduced here and prepare students for the next section on cyclic groups. In addition, they help students construct examples of subgroups.

Exercises 1.2

1. 3 **2.** 5 **3.** 2 **4.** 4 **5.** 2 **6.** 3 **7.** 4 **8.** 4

9. Infinite **10.** *7* **11.** $n\mathbb{Z}$ for all $n \geq 1$ **12.** $n\mathbb{Z}$ for all $n \geq 1$

13. $\mathbb{R}^*$, $< i >$, $< \cos 2\pi/n + i \sin 2\pi/n >$ **14.** $< 2 >$, $< 4 >$

15. $< \rho >$, $< \mu_1 >$ **16.** $< \rho >$, $\{ \rho_0 , \rho^2 , \tau , \rho^2\tau \}$ **17.** $16\mathbb{Z}$, $24\mathbb{Z}$

18. {Upper triangular invertible matrices} , {Lower triangular invertible matrices }

19. $< i >$, $< j >$

20. For any integer k , $a^k a^{-k} = e$. Hence $a^k = e$ if and only if $(a^{-1})^k = e$ and $|a| = |a^{-1}|$. Furthermore, if $|a| = n$, then $a^k = a^{-n+k} = (a^{-1})^{n-k}$.

In Exercises 21, 22, 23, 24 , 25 and 29 we use repeatedly the subgroup test Theorem 1.2.20.

21. For $x = a + b\sqrt{2}$ and $y = c + d\sqrt{2}$, where a, b, c, d are in $\mathbb{Q}$, $x - y = (a - c) + (b - d)\sqrt{2}$ is in G since $a - c$ and $b - d$ are in $\mathbb{Q}$.

22. If $x = n + mi$ and $y = r + si$ in G then $n - r$ and $m - s$ are in $\mathbb{Z}$. Therefore, $x - y = (n - r) + (m - s)i$ is in G.

23. Let $x = \cos(2k\pi/7) + i \sin(2k\pi/7)$ and $y = \cos(2m\pi/7) + i \sin(2m\pi/7)$ then $xy^{-1} = \cos(2(k-m)\pi/7) + i \sin(2(k-m)\pi/7)$ is in G and $|G| = 7$.

24. If x and y are complex numbers with $|x| = |y| = 1$, then $x = \cos\theta + i \sin\theta$, $y = \cos\varphi + i \sin\varphi$ and $xy^{-1} = \cos(\theta - \varphi) + i \sin(\theta - \varphi) \in G$.

25. (a) $\det A(\chi) = \cos^2\chi + \sin^2\chi = 1$ for any angle χ and $A(\theta)A(\varphi)^{-1} = A(\theta)A(-\varphi) = A(\theta - \varphi) \in G$.

(b) $A(4\pi/3) = A^{-1}(2\pi/3)$ and (c) $|A(2\pi/3)| = 3$

26. (a) $A^3 = \begin{bmatrix} 1 & 6 \\ 0 & 1 \end{bmatrix}$ $A^{11} = A$ and (b) $|A| = 5$

27. $D^{-1}(a, b, c) = D(-a, ac - b, -c)$ and $D(a, b, c)D(x, y, z) = D(x + a, y + az + b, z + c)$. Hence, by Theorem 1.2.13, H is a subgroup of $SL(3, \mathbb{R})$.

28. Let $a, b \in G$ with $|a| = k$ and $|b| = m$. Then, by Exercise 20, $|b^{-1}| = m$ and by Exercise 11 in Section 1.1, $(ab^{-1})^{km} = a^{km}(b^{-1})^{km} = (a^k)^m((b^{-1})^m)^k = e$ and $|ab^{-1}|$ is finite. We obtain a subgroup by Theorem 1.2.13.

29. Let $x, y \in H \cap K$. Then $xy^{-1} \in H$ because H is a subgroup and $xy^{-1} \in K$ because K is a subgroup. Hence $xy^{-1} \in H \cap K$.

30. Let $k = |b|$ and $n = |aba^{-1}|$. Then $(aba^{-1})^k = ab^k a^{-1} = e$ and $n \leq k$.
Also $(aba^{-1})^n = ab^n a^{-1} = e$ which implies $b^n = e$ and $k \leq n$. Hence $n = k$.

31. $(ab)^{k+1} = a(ba)^k b$. Hence $(ba)^k = e$ if and only if $(ab)^k = e$.

32. Let $x, y \in C(a)$. Then $(xy)a = x(ya) = x(ay) = (xa)y = a(xy)$ and $xa = ax$ implies $ax^{-1} = x^{-1}(xa)x^{-1} = x^{-1}(ax)x^{-1} = x^{-1}a$. Hence by Theorem 1.2.13 $C(a)$ is a subgroup of G.

