# Hints and Partial Solutions for *Abstract Algebra, 3rd edition* by David S. Dummit and Richard M. Foote

Mitch Haslehurst

May 21, 2022

# Preliminaries

## 0.1 Basics

1. Computations show that the first, third, and fifth elements are in $\mathcal{B}$, but the second, fourth, and sixth are not.

2. $M(P+Q) = MP + MQ = PM + QM = (P+Q)M$.

3. $M(PQ) = (MP)Q = (PM)Q = P(MQ) = P(QM) = (PQ)M$.

4. We must have

$$\begin{pmatrix} p+r & q+s \\ r & s \end{pmatrix} = \begin{pmatrix} p & p+q \\ r & r+s \end{pmatrix}$$

which means $r = 0$ (since $p + r = p$) and $p = s$ (since $q + s = p + q$). $q$ may be any real number. We see that

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} p & q \\ 0 & p \end{pmatrix} = \begin{pmatrix} p & p+q \\ 0 & p \end{pmatrix} = \begin{pmatrix} p & q \\ 0 & p \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

so the conditions are both necessary and sufficient.

5. The function $f$ in (a) is not well defined since $1/2 = 2/4$, but $1 = f(1/2) \neq f(2/4) = 2$. In (b), however, $f$ is well defined; if $a/b = c/d$, then $ad - bc = 0$, and so $a^2d^2 - b^2c^2 = (ad + bc)(ad - bc) = 0$. It follows that $a^2/b^2 = c^2/d^2$.

6. $f$ is not well defined since decimal representations of real numbers are not necessarily unique. For example, $0.5 = 0.4999\ldots$ so it is not clear whether $f(1/2) = 5$ or $f(1/2) = 4$.

7. It is clear that we have an equivalence relation. Let $E$ be an equivalence class, and pick any $a \in E$. We have

$$f^{-1}(\{f(a)\}) = \{a' \in A : f(a') = f(a)\} = \{a' \in A : a \sim a'\} = E.$$

Conversely, consider a fiber of $f$ over $b \in B$. $f$ is surjective, so pick $c \in A$ so that $f(c) = b$. Then, if $E_c$ is the equivalence class containing $c$,

$$E_c = \{a' \in A : c \sim a'\} = \{a' \in A : f(a') = b\} = f^{-1}(\{b\}).$$

Thus every equivalence class is a fiber, and vice versa.

## 0.2 Properties of the Integers

1. We complete (a); (b) through (f) are omitted. We have

$$\begin{aligned} 20 &= (1)13 + 7 \\ 13 &= (1)7 + 6 \\ 7 &= (1)6 + 1 \\ 6 &= (6)1 \end{aligned}$$

so $(20, 13) = 1$ (though this should have been clear immediately because 13 is prime). The least common multiple is thus $20 \cdot 13 = 260$. Retracing the algorithm, we have

$$\begin{aligned} 1 &= 7 - 6 \\ &= 7 - (13 - 7) \\ &= (20 - 13) - (13 - (20 - 13)) \\ &= 20(2) + 13(-3). \end{aligned}$$

2. $a = kc$ and $b = kd$, so $as + bt = (kc)s + (kd)t = k(cs + dt)$.

3. Since $n$ is composite, it has proper divisors greater than 1: there are integers $a$ and $b$ with $1 < a < n$, $1 < b < n$ and $n = ab$. Then $n \mid ab$, but $n \nmid a$ and $n \nmid b$. If one of these were the case, say, $n \mid a$, then there would be an integer $k > 1$ such that $nk = a$, but then $n < nk = a$.

4.

$$\begin{aligned} a\left(x_0 + \frac{b}{d}t\right) + b\left(y_0 - \frac{a}{d}t\right) &= (ax_0 + by_0) + \left(\frac{ab}{d}t - \frac{ab}{d}t\right) \\ &= N + 0 \\ &= N. \end{aligned}$$

5. The values in the left column are $n$, and those in the right are $\varphi(n)$.

| | |
|---|---|
| 1 | 1 |
| 2 | 1 |
| 3 | 2 |
| 4 | 2 |
| 5 | 4 |
| 6 | 2 |
| 7 | 6 |
| 8 | 4 |
| 9 | 6 |
| 10 | 4 |
| 11 | 10 |

| | |
|---|---|
| 12 | 4 |
| 13 | 12 |
| 14 | 6 |
| 15 | 8 |
| 16 | 8 |
| 17 | 16 |
| 18 | 6 |
| 19 | 18 |
| 20 | 8 |
| 21 | 12 |
| 22 | 10 |
| 23 | 22 |
| 24 | 8 |
| 25 | 20 |
| 26 | 12 |
| 27 | 18 |
| 28 | 12 |
| 29 | 28 |
| 30 | 8 |

6. Suppose $A$ is a subset of $\mathbb{Z}^+$ that does not have a minimal element. For $k \in \mathbb{Z}^+$, let $P(k)$ be the property "for all $m \leq k$, $m \notin A$". Clearly $P(1)$ is true since otherwise 1 would be a minimal element of $A$. Suppose $P(k)$ is true for an arbitrary value of $k$. To show that $P(k+1)$ is true, suppose it is false. Then there is an integer $m$ with $m \leq k+1$ and $m \in A$. If $m < k+1$, then $m \leq k$ and $m \in A$, contradicting the truth of $P(k)$. If $m = k+1$, then $k+1$ is a minimal element of $A$ since all integers less than $k+1$ are not in $A$ by the truth of $P(k)$; this cannot be. It follows that $P(k+1)$ is true. By induction, $P(k)$ is true for all postive integers, and $P(k)$ asserts in particular that $k \notin A$. This means that $A$ is empty, and thus that $\mathbb{Z}^+$ is well-ordered.

   Uniqueness of the minimal element is straightforward: If $m$ and $m'$ are two minimal elements of $A$, then $m \leq m'$ because $m$ is minimal, and $m' \leq m$ because $m'$ is minimal. Hence $m = m'$.

7. Suppose there do exist integers $a$ and $b$ with $a^2 = pb^2$. Without loss of generality, suppose that both are postive and $(a, b) = 1$. $a^2$ is divisible by $p$ and thus $a$ is divisible by $p$ (if $p$ does not occur in the factorization of $a$, then it certainly does not in $a^2$). So $a = pk$ for some integer $k$, and thus $a^2 = (pk)^2 = p^2k^2 = pb^2$. This simplifies to $b^2 = pk^2$. A similar argument then shows that $b$ is divisible by $p$, contradicting $(a, b) = 1$.

8. For a fixed prime $p$, let $\nu_p(n)$ be the highest power of $p$ which divides $n$. The formula we seek is

$$\nu_p(n!) = \sum_{i=1}^{\infty} \left[ \frac{n}{p^i} \right].$$

   The following solution is from:

   https://en.wikipedia.org/wiki/Legendre%27s_formula on July 17, 2017.

"Since $n!$ is the product of the integers 1 through $n$, we obtain at least one factor of $p$ in $n!$ for each multiple of $p$ in $\{1, 2, \ldots, n\}$, of which there are $[n/p]$. Each multiple of $p^2$ contributes an additional factor of $p$, each multiple of $p^3$ contributes yet another factor of $p$, etc. Adding up the number of these factors gives the infinite sum for $\nu_p(n!)$."

9. (Omitted)

10. Let $N$ be given. If $n$ is such that $\varphi(n) = N$, then the prime divisors of $n$ must not exceed $N + 1$, for if $p$ divides $n$ and $p > N + 1$, then $n = p^k m$ for some $m$ and $\varphi(n) = \varphi(p^k m) = \varphi(p^k)\varphi(m) \geq p - 1 > N$, a contradiction. So the prime divisors of $n$ must be among the integers $1, 2, \ldots, N + 1$.

    Write $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$. Note that the prime divisors of $n$ were taken from the set $\{1, 2, \ldots, N+1\}$, so the only way there could be infinitely many such $n$ is if the exponents $\alpha_i$ could be arbitrarily large. But this is also impossible: $\varphi(n) = p_1^{\alpha_1 - 1}(p_1 - 1)p_2^{\alpha_2 - 1}(p_2 - 1) \cdots p_s^{\alpha_s - 1}(p_s - 1)$ and so $\varphi(n) \geq p_i^{\alpha_i - 1}$ for every $i$. Thus there must be an upper bound on the possibilities for each $\alpha_i$, since otherwise we might have $\varphi(n) \geq p_i^{\alpha_i - 1} > N$.

    In sum, if $n$ is such that $\varphi(n) = N$, then the prime divisors of $n$ are contained in the finite set $\{1, 2, \ldots, N + 1\}$ and the powers of these primes are bounded above, which means there are only finitely many possibilities for such $n$.

11. If $d$ divides $n$, then every prime in the factorization of $d$ occurs in the factoriztion on $n$ with an equal or greater exponent: if $d = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, then $n = p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s} p_{s+1}^{\beta_{s+1}} \cdots p_t^{\beta_t}$ where $\alpha_i \leq \beta_i$ for all $i$ such that $1 \leq i \leq s$. Then, using the useful formula for the Euler $\varphi$-function,

$$\varphi(d) = p_1^{\alpha_1 - 1}(p_1 - 1)p_2^{\alpha_2 - 1}(p_2 - 1) \cdots p_s^{\alpha_s - 1}(p_s - 1)$$

    and

$$\varphi(n) = p_1^{\beta_1 - 1}(p_1 - 1)p_2^{\beta_2 - 1}(p_2 - 1) \cdots p_t^{\beta_t - 1}(p_t - 1).$$

    Now it it easy to see that each factor of the form $p_i - 1$ of $\varphi(d)$ is a factor of $\varphi(n)$, as is each factor of the form $p_i^{\alpha_i - 1}$ (since $\alpha_i \leq \beta_i$, it is true that $\alpha_i - 1 \leq \beta_i - 1$).

## 0.3 $\mathbb{Z}/n\mathbb{Z}$: The Integers Modulo $n$

1. Perhaps not so explicitly, the residue classes are

$$\begin{aligned} \overline{0} &= \{\ldots, -36, -18, 0, 18, 36, \ldots\}, \\ \overline{1} &= \{\ldots, -35, -17, 1, 19, 37, \ldots\}, \\ &\vdots \\ \overline{17} &= \{\ldots, -19, -1, 17, 35, 53, \ldots\}. \end{aligned}$$

2. Let $n$ be a fixed positive integer. It is clear that $\overline{0}, \overline{1}, \ldots, \overline{n-1}$ are all distinct, since if $i, j \in \{0, 1, \ldots, n-1\}$ and $i \neq j$, then $0 < |i - j| < n$ and so neither $i$ nor $j$ differs from the other by a multiple of $n$. Now suppose $k$ is any other integer besides $0, 1, \ldots, n-1$. By the

Division Algorithm, there are unique integers $q$ and $r$ such that $k = qn + r$ and $0 \leq r < n$. But the condition $0 \leq r < n$ implies that $r \in \{0, 1, \ldots, n-1\}$. Thus $k - r = qn$ and $k$ differs from one of the integers $0, 1, \ldots, n-1$ by a multiple of $n$, which implies that it must be a member of one of $\overline{0}, \overline{1}, \ldots, \overline{n-1}$.

3. Note that since $10 \equiv 1 \mod 9$, we have $10^k \equiv 1^k \equiv 1 \mod 9$ for all integers $k$. So

$$a = a_n 10^n + \cdots + a_1 10 + a_0 \equiv a_n + \cdots + a_0 \mod 9$$

using the rules derived in Theorem 3.

4. $37 \equiv 8 \mod 29$, so $37^2 \equiv 8^2 = 64 \equiv 6 \mod 29$. Continuing in this way using powers of 2 as exponents,

$$\begin{aligned}
37^4 = (37^2)^2 \equiv 6^2 = 36 \equiv 7 \mod 29, \\
37^8 = (37^4)^2 \equiv 7^2 = 49 \equiv 20 \mod 29, \\
37^{16} = (37^8)^2 \equiv 20^2 = 400 = 10 \cdot 40 \equiv 10 \cdot 11 = 110 \equiv 23 \mod 29, \\
37^{32} = (37^{16})^2 \equiv 23^2 = 529 = 580 - 51 \equiv 0 - 51 \equiv 7 \mod 29, \\
37^{64} = (37^{32})^2 \equiv 7^2 \equiv 20 \mod 29.
\end{aligned}$$

Then, $37^{100} = 37^{64}37^{32}32^4 \equiv 20 \cdot 7 \cdot 7 = 35 \cdot 28 \equiv 6 \cdot 28 = 42 \cdot 4 \equiv 13 \cdot 4 = 52 \equiv 23 \mod 29$.

5.

$$\begin{aligned}
9^3 = 729 \equiv 29 \mod 100, \\
9^6 = (9^3)^2 \equiv 29^2 = 841 \equiv 41 \mod 100, \\
9^{12} = (9^6)^2 \equiv 41^2 = 1681 \equiv 81 \mod 100, \\
9^{24} = (9^{12})^2 \equiv 81^2 = 6561 \equiv 61 \mod 100, \\
9^{48} = (9^{24})^2 \equiv 61^2 = 3721 \equiv 21 \mod 100, \\
9^{96} = (9^{48})^2 \equiv 21^2 = 441 \equiv 41 \mod 100,
\end{aligned}$$

after which we see a pattern emerge. From this point,

$$\begin{aligned}
9^{192} \equiv 81 \mod 100, \\
9^{384} \equiv 61 \mod 100, \\
9^{768} \equiv 21 \mod 100.
\end{aligned}$$

Finally, $9^{1500} = 9^{768}9^{384}9^{192}9^{96}9^{48}9^{12} \equiv 21 \cdot 61 \cdot 81 \cdot 41 \cdot 21 \cdot 81 \equiv 41^2 \cdot 61^2 \equiv 41^2 \cdot 21 = 35301 \equiv 1 \mod 100$, so the last two digits are 0 and 1.

6. $0^2 \equiv 0 \mod 4$, $1^2 \equiv 1 \mod 4$, $2^2 = 4 \equiv 0 \mod 4$, and $3^2 = 9 \equiv 1 \mod 4$.

7. By the previous exercise, the only possibilities for squares are to be 0 or 1 in $\mathbb{Z}/4\mathbb{Z}$. Thus, for a sum of squares, the only posibilities are $0+0=0$, $0+1=1+0=1$, or $1+1=2$, eliminating 3 as a possibility.

8. Suppose there are solutions for nonzero integers $a$, $b$ and $c$. We can assume that $a$, $b$ and $c$ have no factors in common. By Exercise 6, $c^2$ is either 0 or 1 in $\mathbb{Z}/4\mathbb{Z}$, so $3c^2$ is either 0 or 3. By Exercise 7, $a^2+b^2$ is not 3 in $\mathbb{Z}/4\mathbb{Z}$ so it must be that $3c^2 \equiv 0 \mod 4$. This means that $a^2+b^2$ is disvisible by 4, which means that $a$ and $b$ must both be even (if they were both odd, then it is easily checked that $a^2+b^2 = 4k+2$ for some integer $k$). $c$ must also be even if $3c^2$ is to be divisible by 4. All three being even contradicts the fact that they have no factors in common.

9. It's enough to check that all of the odd elements in $\mathbb{Z}/8\mathbb{Z}$ yield 1 when squared. Indeed, $1^2 \equiv 1$, $3^2 = 9 \equiv 1$, $5^2 = 25 \equiv 1$ and $7^2 = 49 \equiv 1$.

10. This will follow once we prove Proposition 4 in Excercises 12-14.

11. Since $\overline{a}$ and $\overline{b}$ are in $(\mathbb{Z}/n\mathbb{Z})^\times$, there are $\overline{c}$ and $\overline{d}$ such that $\overline{a}\cdot\overline{c} = \overline{1}$ and $\overline{b}\cdot\overline{d} = \overline{1}$. Then $(\overline{a}\cdot\overline{b})\cdot(\overline{d}\cdot\overline{c}) = \overline{a}\cdot(\overline{b}\cdot\overline{d})\cdot\overline{c} = \overline{a}\cdot\overline{1}\cdot\overline{b} = \overline{a}\cdot\overline{c} = \overline{1}$.

12. Let $d$ be a common divisor of $a$ and $n$ which is greater than 1. Let $b = n/d$. Then $0 < b < n$ and since $a = kd$ for some integer $k$, $ab = (kd)(n/d) = kn \equiv 0 \mod n$. If there were an integer $c$ such that $ac \equiv 1 \mod n$, then $b = b\cdot 1 \equiv b(ac) = (ba)c \equiv 0\cdot c \equiv 0 \mod n$, which is a contradiction since $0 < b < n$.

13. Write $ax + ny = 1$ for some integers $x$ and $y$. Then $ax$ differs from 1 by a multiple of $n$, and so $ax \equiv 1 \mod n$. We also see that the multiplicative inverse of $\overline{a}$ in $\mathbb{Z}/n\mathbb{Z}$ is given by $\overline{x}$.