33. $C(\mu_1) = \langle \mu_1 \rangle$ **34.** $C(\rho_2) = D_2$

35. $C(a) = G$ means $xa = ax$ for all $x \in G$. Hence $C(a) = G$ is equivalent to $a \in Z(G)$.

36. $Z(S_3) = \{\rho_0\}$.

1.3 Cyclic Groups

In this section Theorem 1.3.16 allows students to calculate orders of elements in a cyclic group in a direct way. Corollary 1.3.12 of Theorem 1.3.11 clarifies a very common misconception that students have about the order of an element. This Corollary is used repeatedly throughout the book. In Theorem 1.3.26 it should be pointed out that it is the subgroup of order d that is unique while the number of elements of order d can be larger, it is actually $\phi(d)$ as is shown in Exercise 26.

Exercises 1.3

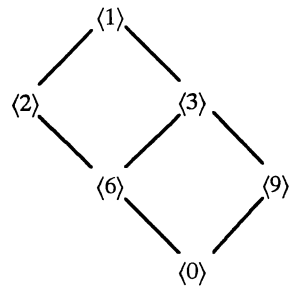
1. (a) 5 (b) 5 (c) 21 (d) 30 (e) 21 (f) 3

2. 21, 7, 21, 7, 3, 7, 7 **3.** (a) $< a > = \{e, a, a^2, a^3, a^4, a^5\}$, (b) a^2, a^5, a^4

4. In $\mathbb{Z}_{10}$ 1, 3, 7, 9 . In $\mathbb{Z}_{12}$ 1, 5, 7, 11. In $\mathbb{Z}_{15}$ 1, 2, 4, 7, 8, 11, 13, 14.

5. $a, a^7, a^{11}, a^{13}, a^{17}, a^{19}, a^{23}, a^{29}$

6.



7. 3, 6, 9, 12 **8.** a^2, a^6, a^{14}, a^{18}

9. $< \rho_0 >, < \rho >, < \mu_1 >, < \mu_2 >, < \mu_3 >$. All proper subgroups of S_3 are cyclic.

10. $< \rho_0 >, < \rho >, < \rho^2 >, < \tau >, < \rho\tau >, < \rho^2\tau >, < \rho^3\tau >$.
$\{ \rho_0 , \rho^2, \tau , \rho^2\tau \}$ is a non cyclic proper subgroup of D_4 .

11. Counterexample given in Exercise 9 with S_3 . **12.** $< i >, < \cos 2\pi/n + i \sin 2\pi/n >$

13. ($\Rightarrow$) If $a^k = e$ then $a^k = a^0$. Hence by Theorem 1.3.11 part (2) $n \mid k$.
($\Leftarrow$) If $n \mid k$, then $k = nr$ and $a^k = (a^n)^r = e$.

14. By definition $< a > = \{ a^k \mid k \in \mathbb{Z} \}$. Let $n = |a|$, then for any integer k, when divided by n we have $k = qn + r$, where $0 \le r \le n - 1$. Hence $a^k = a^{qn+r} = (a^n)^q a^r = a^r$.

15. If $0 \le i, j \le n - 1$ and $a^i = a^j$ then $a^{j-i} = e$ and by Corollary 1.3.12 $n \mid j - i$.
Hence $j - i = 0$ and $|< a >| = n = |a|$.

16. Let $x, y \in G = < a >$. Then $x = a^k$ and $y = a^m$ for some integers k and m and $xy = a^k a^m = a^{k+m} = a^{m+k} = a^m a^k = xy$.

17. (a) $\mathbb{Z}$, $2\mathbb{Z}$, $n\mathbb{Z}$ (b) $\mathbb{Q}, \mathbb{R}, \mathbb{R}^*, \mathbb{C}^*$ (c) $\mathbb{Z}_7, \mathbb{Z}_{14}$ (d) Klein 4-group

18. $H = < a >$ with $|a| = 10$ and $K = < b >$ with $|b| = 14$. Define $L = < b^2 > \leq K$. Then $|L| = 7$ and $H \cap L = \{e\}$. Hence if $k = |(ab^2)|$, then $e = (ab^2)^k = a^k b^{2k}$, which implies $a^k = b^{-2k} = e \in H \cap L$. Therefore, $10 \mid k$, $7 \mid k$, hence $70 \mid k$. Also , since the group is Abelian , by Exercise 11 in Section 1.1, $(ab^2)^{70} = a^{70} b^{140} = e$ and $k \mid 70$. Therefore, $< ab^2 >$ is a cyclic subgroup of order 70.

19. (a) If $G \neq \{e\}$ let $a \neq e$ in G. Then $< a >$ is a nontrivial subgroup of G. Hence it can not be a proper subgroup. Thus $G = < a >$.
(b) Suppose G is infinite. In this case $a^2 \neq e$. Consider $< a^2 >$. If $a \notin < a^2 >$ this would be a proper nontrivial subgroup which is impossible. Therefore, $a = a^{2k}$ for some integer k, which implies $a^{2k-1} = e$ and G is a finite cyclic group. Also, by Theorem 1.3.26, $|G|$ must be prime. So G is a finite cyclic group of prime order.