14. From the previous two exercises, we see that $\overline{a}$ has a multiplicative inverse in $(\mathbb{Z}/n\mathbb{Z})^\times$ if and only if $(a,n) = 1$. For the case $n = 12$, we have $1\cdot 1 \equiv 1$, $5\cdot 5 = 25 \equiv 1 \mod 12$, $7\cdot 7 = 49 \equiv 1 \mod 12$, and $11\cdot 11 = 121 \equiv 1 \mod 12$ (they all happen to be their own inverses). Meanwhile, $2\cdot 6 = 12 \equiv 0 \mod 12$, $3\cdot 4 = 12 \equiv 0 \mod 12$, $4\cdot 3 = 12 \equiv 0 \mod 12$, $6\cdot 2 = 12 \equiv 0 \mod 12$, $8\cdot 3 = 24 \equiv 0 \mod 12$, $9\cdot 4 = 36 \equiv 0 \mod 12$, and $10\cdot 6 = 60 \equiv 0 \mod 12$.

15. We do (a). In Exercise 1 in Section 0.2 we found that 13 and 20 are relatively prime. We also found that $1 = 20(2) + 13(-3)$, so the multiplicative inverse of 13 in $\mathbb{Z}/20\mathbb{Z}$ is equivalent to $-3$. The number we seek is thus $-3 + 20 = 17$. Indeed, $13\cdot 17 = 201 \equiv 1 \mod 20$.

16. (Omitted)

# Part I

# Group Theory

# Chapter 1

# Introduction to Groups

## 1.1 Basic Axioms and Examples

1. (a) No: $(1-1)-1=-1\neq 1=1-(1-1)$.
   (b) Yes: $(a\star b)\star c=(a\star b)+c+(a\star b)c=(a+b+ab)+c+(a+b+ab)c$ and $a\star(b\star c)=a+(b\star c)+a(b\star c)=a+(b+c+bc)+a(b+c+bc)$. Simplifying both expressions reveals that they are both equal to $a+b+c+ab+bc+ac+abc$.
   (c) No: $(1\star 1)\star 2=2/5\star 2=(2/5+2)/5=12/25\neq 8/25=(1+3/5)/5=1\star 3/5=1\star(1\star 2)$
   (d) Yes: $[(a,b)\star(c,d)]\star(e,f)=(ad+bc,bd)\star(e,f)=([ad+bc]f+bde,bdf)=(adf+b[cf+de],bdf)=(a,b)\star(cf+de,df)=(a,b)\star[(c,d)\star(e,f)]$. (Note the similarity to the operation of adding rational numbers.)
   (e) No: $(1\star 1)\star 2=1\star 2=1/2\neq 2=1\star(1/2)=1\star(1\star 2)$.

2. (a) No: $1-0=1\neq -1=0-1$.
   (b) Yes: $a\star b=a+b+ab=b+a+ba=b\star a$.
   (c) Yes: $a\star b=(a+b)/5=(b+a)/5=b\star a$.
   (d) Yes: $(a,b)\star(c,d)=(ad+bc,bd)=(cb+da,db)=(c,d)\star(a,b)$.
   (e) No: $1/2\neq 2/1$.

3. $(\overline{a}+\overline{b})+\overline{c}=\overline{a+b}+\overline{c}=\overline{(a+b)+c}=\overline{a+(b+c)}=\overline{a}+\overline{b+c}=\overline{a}+(\overline{b}+\overline{c})$.

4. Same idea as in Exercise 3.

5. The element $\overline{0}$ does not have an inverse since $\overline{0}\cdot\overline{k}=\overline{0k}=\overline{0}$ for all $k$.

6. (a) Yes, since the least common multiple of two odd numbers is odd.
   (b) No: $1/2+1/2=1/1$ and 1 is not even.
   (c) No: $1/2+1/2=1$ and $1\not<1$.
   (d) No: $2+(-3/2)=1/2$ and $1/2\not\geq 1$.
   (e) Yes, since the least common multiple of 1 and 2 is 2.

(f) No: $1/2 + 1/3 = 5/6$.

7. Suppose $x = x'$ and $y = y'$ in $G$. Then $x + y = x' + y'$ and so $[x + y] = [x' + y']$. This implies that $x + y - [x + y] = x' + y' - [x' + y']$, and thus the binary operation is well defined. We have $(x \star y) \star z = (x + y - [x + y]) \star z = (x + y - [x + y]) + z - [(x + y - [x + y]) + z]$ and $x \star (y \star z) = x \star (y + z - [y + z]) = x + (y + z - [y + z]) - [x + (y + z - [y + z])]$, so we want to show that

$$(x + y - [x + y]) + z - [(x + y - [x + y]) + z] = x + (y + z - [y + z]) - [x + (y + z - [y + z])].$$

Immediately cancelling $x + y + z$, we are left with

$$-[x + y] - [(x + y - [x + y]) + z] = -[y + z] - [x + (y + z) - [y + z])]. \tag{1.1}$$

Note that since $x$, $y$, and $z$ are all less than 1, $x+y < 2$ and $y+z < 2$. So the only possibilities for $[x + y]$ and $[y + z]$ are 0 and 1. If both are 0, then (1.1) becomes

$$-[x + y + z] = -[x + y + z],$$

which is true. The case when $[x + y] = [y + z] = 1$ is similar. If $[x + y] = 1$ and $[y + z] = 0$, then

$$-1 - [(x + y - 1) + z] = -[x + y + z].$$

Since $[x - 1] = [x] - 1$ for all real numbers $x$, it follows that

$$-1 - [(x + y - 1) + z] = -1 - [x + y + z] + 1 = -[x + y + z]$$

which shows that (1.1) is true in this case as well. The case when $[x + y] = 0$ and $[y + z] = 1$ is similar. The computation

$$x \star 0 = x + 0 - [x + 0] = x - [x] = x - 0 = x$$

as well as the similar computation for $0 \star x$ shows that 0 is the identity. The inverse of $x$ is $1 - x$, since

$$x \star (1 - x) = x + (1 - x) - [x + (1 - x)] = 1 - [1] = 0$$

(again, the computation for $(1 - x) \star x$ is similar). It is easy to see that $G$ is abelian:

$$x \star y = x + y - [x + y] = y + x - [y + x] = y \star x.$$

8. First note that $G$ is all complex numbers on the unit circle, i.e., of modulus 1 (this is easily shown by ruling out the cases $|z| < 1$ and $|z| > 1$). Suppose $w^m = 1$ and $z^n = 1$. Then $(wz)^{mn} = w^{mn}z^{mn} = (w^m)^n(z^n)^m = 1^n 1^m = 1$. Associativity is inherited from $\mathbb{C}$. The identity is 1, and the inverse of $z$ is $\overline{z}$ (complex conjugate): $z\overline{z} = |z|^2 = 1$. Thus (a) has been shown, and (b) is easily seen to be true since $1 + 1 = 2 \notin G$.

9. (a) $(a+b\sqrt{2})+(c+d\sqrt{2}) = (a+b)+(c+d)\sqrt{2}$. The identity is $0 = 0+0\sqrt{2}$ and the inverse of $a + b\sqrt{2}$ is $-a - b\sqrt{2}$. Associativity is inherited from $\mathbb{R}$.

   (b) $(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$. The identity is $1 = 1 + 0\sqrt{2}$, and the inverse of $a + b\sqrt{2}$ is $a/(a^2 + 2b^2) - b\sqrt{2}/(a^2 + 2b^2)$.

10. The matrix is symmetric if and only if the $i, j$ entry is equal to the $j, i$ entry for all $i$ and $j$, and this is if and only if $g_i g_j = g_j g_i$ for all $i$ and $j$.

11. The orders of $\overline{0}, \overline{1}, \ldots, \overline{11}$ are, respectively, $1, 12, 6, 4, 3, 12, 2, 12, 3, 4, 6, 12$.

12. The orders are, respectively, $1, 2, 2, 2, 2, 1$.

13. The orders are, respectively, $36, 18, 6, 4, 18, 3, 36, 18, 2$.

14. The orders are, respectively, $1, 2, 36, 36, 36, 36$.

15. We have $a_1 a_2 a_2^{-1} a_1^{-1} = a_1 a_1^{-1} = 1$, so it is true for $n = 2$. If it is true for $n = k - 1$, then

$$(a_1 a_2 \cdots a_k)^{-1} = a_k^{-1}(a_1 a_2 \cdots a_{k-1})^{-1} = a_k^{-1} a_{k-1}^{-1} \cdots a_1^{-1}.$$

16. Since $x^2 = 1$, $|x| \leq 2$. The other direction is just as easy.

17. We need to show that $x^{n-1}$ is the inverse of $x$, or that $xx^{n-1} = x^{n-1}x = 1$. We have

$$xx^{n-1} = x\overbrace{xx\cdots x}^{n-1} = \overbrace{xx\cdots x}^{n} = x^n = 1,$$

    and similarly for $x^{n-1}x$.

18. Easy.

19. (a) We have

$$x^{a+b} = \overbrace{xx\cdots x}^{a+b} = \overbrace{xx\cdots x}^{a}\overbrace{xx\cdots x}^{b} = x^a x^b,$$

    and thus

$$(x^a)^b = \overbrace{x^a x^a \cdots x^a}^{b} = x^{\overbrace{a + a + \cdots + a}^{b}} = x^{ab}.$$

    (b) Use Exercise 15.

(c) Suppose $a > 0$, $b < 0$, and $a + b < 0$. This means that $a < -b$ and so

$$x^a x^b = \overbrace{xx\cdots x}^{a}\overbrace{x^{-1}x^{-1}\cdots x^{-1}}^{-b} = \overbrace{xx\cdots x}^{a}(\overbrace{xx\cdots x}^{a})^{-1}\overbrace{x^{-1}x^{-1}\cdots x^{-1}}^{-b-a} = 1\overbrace{x^{-1}x^{-1}\cdots x^{-1}}^{-b-a} = x^{a+b},$$

where the second equality used part (b). The other cases are no harder.

20. Suppose $|x| = n$. By Exercise 15 we have $(x^{-1})^n = (x^n)^{-1} = 1^{-1} = 1$, so $|x^{-1}| \leq n$. But if $k < n$, then $(x^{-1})^k = (x^k)^{-1} \neq 1^{-1} = 1$, so $|x^{-1}| = n$.

21. If $n$ is odd, then $n = 2k - 1$ for some integer $k \geq 1$. Then, using Exercise 19, $1 = x^n = x^{2k-1} = x^{2k}x^{-1} = (x^2)^k x^{-1}$, and multiplying on the right by $x$ gives $x = (x^2)^k$.

22. Let $|x| = n$. Then

$$(g^{-1}xg)^n = g^{-1}xgg^{-1}xg\cdots g^{-1}xg = g^{-1}x^n g = g^{-1}g = 1$$

so $|g^{-1}xg| \leq n$. But if $|g^{-1}xg| = k < n$, then $g^{-1}x^k g = 1$ and so $|x| \leq k$, a contradiction. The conclusion that $|ab| = |ba|$ follows from letting $x = ab$ and $g = a$.

23. $(x^s)^t = x^{st} = x^n = 1$, so $|x^s| \leq t$. If $r < t$, then $sr < st = n$ and so $(x^s)^r = x^{sr} \neq 1$. Thus $|x^s| \neq r$ and $|x^s| = t$.

24. The $n = 1$ case is trivial. Suppose it is true for an arbitrary value of $n$. Then

$$(ab)^{n+1} = (ab)^n(ab) = a^n b^n ab = a^n ab^n b = a^{n+1}b^{n+1}.$$

We were able to interchange $a$ and $b^n$ since $a$ and $b$ commute. Now we consider the case when $n$ is negative.

$$(ab)^{-n} = ((ab)^{-1})^n = (b^{-1}a^{-1})^n = (a^{-1}b^{-1})^n = a^{-n}b^{-n}.$$

25. Let $x$ and $y$ be in $G$. Then, because $x^2 = y^2 = (xy)^2 = 1$, $xyxy = xxyy$. Multiplying both sides on the left by $x^{-1}$ and on the right by $y^{-1}$ yields $xy = yx$.

26. Because $H$ is closed under the operation restricted to $G$, the operation is a well-defined binary operation when viewed only on $H$. Associativity of the operation follows from being true in $G$. The presence of the identity is given from the fact that products and inverses remain in $H$, and so $hh^{-1} = 1 \in H$. Inverses are given to be in $H$.

27. Let $H = \{x^n : n \in \mathbb{Z}\}$. Write two arbitrary elements in $H$ as $x^m$ and $x^k$. Then $x^m x^k = x^{m+k}$, so their product is in $H$. 1 is in $H$ since $x^0 = 1$, and the inverse of $x^m$ is easily checked to be $x^{-m}$.

28. Easy.

29. If both $A$ and $B$ are abelian, then $(a_1, b_1)(a_2, b_2) = (a_1a_2, b_1b_2) = (a_2a_1, b_2b_1) = (a_2, b_2)(a_1, b_1)$. If $A$ is not abelian, then there are elements $x$ and $y$ in $A$ such that $xy \neq yx$. Then $(x, 1)(y, 1) = (xy, 1) \neq (yx, 1) = (y, 1)(x, 1)$. If $B$ is not abelian, a similar proof works.

30. $(a,1)(1,b) = (a,b) = (1,b)(a,1)$. Let $|a| = m$ and $|b| = n$. Then $(a,1)^m = (a^m, 1^m) = (1,1)$ and $(1,b)^n = (1^n, b^n) = (1,1)$. If $k$ is the least common multiple of $m$ and $n$, then $a^k = b^k = 1$ and so $(a,b)^k = [(a,1)(1,b)]^k = (a,1)^k(1,b)^k = (1,1)(1,1) = (1,1)$. Now suppose $|(a,b)| = \ell < k$. Then $\ell$ is not a multiple of at least one of $m$ and $n$; suppose it is not a multiple of $m$ without loss of generality. Then $\ell = mq + r$ where $0 < r < m$, and $(a,b)^\ell = (a^\ell, b^\ell)$ as before. Now $a^\ell = a^{mq+r} = (a^m)^q a^r = 1^q a^r = a^r \neq 1$ since $0 < r < |a|$. So it cannot be that $(a^\ell, b^\ell) = (1,1)$.

31. $t(G)$ can be partitioned into sets of the form $\{g, g^{-1}\}$ for $g \in t(G)$, each of which have cardinality 2 since $g \neq g^{-1}$ (note that if $g \in t(G)$, then $g^{-1} \in t(G)$). $t(G)$ is thus a disjoint union of two-element sets and so has even cardinality. This means that $G - t(G)$ has even cardinality as well. But the cardinality of $G - t(G)$ cannot be 0 since it contains 1. So it is at least 2, and thus contains at least one nonidentity element, say $h$. Then $h = h^{-1}$, and multiplying by $h$ gives $h^2 = 1$.

32. Suppose there are integers $i$ and $j$ with $0 \leq i < j < n$ and $x^i = x^j$. Multiplying both sides by $x^{n-j}$ gives $x^{n+(i-j)} = 1$. This is a contradiction since $0 < n + (i-j) < n$. It follows that $G$ contains at least $n$ elements, so $|x| = n \leq |G|$.

33. For (a), suppose $x^i = x^{-i}$ for some $i = 1, 2, \ldots, n-1$. Multiply both sides by $x^i$ to get $x^{2i} = 1$. Thus $2i$ is a multiple of $n$, but $2i < 2n$, so $2i = n$. This contradicts $n$ being odd. For (b), suppose $x^i = x^{-i}$. Then, as before, we obtain $2i = n$, and so $i = k$. Conversely, if $i = k$, then $x^n = x^{2k} = x^{2i} = 1$ which implies that $x^i = x^{-i}$.

34. Suppose $i$ and $j$ are integers with $i < j$ and $x^i = x^j$. Multiply both sides by $x^{-i}$ to get $x^{j-i} = 1$, which is a contradiction since $x$ has infinite order.

35. Let $m$ be an arbitrary integer. By the Division Algorithm, there are integers $q$ and $r$ such that $0 \leq r < n$ and $m = nq + r$. Then $x^m = x^{nq+r} = (x^n)^q x^r = 1^q x^r = x^r$. Since $0 \leq r < n$, $x^r$ is a member of the set $\{1, x, x^2, \ldots, x^{n-1}\}$.

36.

## 1.2 Dihedral Groups

1. For $D_6$, $|1| = 1$, $|r| = 3$, $|r^2| = 3$, $|s| = 2$, $|sr| = 1$, $|sr^2| = 2$.
For $D_8$, $|1| = 1$, $|r| = 4$, $|r^2| = 2$, $|r^3| = 4$, $|s| = 2$, $|sr| = 2$, $|sr^2| = 2$, $|sr^3| = 1$.
For $D_{10}$, $|1| = 1$, $|r| = 5$, $|r^2| = 5$, $|r^3| = 5$, $|r^4| = 5$, $|s| = 2$, $|sr| = 2$, $|sr^2| = 2$, $|sr^3| = 2$, $|sr^4| = 2$.