20. (a) Let $x = mk + nl$ and $y = mr + ns$, then $x - y = m(k - r) + n(l - s)$
(b) By Theorem 0.3.16, $3 = \gcd(12, 21) \in 12\mathbb{Z} + 21\mathbb{Z}$. Hence 3 is a generator.
(c) $m\mathbb{Z} + n\mathbb{Z} = < \gcd(m, n) >$.

21. $< 30 > = 6\mathbb{Z} + 15\mathbb{Z}$ **22.** $< \text{lcm}(m, n) >$

23. (a) Yes , $U(10) = < 3 > = < 9 >$ (b) No, $|5| = |7| = |11| = 2$
(c) No, $|3| = |7| = |13| = |17| = 4$ and $|9| = |11| = 2$

24. Let $H = < a > \cap < b >$. Then H is a subgroup of $< a >$ and $|H|$ divides $|a|$. Similarly $|H|$ divides $|b|$. Therefore $|H| = 1$ and $H = \{e\}$.

25. K is a nontrivial proper subgroup of G. Hence $|K| = 2, 4, 5$ or 10. H is a nontrivial proper subgroup of K , therefore $|K| \neq 2$. Also, since $a^4 \notin K$ we have $|K| \neq 5$. If $|K| = 10$, then $a^2 \in K$ which implies $a^4 \in K$. Therefore, $|K| = 4$, $|H| = 2$, $K = \{e, a^5, a^{10}, a^{15}\}$ and $H = \{e, a^{10}\}$.

26. Let H be the unique subgroup of G of order d. If $b \in G$ with $|b| = d$, then $< b > = H$ and b is a generator of H. Therefore the elements of order d in G are exactly the generators of H. By Corollary 1.3.21 there are $\varphi(d)$ of them.

1.4 Permutations

Throughout the text the notation used for the product of two permutations is that of the composition of two functions which is easier for students to remember. Thus $\rho\tau$ stands for the composite function $\rho(\tau(x))$ and the product permutation is always calculated from right to left. The fact that some textbooks perform the product of two

permutations from left to right is not mentioned in the text to avoid confusion. This section contains a lot of calculations students learn easily. Permutations give them concrete examples of the notions they have learned so far. Seeing some of the finite groups they encountered in Section 1.1, such as D_n , as subgroups of some S_n, make these groups easier to work with.

Exercises 1.4

1. Yes **2**. No **3**. No **4**. Yes **5**. Yes

6. $1 \to 7 \to 5 \to 1$, $2 \to 6 \to 4 \to 2$ and $3 \to 3$

7. $1 \to 6 \to 8 \to 2 \to 5 \to 1$, $3 \to 9 \to 3$, $4 \to 4$ and $7 \to 7$

8. $5\mathbb{Z}$, $1+5\mathbb{Z}$, $2+5\mathbb{Z}$, $3+5\mathbb{Z}$, $4+5\mathbb{Z}$ **9**. $3\mathbb{Z}$, $1+3\mathbb{Z}$, $2+3\mathbb{Z}$

10. (a)

$$\phi\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 1 & 3 & 8 & 2 & 5 & 6 & 4 \end{pmatrix}, \tau\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 3 & 2 & 6 & 8 & 5 & 4 & 7 \end{pmatrix}$$

(b)

$$\phi^2\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 8 & 6 & 7 & 1 \end{pmatrix}, \phi\tau^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 8 & 7 & 1 & 6 & 4 & 2 & 3 \end{pmatrix}$$

(c)

$$\phi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 7 & 1 & 3 & 8 & 5 & 6 & 2 \end{pmatrix}, \tau^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 8 & 2 & 7 & 1 & 5 & 6 \end{pmatrix}$$

(d) $|\varphi| = 15$, $|\tau| = 4$

11. $\varphi = (2\,8\,3)(4\,9\,10\,6\,5\,7)$ and $|\varphi| = 6$ **12**. $\varphi = (2\,7\,6)(3\,4)$ and $|\varphi| = 6$

13. $\varphi = (1\,4)(2\,5)$ and $|\varphi| = 2$

14. Let $\sigma = (a_1\, a_2\, a_3 \ldots a_n)$, then $\sigma^i(a_1) = a_{1+i}$ for all $1 \le i < n$ and $\sigma^n(a_1) = a_1$. Similarly n is the least positive integer such that $\sigma^n(a_j) = a_j$.