2. By the discussion in the text, $x = sr^k$ for some $k = 0, 1, \ldots, n-1$. Then $rx = r(sr^k) = (rs)r^k = sr^{-1}r^k = sr^{k-1} = (sr^k)r^{-1} = xr^{-1}$.

3. Let $x = sr^k$ as in the previous exercise. If $k$ is 0, then $x$ clearly has order 2. Suppose $x$ has order 2 when $k$ is arbitrary. Then

$$(sr^{k+1})^2 = sr^{k+1}sr^{k+1} = sr^k(rs)r^{k+1} = sr^k sr^{-1}r^{k+1} = sr^k sr^k = 1$$

by the induction hypothesis. Since $r = s(sr)$, an arbitrary element of $D_{2n}$ can be written as $s^i r^k = s^i (ssr)^k$.

4. Clearly $r^k$ has order 2. We have $(r^k)(s^i r^j) = s^i r^{-k} r^j = s^i r^j r^{-k} = (s^i r^j)(r^k)$ since $r^k = r^{-k}$. It is easy to see that the condition $r^k = r^{-k}$ is also necessary for $r^k$ to commute with every element, so if $k \neq n/2$, then $r^k$ does not commute with every element. It is also easy to check that $sr^k$ does not commute with $r$.

5. As we saw in the previous exercise, if $r^k$ commutes with all elements we must have $r^{2k} = 1$. But then $n = 2k$, which contradicts $n$ being odd.

6. Since $|x| = |y| = 2$, we have $x = x^{-1}$ and $y = y^{-1}$. It follows that $tx = (xy)x = x(yx) = x(y^{-1}x^{-1}) = x(xy)^{-1} = xt^{-1}$.

7. First we establish that the original relations follow from the new ones. $a = s$, so $s^2 = a^2 = 1$. $r = ab$, so $r^n = (ab)^n = 1$. To see that $rs = sr^{-1}$, use the previous exercise with $x = a$ and $y = b$ (and thus $t = r$). Now we show that the original relations imply the new ones. Showing that $a^2 = 1$ and $(ab)^n = 1$ would be analogous to before. By Exercise 3, $b = sr$ has order 2.

8. The order of said group is $n$: it is the group $\{1, r, r^2, \ldots, r^{n-1}\}$.

9. There are 4 faces on a tetrahedron and 3 vertices on each face. So once a face is fixed in one of the 4 possible positions, there are 3 positions for the 3 vertices, so $|G| = 4 \cdot 3 = 12$.

10. 6 faces and 4 vertices on each face, so $|G| = 6 \cdot 4 = 24$.

11. 8 faces and 3 vertices on each face, so $|G| = 8 \cdot 3 = 24$.

12. 12 faces and 5 vertices on each face, so $|G| = 12 \cdot 5 = 60$.

13. 20 faces and 3 vertices on each face, so $|G| = 20 \cdot 3 = 60$.

14. An obvious choice would be $\mathbb{Z} = \langle 1 \rangle$. Another would be any pair of relatively prime integers, such as $\mathbb{Z} = \langle 2, 3 \rangle$.

15. $\mathbb{Z}/n\mathbb{Z} = \langle \overline{1} : n \cdot \overline{1} = \overline{0} \rangle$ (recall that 0 is the identity, not 1).

16. Since $x_1 y_1 x_1 y_1 = 1$ and $y_1 = y_1^{-1}$, we easily deduce that $x_1 y_1 = y_1 x_1^{-1}$. This shows that the group is $D_{2n}$ for some $n$, and the fact that $n = 2$ follows from $x_1^2 = 1$.

17. It was shown in the text that $x^3 = 1$, and explained how every element can be written in the form $y^k x^i$. So the elements of the group, listed exhaustively, are $1, x, x^2, y, yx, yx^2$. So if $n$ is a multiple of 3, then we must have $n = 3$ since $x^3 = 1$. So in the case of (a), $|X_{2n}| = 6$. If $(3, n) = 1$, then there are integers $a$ and $b$ such that $3a + nb = 1$, and so

$$x = x^1 = x^{3a+nb} = x^{3a} x^{nb} = (x^3)^a (x^n)^b = 1^a 1^b = 1$$

in the case of (b). From the exhaustive list above, we see that the only elements are 1 and $y$.

18. (a) is easy. Following the hint for (b), we have

$$v^2u^3v = (v^2u^2)(uv) = (uv)(uv) = (uv)(v^2u^2) = u(v^3)u^2 = u^3.$$

Using part (a), we then have $v^{-1}u^3v = u^3$, so $v$ commutes with $u^3$. For (c), we have $u^9 = u$ since $u^4 = 1$, and thus

$$uv = u^9v = (u^3)^3v = v(u^3)^3 = vu^9 = vu.$$

Since $u$ and $v$ commute, we have $uv = v^2u^2 = (uv)^2$, and thus $uv = 1$. Having established (d), we now have

$$1 = u^4v^3 = uuu(uv)vv = uu(uv)v = u(uv) = u$$

and thus $v = 1$ also by (d).

## 1.3 Symmetric Groups

1. $\sigma = (1\ 3\ 5)(2\ 4)$, $\tau = (1\ 5)(2\ 3)$, $\sigma^2 = (1\ 5\ 3)$, $\sigma\tau = (2\ 5\ 3\ 4)$, $\tau\sigma = (1\ 2\ 4\ 3)$, and since $\tau^2 = 1$, $\tau^2\sigma = \sigma$.

2. $\sigma = (1\ 13\ 5\ 10)(3\ 15\ 8)(4\ 14\ 11\ 7\ 12\ 9)$,
$\tau = (1\ 14)(2\ 9\ 15\ 13\ 4)(3\ 10)(5\ 12\ 7)(8\ 11)$,
$\sigma^2 = (1\ 5)(3\ 8\ 15)(4\ 11\ 12)(7\ 9\ 14)(10\ 13)$,
$\sigma\tau = (1\ 11\ 3)(2\ 4)(5\ 9\ 8\ 7\ 10\ 15)(13\ 14)$,
$\tau\sigma = (1\ 4)(2\ 9)(3\ 13\ 12\ 15\ 11\ 5)(8\ 10\ 14)$, and
$\tau^2\sigma = (1\ 2\ 15\ 8\ 3\ 4\ 14\ 11\ 12\ 13\ 7\ 5\ 10)$.

3. The orders are, respectively, $6, 2, 3, 4, 4, 36, 30, 6, 6, 13$.

4. Use Exercise 15.

5. $|(1\ 12\ 8\ 10\ 4)(2\ 13)(5\ 11\ 7)(6\ 9)| = 30$ by Exercise 15.

6. $(1\ 2\ 3\ 4)$, $(1\ 2\ 4\ 3)$, $(1\ 3\ 2\ 4)$, $(1\ 3\ 4\ 2)$, $(1\ 4\ 2\ 3)$, $(1\ 4\ 3\ 2)$.

7. $(1\ 2)$, $(1\ 3)$, $(1\ 4)$, $(2\ 3)$, $(2\ 4)$, $(3\ 4)$, $(1\ 2)(3\ 4)$, $(1\ 3)(2\ 4)$, $(1\ 4)(2\ 3)$.

8. The permutations

$$\sigma_n(k) = \begin{cases} k+1 & 1 \le k \le n-1 \\ 1 & k = n \\ k & k \ge n \end{cases}$$

are in $S_\Omega$ for every $n$, and $\sigma_m \neq \sigma_n$ if $m \neq n$ because if $m < n$, say, then $\sigma_m(n) = n$ while $\sigma_n(n) = 1$. This shows the existence of countably many elements in $S_\Omega$.

9. For (a), 5, 7 and 11. For (b), 3, 5, 7. For (c), 3, 5, 7, 9, 11, 13.

10. If $k+i \leq m$, then $\sigma^i(a_k) = \sigma^{i-1}(\sigma(a_k)) = \sigma^{i-1}(a_{k+1}) = \cdots = \sigma(a_{k+i-1}) = a_{k+i}$. If $k+i > m$, let $j = m-k$. Then $\sigma^i(a_k) = \sigma^{i-j}(\sigma^j(a_k)) = \sigma^{i-j}(a_m) = \sigma^{i-j-1}(a_1) = a_{i-j}$, and $i-j \equiv k+i \mod m$.

11.

12.

13.

14.

15.

16.

17.

18.

19.

20.

## 1.4 Matrix Groups

1. We seek the number of elements of the form

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \text{ where } a, b, c, d \in \mathbb{F}_2 \text{ and } ad - bc \neq 0.$$

Since $\mathbb{F}_2$ consists only of the elements 0 and 1,

2.

3.

4. Use Exercise 12 in Section 0.3.

## 1.5 The Quaternion Group

1. $|1| = 1$, $|-1| = 2$, and $|i| = |j| = |k| = |-i| = |-j| = |-k| = 4$.

## 1.6 Homomorphisms and Isomorphisms

1. A simple in induction proof does the trick for (a). For (b), first note that $\varphi(1) = 1$ since $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1)\varphi(1)$. Then $1 = \varphi(1) = \varphi(xx^{-1}) = \varphi(x)\varphi(x^{-1})$, and the rest follows by simplifying.

2. If $|x| = n$, then $\varphi(x)^n = \varphi(x^n) = \varphi(1) = 1$ by Exercise 1. So $|\varphi(x)| \leq n$, but if $k < n$ and $\varphi(x)^k = 1$, then $\varphi(x^k) = 1$ and $x^k \neq 1$ so $\varphi$ sends both $x^k$ and 1 to 1, a contradiction to the injectivity of $\varphi$. If $\varphi$ is simply a homomorphism, this may be false, for example, if $\varphi$ is the trivial homomorphism on a nontrivial group containing elements of order greater than 1.

3. If $H$ is abelian, then $\varphi(xy) = \varphi(x)\varphi(y) = \varphi(y)\varphi(x) = \varphi(yx)$, and injectivity of $\varphi$ yields $xy = yx$. If $G$ is abelian, simply replace $\varphi$ with $\varphi^{-1}$. If $\varphi$ is merely a homomorphism, then it must be surjective: let $G = 1$ and $H$ be any nontrivial nonabelian group with $\varphi(1) = 1$. But if $\varphi$ is surjective and $G$ is abelian, then take $x$ and $y$ in $H$, choose $a$ and $b$ in $G$ so that $\varphi(a) = x$ and $\varphi(b) = y$ and then $xy = \varphi(a)\varphi(b) = \varphi(ab) = \varphi(ba) = \varphi(b)\varphi(a) = yx$.

4. The element $\sqrt{-1}$ has order 4 in $\mathbb{C} - \{0\}$, but no element in $\mathbb{R} - \{0\}$ has order 4 (apply Exercise 2).

5. The groups have different orders.

6. $\mathbb{Q}$ has no generators while $\mathbb{Z} = \langle 1 \rangle$.

## 1.7 Group Actions

1.

# Chapter 2

# Subgroups

## 2.1 Definition and Examples

1.

2.

3.

4. $G = \mathbb{Z}$ and $H = \mathbb{Z}^+$.

5. This is immediate from Lagrange's Theorem, but we give an elementary proof here. First observe that 1 is in $H$ (let $x = y$ in (2) of Proposition 1). Let $g$ be the single element in $G - H$, and let $k \geq 2$ be its order.

## 2.2 Centralizers and Normalizers, Stabilizers and Kernels

1. This amounts to observing that $gag^{-1} = a$ if and only if $ag^{-1} = g^{-1}a$ if and only if $a = g^{-1}ag$.

2. $C_G(Z(G)) = \{g \in G : gag^{-1} = a \text{ for all } a \in Z(G)\}$. But for $a \in Z(G)$ we have, for any $g \in G$, $gag^{-1} = gg^{-1}a = a$, so $C_G(Z(G)) = G$. Moreover, $C_G(Z(G)) \leq N_G(Z(G))$ and so we have $N_G(Z(G)) = G$ as well.

3. It is clear to see that $C_G(B) \subseteq C_G(A)$: if $g$ commutes with every element of $B$, then, in particular, it commutes with every element of $A$. Since $C_G(B)$ is a subgroup of $G$, it is also a subgroup of $C_G(A)$.

4. We find $Z(S_3)$, $Z(D_8)$ and $C_{S_3}((1\ 2))$, the rest are omitted.

5.

6.

7.

8.

9.

10. We already have $C_G(H) \leq N_G(H)$. Suppose $g \in N_G(H)$, which means $gHg^{-1} = H$. If $h$ is the non identity element in $H$, then $ghg^{-1} \neq 1$, so it must be that $ghg^{-1} = h$. It follows that $g \in C_G(H)$.

    If $C_G(H) = N_G(H) = G$, then everything in $H$ commutes with everything in $G$, so $H \leq Z(G)$.

## 2.3 Cyclic Groups and Cyclic Subgroups

1.

## 2.4 Subgroups Generated by Subsets of a Group

1.

## 2.5 The Lattice of Subgroups of a Group

1.

# Chapter 3

# Quotient Groups and Homomorphisms

## 3.1 Definitions and Examples

1. If $g, h \in \varphi^{-1}(E)$, then $\varphi(gh^{-1}) = \varphi(g)\varphi(h)^{-1} \in E$ since $E$ is a subgroup. If $E$ is normal in $G$, then $\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g)^{-1} \in E$ for $g \in G$ and $h \in \varphi^{-1}(E)$.
2. 
3. 
4. 
5. 
6. 
7. $\ker \pi$ is the line $y = -x$. Fibres are shifts of this line.
8. 
9. 
10. 
11. 
12. 
13. 
14. (a) If $r + \mathbb{Z}$ is a coset, $q = r - [r]$ is the required representative.
    (b) Suppose $q = m/n$. Then $nq = nm/n = m \in \mathbb{Z}$.
    (c) Suppose $x$ is not rational. Then $nx \notin \mathbb{Z}$ for any $n > 0$, so the torsion subgroup of $\mathbb{R}/\mathbb{Z}$ is precisely $\mathbb{Q}/\mathbb{Z}$.

(d) Recall that the group of roots of unity is

$$G = \{z \in \mathbb{C} : z^n = 1 \text{ for some } n\}.$$

Define

$$\varphi : \mathbb{Q}/\mathbb{Z} \to G : r + \mathbb{Z} \mapsto e^{2\pi i r}.$$

$e^{2\pi i r} = 1$ if and only if $r \in \mathbb{Z}$, so $\varphi$ is well defined and injective. The fact that $e^{2\pi i(r+s)} = e^{2\pi i r} e^{2\pi i s}$ shows that it is a homomorphism. Suppose $\theta \in \mathbb{R}$ is such that $e^{2\pi i n\theta} = 1$. Then $n\theta \in \mathbb{Z}$, so $\theta \in \mathbb{Q}$. Thus $\theta + \mathbb{Z}$ is the required preimage of $e^{2\pi i\theta}$.

## 3.2 More on Cosets and Lagrange's Theorem

1.

## 3.3 The Isomorphism Theorems

1. The determinant $\det : GL_n(F) \to F^\times$ is a homomorphism ($F^\times$ is a group with multiplication). It is surjective since

$$\det \begin{bmatrix} q & 0 & 0 & \cdots \\ 0 & 1 & 0 & \cdots \\ 0 & 0 & 1 & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{bmatrix} = q$$

for all $q$ in $F^\times$. Its kernel is $SL_n(F)$, so $GL_n(F)/SL_n(F) \cong F^\times$ and thus

$$|GL_n(F) : SL_n(F)| = |GL_n(F)|/|SL_n(F)| = |F^\times| = q - 1.$$

## 3.4 Composition Series and the Hölder Program

1.

## 3.5 Transpositions and the Alternating Group

1.

# Chapter 4

# Group Actions

## 4.1 Group Actions and Permutation Representations

1. If $h$ is in $gG_ag^{-1}$, write $k = gkg^{-1}$ for some $k$ in $G_a$. Then

$$h \cdot b = (gkg^{-1}) \cdot b = (gk) \cdot a = g \cdot a = b$$

so $h$ is in $G_b$. If $h$ is in $G_b$ then

$$(g^{-1}hg) \cdot a = (g^{-1}h) \cdot b = g^{-1} \cdot b = a$$

so $g^{-1}hg$ is in $G_a$, hence $h = g(g^{-1}hg)g^{-1}$ is in $gG_ag^{-1}$. If $G$ acts transitively on $A$, then every element $b$ in $A$ can be written as $b = g \cdot a$ for some $g$ in $G$ and some fixed $a$ in $A$. Thus the kernel of the action is

$$\bigcap_{b \in A} G_b = \bigcap_{g \in G} gG_ag^{-1}$$

2. The proof is analogous to the previous exercise. If $G$ acts transitively on $A$, the set $\bigcap_{\sigma \in G} \sigma G_a \sigma^{-1}$ is the kernel of the action by the previous exercise. But the kernel of a permutation group action is trivial since the identity is the only permutation that fixes every element of $A$.