15. If ρ and σ are disjoint cycles in S_n, then $< \rho > \cap < \sigma > = < \rho_0 >$ and by Proposition 1.4.22 $\rho\sigma = \sigma\rho$. Hence $\rho_0 = (\rho\sigma)^k = \rho^k \sigma^k$ implies $\rho^k = (\sigma^{-1})^k = \rho_0$. Hence $|\rho\sigma| = \text{lcm}\,(|\rho|, |\sigma|)$.

16. $(a_1\ a_2\ a_3\ \ldots\ a_m) = (a_1\ a_m)(a_1\ a_{m-1})\ \ldots\ (a_1\ a_2)$ and the number of 2-cycles is m - 1.

17. In Exercise 11 odd, Exercise 12 odd, Exercise 13 even

18. (a) The identity is an even permutation and (b) The product of two odd permutations is an even permutation.

19. 4 **20.** 6 **21.** 6 **22.** 12 **23.** 5 **24.** 5 **25.** 7

26. If all the elements of H are even permutations there is nothing to prove. So suppose H contains an odd permutation ρ. Let E be the set of all even permutations in H and O the set of all odd permutations in H . Let $\chi : E \to O$ be the map defined by $\chi(\tau) = \tau\rho$ for every even permutation $\tau \in E$. The map χ is one to one and onto which shows that $|E| = |O|$.

The group table of A_4 is not given in the text only the twelve elements are described in Example 1.4.35. Exercise 27 together with Exercise 38 should give students a very good picture of this very important group.

27. The group table of A_4 with the notation as in Example 1.4.35

	ρ_0	ρ_1	ρ_1^2	ρ_2	ρ_2^2	ρ_3	ρ_3^2	ρ_4	ρ_4^2	σ_1	σ_2	σ_3
ρ_0	ρ_0	ρ_1	ρ_1^2	ρ_2	ρ_2^2	ρ_3	ρ_3^2	ρ_4	ρ_4^2	σ_1	σ_2	σ_3
ρ_1	ρ_1	ρ_1^2	ρ_0	σ_3	ρ_4	ρ_2	σ_1	σ_2	ρ_3^2	ρ_4^2	ρ_2^2	ρ_3
ρ_1^2	ρ_1^2	ρ_0	ρ_1	ρ_3	σ_2	σ_3	ρ_4^2	ρ_2^2	σ_1	ρ_3^2	ρ_4	ρ_2
ρ_2	ρ_2	σ_2	ρ_4^2	ρ_2^2	ρ_0	σ_1	ρ_1	ρ_3	σ_3	ρ_4	ρ_3^2	ρ_1^2
ρ_2^2	ρ_2^2	ρ_3^2	σ_3	ρ_0	ρ_2	ρ_4	σ_2	σ_1	ρ_1^2	ρ_3	ρ_1	ρ_4^2
ρ_3	ρ_3	ρ_4	σ_1	σ_2	ρ_1^2	ρ_3^2	ρ_0	σ_3	ρ_2	ρ_2^2	ρ_4^2	ρ_1
ρ_3^2	ρ_3^2	σ_3	ρ_2^2	ρ_4^2	σ_1	ρ_0	ρ_3	ρ_1	σ_2	ρ_1^2	ρ_2	ρ_4
ρ_4	ρ_4	σ_1	ρ_3	ρ_1	σ_3	σ_2	ρ_2^2	ρ_4^2	ρ_0	ρ_2	ρ_1^2	ρ_3^2
ρ_4^2	ρ_4^2	ρ_2	σ_2	σ_1	ρ_3^2	ρ_1^2	σ_3	ρ_0	ρ_4	ρ_1	ρ_3	ρ_2^2
σ_1	σ_1	ρ_3	ρ_4	ρ_3^2	ρ_4^2	ρ_1	ρ_2	ρ_1^2	ρ_2^2	ρ_0	σ_3	σ_2
σ_2	σ_2	ρ_4^2	ρ_2	ρ_1^2	ρ_3	ρ_2^2	ρ_4	ρ_3^2	ρ_1	σ_3	ρ_0	σ_1
σ_3	σ_3	ρ_2^2	ρ_3^2	ρ_4	ρ_1	ρ_4^2	ρ_1^2	ρ_2	ρ_3	σ_2	σ_1	ρ_0

28. (a) For any σ , τ in H we have $\sigma\tau^{-1}(2) = \sigma(2) = 2$ and $\sigma\tau^{-1}$ is in H.
(b) $|H| = 6$ and (c) $\{\ \rho_0, (1\,3\,4), (1\,4\,3)\ \}$

29. (a) For any σ , τ in H we have $\sigma\tau^{-1}(i) = \sigma(i) = i$ and $\sigma\tau^{-1}$ is in H.
(b) $|H| = (n - 1)!$ and (c) All the even permutations on the set of n - 1 elements $\{1, 2, \ldots, i - 1, i + 1, \ldots, n\}$

30. $(1\,2\,3)(1\,2) \neq (1\,2)(1\,2\,3)$ and $(1\,2\,3)$ and $(1\,2)$ are permutations in S_n for all $n \geq 3$

31. (1 2) , (1 3) , (1 4) , (2 3) , (2 4) , (3 4) and σ_1, σ_2, σ_3 as in Example 1.4.35

32. If $\tau = \sigma_1 \sigma_2 \ldots \sigma_n$, where the σ_i are disjoint cycles, then $|\tau| = \text{lcm}(|\sigma_1|,\ldots,|\sigma_n|) = 2$ implies $|\sigma_i| = 2$ for all i . Therefore the σ_i are all 2-cycles.