3. We have $\sigma G_a \sigma^{-1} = G_a$ for all $a$ and all $\sigma$ since $G$ is abelian, and hence

$$G_a = \bigcap_{\sigma \in G} \sigma G_a \sigma^{-1} = 1$$

for all $a$ by the previous exercise. Thus the identity permutation is the only permutation that fixes elements. If $a$ is fixed, the map $\sigma \mapsto \sigma(a)$ from $G$ to $A$ is surjective because $G$ is transitive, and injective since $\sigma(a) = \tau(a)$ implies $\tau^{-1}\sigma(a) = a$, whence $\tau^{-1}\sigma = 1$. It follows that $\sigma = \tau$ and that $|G| = |A|$.

4. Listing $S_3 = \{1, (12), (13), (23), (123), (132)\}$, For $(1,1)$ and applying these to $(1,1)$ and $(1,2)$ in this order, we compute the orbits to be

$$\{(1,1),(2,2),(3,3)\}, \{(1,2),(2,1),(3,2),(1,3),(2,3),(3,1)\}$$

Labelling $(i,j)$ as $g_{3(i-1)+j}$ and letting $S_9$ act on $\{g_1, g_2, \ldots, g_9\}$, we compute the cycle decomposition of (12) to be (159)(24)(36)(78) in $S_9$ (the others are left to you).

5.

6.

7. (a) Clearly $G_B$ is a subgroup. If $\sigma$ is in $G_a$, then either $\sigma(B) = B$ or $\sigma(B) \cap B = \varnothing$. Since $\sigma(a) = a$ and $a$ is in $B$, it must be the former.

   (b) The sets union to $A$ since $G$ is transitive. For $i \neq j$ we also have

   $$\sigma_i(B) \cap \sigma_j(B) = \varnothing \iff \sigma_i^{-1}(\sigma_i(B) \cap \sigma_j(B)) = B \cap \sigma_i^{-1}\sigma_j(B) = \varnothing.$$

   The second statement is true because $B$ is a block and we cannot have $\sigma_i^{-1}\sigma_j(B) = B$, for then $\sigma_i(B) = \sigma_j(B)$, and they are supposed to be distinct images.

   (c) $\{1,2\}$ is not a block since $\sigma = (23)$ gives $\sigma(\{1,2\}) = \{1,3\}$. The other 17 subsets of size two or three are not blocks for similar reasons. Pairs of opposite vertices give two nontrivial blocks in $D_8$.

   (d) If $G$ is not primitive, there is a nontrivial block $B$. If $a$ is in $B$, then $G_a \leq G_B \leq G$ by part (a). Use transitivity of $G$ to see that the containments are strict. Conversely, suppose there exists $a$ and $H$ such that $G_a \leq H \leq G$, where the containments are strict. Let $B = \bigcup_{\sigma \in H} \{\sigma(a)\}$. Then $B$ is a nontrivial block.

8. (a) Easy.

   (b) If a doubly transitive group $G$ had a nontrivial block $B \subseteq A$, one could pick distinct $a$ and $b$ in $B$ so that there exists some $\sigma$ in $G_a$ with $\sigma(b)$ not in $B$.

## 4.2 Groups Acting on Themselves by Left Multiplication–Cayley's Theorem

1.

## 4.3 Groups Acting on Themselves by Conjugation–The Class Equation

1.

## 4.4 Automorphisms

1.

2.

3.

4.

5.

6.

7.

8.

9.

10.

11.

12.

13. $H$ is cyclic, so $|Aut(H)| = 6$. Thus $|G/C_G(H)|$ divides both 6 and 203, so $|G/C_G(H)| = 1$. This implies $G = C_G(H)$ and thus $H \leq Z(G)$.

## 4.5 The Sylow Theorems

1.

## 4.6 The Simplicity of $A_n$

1.

# Chapter 5

# Direct and Semidirect Products and Abelian Groups

## 5.1 Direct Products

1.

## 5.2 The Fundamental Theorem of Finitely Generated Abelian Groups

1.

## 5.3 Table of Groups of Small Order

1.

## 5.4 Recognizing Direct Products

1. Easy.
2. See Proposition 7(2) and the previous exercise.

## 5.5 Semidirect Products

1.

# Chapter 6

# Further Topics in Group Theory

## 6.1 $p$-groups, Nilpotent Groups, and Solvable Groups

1.

## 6.2 Applications in Groups of Medium Order

1.

## 6.3 A Word on Free Groups

1.

# Part II

# Ring Theory

# Chapter 7

# Introduction to Rings

## 7.1 Basic Definitions and Examples

1. $(-1)^2 = (-1)^2 + (-1) + 1 = (-1)((-1) + 1) + 1 = (-1)(0) + 1 = 1$.

2. $(-u)(-v) = uv = 1$ by Proposition 1.

3. If $u$ is an unit in $S$, then there is an element $v$ of $S$ such that $uv = 1$. But both $u$ and $v$ are in $R$ as well, so $u$ is a unit in $R$. As a counterexample for the converse, take $R = \mathbb{Q}$, $S = \mathbb{Z}$, and $u = 2$.

4. Let $\{S_\lambda\}$ be a collection of subrings of a ring $R$. If $r, s \in \bigcap_\lambda S_\lambda$, then $r, s \in S_\lambda$ for all $\lambda$. Thus $r + s \in S_\lambda$ for all $\lambda$, so $r + s \in \bigcap_\lambda S_\lambda$. Multiplication is analogous.

5. (a) Yes, we have

$$\frac{n}{2k+1} + \frac{m}{2\ell+1} = \frac{n(2\ell+1) + m(2k+1)}{(2k+1)(2\ell+1)} \qquad \frac{n}{2k+1}\frac{m}{2\ell+1} = \frac{nm}{(2k+1)(2\ell+1)}$$

   and both denominators are odd.

6.

7.

8.

9. If $r, s \in C(a)$, then

$$(r + s)a = ra + sa = ar + as = a(r + s).$$

   Multiplication is analogous. $a$ is clearly in $C(a)$ since $a$ commutes with itself.

10.

11. We have $(x + 1)(x - 1) = 0$, so if $x \neq \pm 1$, then $x + 1$ and $x - 1$ are zero divisors.

12.

13.

14.

15.

16. If $R$ is a Boolean ring and an integral domain and $r \in R$, then $r^2 = r$, so $r(r-1) = 0$ and thus either $r = 0$ or $r = 1$ since there are no zero divisors.

## 7.2 Examples: Polynomial Rings, Matrix Rings, and Group Rings

1.

2.

3.

4.

5.

6. (a) The $k, \ell$ entry of $E_{ij}A$ is

$$\sum_{m=1}^{n} (E_{ij})_{km} A_{m\ell}$$

which is 0 if $k \neq i$ and $A_{j\ell}$ if $k = i$. In other words, if we are not in the $i$th row of $E_{ij}A$, we are zero, and if we are, we are the element from the $j$th row of $A$.

(b) The argument is symmetric to the one in (a).

(c) $E_{pq}A$ has only the $q$th row of $A$ in its $p$th row, and hence $E_{pq}AE_{rs} = (E_{pq}A)E_{rs}$ has $a_{qr}$ in the $p, s$ spot and 0 everywhere else.

7.

8.

9.

10.

11.

12.

## 7.3 Ring Homomorphisms and Quotient Rings

1. Suppose there were an isomorphism $\varphi : 2\mathbb{Z} \to 3\mathbb{Z}$. We have

$$\varphi(2) + \varphi(2) = \varphi(2+2) = \varphi(4) = \varphi(2 \cdot 2) = \varphi(2)^2.$$

Let $k = \varphi(2)$. Then $k$ is an integer divisible by 3 and $k^2 = 2k$. Then $k^2$ is even, hence $k$ is even and $k$ is divisible by 6. But this means that $\varphi$ is not surjective, for

$$3 = \varphi(\pm 2 \pm 2 \pm \cdots \pm 2) = \pm\varphi(2) \pm \varphi(2) \pm \cdots \pm \varphi(2)$$

would mean that 6 divides 3, which is not true.

2.

3. Let $\varphi : \mathbb{Z} \to R$ be a homomorphism. By Theorem 7, $\varphi(\mathbb{Z})$ is isomorphic to $\mathbb{Z}/\ker\varphi$. By Example 2, the only ideals of $\mathbb{Z}$ are $n\mathbb{Z}$ for $n \in \mathbb{Z}$, so $\ker\varphi = n\mathbb{Z}$ for some $n$. We also have that $n\mathbb{Z}$ is the kernel of some homomorphism of $\mathbb{Z}$; take the quotient mapping $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. So every homomorphic image of $\mathbb{Z}$ is precisely $\mathbb{Z}/n\mathbb{Z}$ for some $n \in \mathbb{Z}$.