33. Let $\sigma \in A_n$. Then σ can be written as the product of an even number of 2-cycles, let's say $\sigma = (\rho_1 \rho_2)(\rho_3 \rho_4) \ldots (\rho_{2s-1} \rho_{2s})$ where the ρ_j are all 2-cycles. If a pair $(\rho_r \rho_{r+1})$ of 2-cycles is not disjoint it can be replaced by a 3-cycle as follows:
$(i\ j)(j\ k) = (j\ k\ i)$ and if it is disjoint it can be replaced by 3-cycles as follows:
$(i\ j)(k\ l) = (i\ k\ j)(k\ l\ i)$.

Exercise 34 should be assigned together with Exercise 33 .

34. $(1\ 2\ k)(1\ 2\ k)(1\ 2\ i) = (2\ i\ k)$. Therefore, the 3-cycles $(1\ 2\ s)$ generate all the 3-cycles of type $(2\ i\ k)$ where $i, k \geq 3$. Furthermore, $(2\ i\ k)(2\ k\ j) = (i\ k\ j)$ and the the 3-cycles $(1\ 2\ s)$ generate all the 3-cycles in S_n . The exercise now follows from Exercise 33.

35. We will use induction on $j - i$ for $1 \leq i \leq j \leq n$. If $j - i = 1$ then $(i\ j) = (i\ i + 1)$. Assume that any 2-cycle $(i\ j)$ with $j - i = k$ can be written as the product of 2-cycles of type $(s\ s+1)$. Consider a 2-cycle $(i\ j)$ with $j - i = k + 1$. Then
$(i\ j) = (i+ 1\ \ j)(i\ i+1)(i + 1\ j)$ .By our induction hypothesis $(i + 1\ j)$ can be written as the product of 2-cycles of type $(s\ s+1)$ and therefore $(i\ j)$ also.

Exercise 36 should be assigned together with Exercise 35.

36. $(1\ 2\ 3 \ldots n)(1\ 2)(1\ \ n\ \ n - 1 \ldots 3\ 2) = (2\ 3)$ and
$(1\ 2\ 3 \ldots n)(i\ \ i+ 1)(1\ n\ \ n - 1 \ldots 3\ 2) = (i + 1\ \ i + 2)$. Therefore, the cycles $(1\ 2\ 3 \ldots n)$ and $(1\ 2)$ generate all the 2-cycles of type $(s\ s + 1)$. Hence, by Exercise 35, they generate all the permutaions in S_n .

37. For an m-cycle $(a_1\ a_2\ a_3 \ldots a_m)$ there are n choices for the value of a_1, n -1 choices for a_2, . . . and $n - m + 1$ choices for a_m . Hence we have found $n(n - 1)...(n - m + 1)$ choices but the same m-cycle can be written m different ways since $(a_1\ a_2\ a_3 \ldots a_m) = (a_m\ a_1\ a_2 \ldots a_{m-1}) = \ldots = (a_2\ a_3\ a_4 \ldots a_m\ a_1)$.

38. (a) With $1 \leq i \leq 4$, ρ_i and ρ_i^2 give the two rotations with vertex i fixed .
σ_1 the rotation around the axis through the edges 1 - 2 and 3 - 4,
σ_2 the rotation around the axis through the edges 1 - 3 and 2 - 4 and
σ_3 the rotation around the axis through the edges 1 - 4 and 2 - 3.
(b) A_4

39. S_4 .

40. Let X denote the empty square. Every rearrangement is obtained by a series of exchanges of X with an adjacent square. Such an exchange can be written as a 2-cycle. In order for X to end up where it started from, the bottom right corner, it must move to the left as many squares as it moves to the right and it must move up as many squares as it moves down. Therefore, the rearrangement can be written as the product of an even number of 2-cycles.

41. The rearrangement corresponds to the permutation
(1 2 3)(4 5 6)(7 8 9)(10 11 12)(13 14 15) which is an even permutation therefore a possible arrangement.

42. (1 8 11 3 5 6)(2 12 4 7 15 10 14) is an odd permutation hence not a possible arrangement.

43. An even permutation , hence the arrangement is possible.

44. Let σ be the permutation that gives a "perfect" shuffle.Then $\sigma(x) \equiv 2x \bmod 2n + 1$ and $\sigma^k(x) \equiv 2^k x \bmod 2n + 1$. Therefore, the order of σ is the order of 2 in the group $U(2n + 1)$. In the case of $2n = 52$ the order of σ is 52 and in the case of $2n = 50$ the order of σ is 8 .

Chapter 2

Group Homomorphisms

2.1 Cosets and Lagrange's Theorem

Cosets of a subgroup are introduced as equivalence classes. Theorem 0.2.4 gives us right away the partition of a finite group and Lagrange's theorem follows easily. The fact that two cosets of a subgroup H are equal, $aH = bH$, exactly when $a^{-1}b \in H$ needs to be emphasized to facilitate later on the understanding of quotient groups and quotient rings.

Exercises 2.1

1. $5\mathbb{Z}, 1+5\mathbb{Z}, 2+5\mathbb{Z}, 3+5\mathbb{Z}, 4+5\mathbb{Z}$

2. $9\mathbb{Z}, 1+9\mathbb{Z}, 2+9\mathbb{Z}, 3+9\mathbb{Z}, 4+9\mathbb{Z}, 5+9\mathbb{Z}, 6+9\mathbb{Z}, 7+9\mathbb{Z}, 8+9\mathbb{Z}$ and in $3\mathbb{Z}$ the cosets are $9\mathbb{Z}, 3+9\mathbb{Z}, 6+9\mathbb{Z}$

3. $<6>, 1+<6>, 2+<6>, 3+<6>, 4+<6>, 5+<6>$ and in $<2>$ the cosets are $<6>, 2+<6>, 4+<6>$

4. $<\tau>, \rho<\tau> = <\tau>\rho^3, \rho^2<\tau> = <\tau>\rho^2, \rho^3<\tau> = <\tau>\rho$

5. 2 **6.** 3 **7.** 4 **8.** n

9. (1) Since H is a subgroup $aa^{-1} = e \in H$ and $a \sim a$ for all $a \in G$
(2) $ab^{-1} \in H$ implies $(ab^{-1})^{-1} = ba^{-1} \in H$ since H is a subgroup and
(3) $ab^{-1} \in H$ and $bc^{-1} \in H$ imply $ab^{-1}bc^{-1} = ac^{-1} \in H$.
Finally, $x = ha$ for some $h \in H$ is equivalent to $xa^{-1} \in H$ and $x \sim a$

10. Consider the map $\chi : H \to Ha$ defined by $\chi(h) = ha$ for all $h \in H$. (1) χ is one to one since $\chi(h_1) = h_1a = h_2a = \chi(h_2)$ implies $h_1 = (h_1a)a^{-1} = (h_2a)a^{-1} = h_2$ and (2) χ is onto since for any $y \in Ha$ we have $y = ha$ for some $h \in H$ and $\chi(h) = ha = y$. Thus $|Ha| = H$

11. Immediate from Lemma 0.2.4 part (4) and Exercise 9

12. Immediate from Lemma 0.2.4 part (3) and Exercise 9

13. By Lemma 2.1.7 part (2) $aH = H$ if an only if $a = ae^{-1} \in H$

14. (a) Yes, since $27 - 12 \in H$ (b) Yes, since $13 - (-2) \in H$
(c) No, since $126 - (-1) \notin H$

15. $|H| = 1, 2, 3, 6, 7, 14, 21, 42$ and $[G:H] = 42, 21, 14, 7, 6, 3, 2, 1$, respectively

16. $|H| = |a^{35}| = 12$, $[G:H] = 5$ and $H = < a^{35} > = < a^5 >$. Therefore, H, aH, a^2H, a^3H and a^4H are exactly all the left cosets of H

17. $|a|$ is a divisor of $36 = 2^2 3^2$. Therefore, $a^{12} \neq e$ implies $|a| \neq 1, 2, 3, 4, 6$ or 12 . In addition, $|a| \neq 9$ or 18 because $a^{18} \neq e$. Hence $|a| = 36$ and $G = < a >$

18. 216 **19**. $|H \cap K| = 3$ because $|H \cap K|$ is a common divisor of 9 and 12 and $[G:H \cap K] \neq |G|$ implies $|H \cap K| > 1$

20. Let H be a proper subgroup of G. Then $|H| = 1$ and $H = < e >$ or $|H| = p$ and by Theorem 2.1.16 cyclic

21. Let H be a proper subgroup of G. Then $|H| = 1$ and $H < e >$ or $|H| = p$ or q and by Theorem 2.1.16 cyclic

22. $H \cap K$ is a subgroup of both H and K. Hence $|H \cap K|$ is a common divisor of n and m. Since $\gcd(n,m) = 1$,we have $|H \cap K| = 1$ and $H \cap K = \{e\}$

23. Let $H = < a >$ and $K = < b >$. Then by Exercise 22 , $H \cap K = \{e\}$. If for some k $a^k = b^k$, then $a^k = e = b^k$. By Corollary 1.3.12, n must divide k and m must divide k. Finally, by Proposition 0.3.29 we have nm divides k

24. Suffices to show that 3 and 7 divide $n(n^{18} - 1)$. (1) If $3 \mid n$, then $3 \mid n(n^{18} - 1)$. If 3 does not divide n, then $n^2 \equiv 1 \bmod 3$, $n^{18} - 1 \equiv (n^2)^9 - 1 \equiv 0 \bmod 3$and 3 divides $n^{18} - 1$. (2) If 7 divides n, then $7 \mid n(n^{18} - 1)$. If 7 does not divide n, then $n^6 \equiv 1 \bmod 7$, $(n^6)^3 - 1 \equiv 0 \bmod 7$ and 7 divides $n^{18} - 1$

25. $9^{1573} \equiv 9^3 \equiv (-2)^3 \equiv 3 \bmod 11$ **26**. $\varphi(p^2) = p^2 - p = p(p - 1)$

27. $\varphi(pq) = (p - 1)(q - 1)$

28. $\varphi(12) = 4$, therefore by Theorem 2.1.18 , $5^{1258} \equiv (5^4)^{314} 5^2 \equiv 5^2 \equiv 1 \bmod 12$

Exercises 29 and 30 sould be assigned together. Exercises 30 and 32 use a very similar construction.

29. For any $a \in G$ we have $|a| = 1, 2, p$ or $2p$. By Exercise 18 in Section 1.1, since G is not Abelian there exists an element g in G with $g^2 \neq e$. Hence $|g| = p$ or $2p$.

If $|g| = 2p$ then $|g^2| = p$

30. By Exercise 29 there exists an element g in G with $|g| = p$. Let $H = < g >$ and let $a \in G$ such that $a \notin H$. $|a| = 2$ or p since G is not cyclic. Furthermore, $H \cap < a > = \{e\}$, since they are both of prime order and $a \notin H$. $[G:H] = 2$, hence H and aH are the two left cosets of H. The left coset $a^2H \neq aH$ because $a \notin H$, hence $a^2H = H$ and $a^2 \in H \cap < a > = \{e\}$. Therefore, $|a| = 2$. Since there are p elements in G not in H , there are p elements in G of order 2.

31. See Solution of Exercise 19 in Section 1.3

32. Let $a \neq e$ be an element of G. If $|a| = 3$ or 15 we are done since $|a| = 15$ implies $|a^5| = 3$. So assume $|a| = 5$. Let $H = < a >$ and let $b \in G$ such that $b \notin H$. Again if $|b| = 15$ we are done. So assume $|b| = 3$ or 5 . Then $H \cap < b >$ is a proper subgroup of both H and $< b >$, hence $H \cap < b > = \{e\}$ since they are both of prime order and $b \notin H$. $[G : H] = 3$ and H, bH, b^2H are the three distinct left cosets of H. Consider now b^3H. Since $b \notin H$ and $b^2 \notin H$ we obtain $b^3H = H$. Therefore $b^3 \in H \cap < b > = \{e\}$ and $|b| = 3$.

Exercise 33 is assumed in Exercise 35, so the two exercises could be assigned together. The fact shown in Exercise 33 will be used repeatedly in later exercises and should either be assigned as a homework problem or the proof be given in class.

33. First we show that $\{x_iy_jK\}$, where $1 \leq i \leq n$ and $1 \leq j \leq m$, are all the left cosets of K in G. For let $g \in G$, then $g \in x_iH$, for some i , and $g = x_ih$ for some $h \in H$. Also, $h \in y_jK$, for some j and $h = y_jk$ for some $k \in K$. Hence for all $g \in G$ we have $g \in x_iy_jK$ for some i and j. Second we show that the $\{x_iy_jK\}$ are all distinct. If there exists $g \in x_iy_jK \cap x_my_lK$, then $g = x_iy_jk = x_my_lk'$ for some k and k' in K. But this implies that $x_m^{-1}x_i \in H$, since y_jk and y_lk' are in H, thus $x_iH = x_mH$ and $x_i = x_m$. Hence $y_jk = y_lk'$ and $y_l^{-1}y_j \in K$ which implies $y_jK = y_lK$ and $y_j = y_l$.

34. (1) $a = eae$, hence $a \sim a$.(2) If $a \sim b$ then $a = hbk$ which implies $h^{-1}ak^{-1} = b$ and $b \sim a$. (3) If $a \sim b$ and $b \sim c$ then $a = hbk$ and $b = h'ck'$, $a = (hh')c(kk')$ and $a \sim b$

35. By Exercise 33, $[G:H \cap K] = [G:H][H:H \cap K] = n\,[H:H \cap K] = m\,[K:H \cap K]$ and $\text{lcm}(n, m) \leq [G:H \cap K]$. Furthermore, if $s = [H:H \cap K]$ and $h_1(H \cap K)$, . . . , $h_s(H \cap K)$ are the s-distinct left cosets of $H \cap K$ in H then $h_j^{-1}h_i \notin H \cap K$ implies $h_j^{-1}h_i \notin K$ and h_1K, . . . , h_sK are s distinct left cosets of K in G. Therefore, $[H:H \cap K] = s \leq [G:K] = m$ and $[G:H \cap K] \leq nm$

36. Let $s = [H:H \cap K] = |H| / |H \cap K|$ and let $h_1(H \cap K)$, . . . ,$h_s(H \cap K)$ be the s distinct left cosets of $H \cap K$ in H that is $h_j^{-1}h_i \notin H \cap K$. Consider the left cosets h_1K, . . . , h_sK. They are distinct because $h_j^{-1}h_i \notin H \cap K$ and $h_j^{-1}h_i \in H$, hence

$h_j^{-1}h_i \notin K$. Also, given $hk \in HK$ then $h \in h_i(H \cap K)$ for some i, hence $hk \in h_iK$. Therefore, the $\{h_iK\}$ partition HK. Finally, since $|h_iK| = |K|$ we obtain $|HK| = s|K|$.

37. If $\chi(aH) = Ha^{-1}$ then $Ha^{-1} = Hb^{-1}$ implies $b^{-1}a \in H$ and $aH = bH$. Hence χ is one to one. Also, χ is onto since $\chi(b^{-1}H) = Hb$.

38. Let G be any cyclic group of order n. By Exercise 26 in Section 1.3 for every divisor d of n there are exactly $\varphi(d)$ elements of G of order d. Hence
$n = |G| = \sum_{d|n}\varphi(d)$

39. With the notation as in Example 1.4.35, A_4 has 8 elements of order 3, ρ_i, ρ_i^2 $1 \le i \le 4$. Suppose H is a subgroup of A_4 of order 6. Then at least one element of A_4 of order 3 is not in H, let's say $\rho_j \notin H$. Since $\rho_j = (\rho_j^2)^2$ we have $\rho_j^2 \notin H$. Therefore, H, ρ_jH, ρ_j^2H are three distinct left cosets of H. This is impossible since $[A_4:H] = 2$

2.2 Homomorphisms

With this section students should become comfortable with constructions of homomorphisms between two specific groups and identifying the kernel in each case. Proposition 2.2.15 provides them with basic tools. The importance of part (4) of the proposition should be emphasized. Also, part (4) of Proposition 2.2.23 gives them very strong tools for identifying nonisomorphic groups.

Exercises 2.2

1. No, since $\varphi(n + m) = n + m - 1$, while $\varphi(n) + \varphi(m) = n + m - 2$

2. Yes, $\varphi(n + m) = 3(n + m) = 3n + 3m = \varphi(n) + \varphi(m)$ and Kern $\varphi = \{0\}$

3. Yes, $\varphi(xy) = |xy| = |x|\,|y|$ and Ker $\varphi = \{1, -1\}$

4. Yes, $\varphi(AB) = \det AB = \det A \det B = \varphi(A)\,\varphi(B)$ and Kern $\varphi = SL(2,\mathbb{R})$

5. Yes,(1) If σ and τ are both even permutations, then $\sigma\tau$ is also an even permutation, $\varphi(\sigma\tau) = 0$ and $\varphi(\sigma) + \varphi(\tau) = 0 + 0 = \varphi(\sigma\tau)$. (2) If σ and τ are both odd permutations then $\sigma\tau$ is an even permutation, $\varphi(\sigma\tau) = 0$ and $\varphi(\sigma) + \varphi(\tau) = 1 + 1 = 0 = \varphi(\sigma\tau)$. (3) If only one of them is odd, let's say σ, then $\sigma\tau$ is also odd and $\varphi(\sigma\tau) = 1$ and $\varphi(\sigma) + \varphi(\tau) = 1 + 0 = \varphi(\sigma\tau)$. Kern $\varphi = A_3$

6. Yes, $\varphi(\rho^i\tau\,\rho^j\tau) = \varphi(\rho^{i-j}) = 0$ and $\varphi(\rho^i\tau) + \varphi(\rho^j\tau) = 1 + 1 = 0$,
$\varphi(\rho^i\,\rho^j\tau) = \varphi(\rho^{i+j}\tau) = 1$ and $\varphi(\rho^i) + \varphi(\rho^i\tau) = 0 + 1 = 1$. Kern $\varphi = <\rho>$