4.

5.

6.

7.

8.

9.

10.

11.

12.

13. Let

$$a + bi \mapsto \begin{bmatrix} a & -b \\ b & a \end{bmatrix}.$$

It is clearly injective.

14.

15.

16.

17.

18.

19.

20.

21.

22.

23.

24.

25.

26.

27.

28.

29.

30.

31.

32.

33.

34. (a) Clearly $I + J$ contains both $I$ and $J$. Suppose $K$ is an ideal containing $I$ and $J$. Then if $a$ is in $I$ and $b$ is in $J$, both $a$ and $b$ are in $K$. Then $a + b$ is in $K$ because it's closed under addition.

    (b) It's easy to see it's an ideal. If $a_1b_1 + \cdots a_nb_n$ is in $IJ$, then each term is in $I$ since each $a_i$ is in $I$. Thus the sum is in $I$. Same for $J$.

    (c) $2\mathbb{Z} \cdot 4\mathbb{Z} \neq 2\mathbb{Z} \cap 4\mathbb{Z}$.

    (d) This is the Chinese Remainder Theorem.

## 7.4 Properties of Ideals

1.

## 7.5 Rings of Fractions

1.

## 7.6 The Chinese Remainder Theorem

1.

2.

3.

4.

5.

6.

7.

8. (a) Only transitivity is nontrivial. If $a \in A_i$, $b \in A_j$, and $c \in A_k$ with $a \sim b$ and $b \sim c$, choose $l$ such that $\rho_{il}(a) = \rho_{jl}(b)$ and $m$ so that $\rho_{jm}(b) = \rho_{km}(c)$. The index set is directed, so choose $p$ such that $p \geq l$ and $p \geq m$. Then $\rho_{ip}(a) = \rho_{lp} \circ \rho_{il}(a) = \rho_{lp} \circ \rho_{jl}(b) = \rho_{jp}(b) = \rho_{mp} \circ \rho_{jm}(b) = \rho_{mp} \circ \rho_{km}(c) = \rho_{kp}(c)$.

   (b) Fix $i$ and assume $\rho_i(a) = \rho_i(b)$. This means that $a \sim b$ and so there is some $k$ so that $\rho_{ik}(a) = \rho_{ik}(b)$. But $\rho_{ik}$ is injective, so $a = b$.

   (c) First we show that the definition of $\overline{a} + \overline{b}$ is independent of the choice of $k$.

9. Germs

10. (a) Let $(a_i)$ and $(b_i)$ be in $P$. Then $\mu_{ji}(a_j + b_j) = \mu_{ji}(a_j) + \mu_{ji}(b_j) = a_i + b_i$. Also $\mu_{ji}(a_j^{-1}) = \mu_{ji}(a_j)^{-1} = a_i^{-1}$.

    (b) Let $i$ and $a_i \in A_i$ be arbitrary. By assumption, for each $j \geq i$ there is an element $a_j$ in $A_j$ with $\mu_{ji}(a_j) = a_i$. Then the element $a = (\mu_{i1}(a_i), \mu_{i2}(a_i), \ldots, \mu_{i(i-1)}(a_i), a_i, a_{i+1}, a_{i+2}, \ldots)$ is in $P$ and satisfies $\mu_i(a) = a_i$.

    (c) Similar to (a).

    (d) Assume the existence of the group $D$ and the group homomorphisms $\pi_i$. Define $\pi : D \to P$ by $\pi(d) = (\pi_i(d))_{i \in I}$. The element $(\pi_i(d))_{i \in I}$ is in $P$ because for $i \leq j$ we have $\mu_{ji}(\pi_j(d)) = \pi_i(d)$. We have $\pi(c + d) = (\pi_i(c + d))_{i \in I} = (\pi_i(c) + \pi_i(d))_{i \in I} = (\pi_i(c))_{i \in I} + (\pi_i(d))_{i \in I} = \pi(c) + \pi(d)$, so $\pi$ is a group homomorphism. Clearly $\mu_i \circ \pi(d) = \mu_i((\pi_i(d))_{i \in I}) = \pi_i(d)$. To see that $\pi$ is unique, notice that each component of $\pi(d)$ is determined by the equation $\mu_i(\pi(d)) = \pi_i(d)$, and this determines $\pi$ uniquely.

11. (a) For an element $(a_i)_{i=0}^{\infty}$ in $\mathbb{Z}_p$, the coefficient $b_i$ is the $i$th coefficient in the base $p$ expansion of $a_i$ (and also for $a_j$ if $j \geq i$), and $\mu_{ji}(\sum_{n=0}^{j} b_n p^n) = \sum_{n=0}^{i} b_n p^n$.

# Chapter 8

# Euclidean Domains, Principal Ideal Domains and Unique Factorization Domains

## 8.1 Euclidean Domains

1.

## 8.2 Principal Ideal Domains (P.I.D.s)

1.

## 8.3 Unique Factorization Domains (U.F.D.s)

1.

# Chapter 9

# Polynomial Rings

## 9.1 Definitions and Basic Properties

1.

## 9.2 Polynomial Rings over Fields I

1.

## 9.3 Polynomial Rings that are Unique Factorization Domains

1.

## 9.4 Irreducibility Criteria

1.

## 9.5 Polynomial Rings over Fields II

1.

## 9.6 Polynomials in Several Variables over a Field and Gröbner Bases

1.

# Part III

# Modules and Vector Spaces

# Chapter 10

# Introduction to Module Theory

## 10.1 Basic Definitions and Examples

1.

## 10.2 Quotient Modules and Module Homomorphisms

1.

## 10.3 Generation of Modules, Direct Sums, and Free Modules

1.

## 10.4 Tensor Products of Modules

1.

## 10.5 Exact Sequences–Projective, Injective, and Flat Modules

1.

# Chapter 11

# Vector Spaces

## 11.1 Definitions and Basic Theory

1. We have

$$a_1 0 + a_2 0 + \cdots + a_n 0 = 0,$$
$$a_1(x_1 + x_2') + \cdots + a_n(x_n + x_n') = a_1 x_1 + \cdots + a_n x_n + a_1 x_1' + \cdots + a_n x_n' = 0 + 0 = 0$$
$$a_1(\alpha x_1) + \cdots + a_n(\alpha x_n) = \alpha(a_1 x_1 + \cdots + a_n x_n) = \alpha 0 = 0$$

so that it is a subspace. Define the linear transformation

$$\varphi : V \to \mathbb{R} : (x_1, x_2, \cdots, x_n) \mapsto a_1 x_1 + a_2 x_2 + \cdots + a_n x_n.$$

We seek to find a basis for and determine the dimension of $\ker \varphi$. By Corollary 8, $n = \dim V = \dim(\ker \varphi) + \dim(\varphi(V))$. Now $\dim(\varphi(V))$ is either 0 or 1 (being a subspace of $\mathbb{R}$, which has dimension 1), so $\dim(\ker \varphi)$ is either $n$ or $n-1$. The case where $\dim(\ker \varphi) = n - 1$ is the more interesting one

## 11.2 The Matrix of a Linear Transformation

1.

## 11.3 Dual Vector Spaces

1.

## 11.4 Determinants

1.

## 11.5 Tensor Algebras, Symmetric and Exterior Algebras

1.

# Chapter 12

# Modules over Principal Ideal Domains

## 12.1 The Basic Theory

1.

## 12.2 The Rational Canonical Form

1.

## 12.3 The Jordan Canonical Form

1.

# Part IV

# Field Theory and Galois Theory

# Chapter 13

# Field Theory

## 13.1 Basic Theory of Field Extensions

1. Use Eisenstein's criterion with the prime 3.

2.

3.

4.

5. Write $\alpha = \frac{p}{q}$ where $\gcd(p, q) = 1$. Let $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be the monic polynomial with $p(\alpha) = 0$. Then

$$\left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \cdots + a_1\frac{p}{q} + a_0 = 0$$

multiplying both sides by $q^{n-1}$ and rearranging, we have

$$\frac{p^n}{q} = -a_{n-1}p^{n-1}q^{n-1} - \cdots - a_1 pq^{n-2} - a_0 q^{n-1}$$

The right side is an integer, so $\frac{p^n}{q} \in \mathbb{Z}$. But $p$ and $q$ have no common factors, so $q = 1$.

## 13.2 Algebraic Extensions

1.

## 13.3 Classical Straightedge and Compass Constructions

1.

## 13.4 Splitting Fields and Algebraic Closures

1.

## 13.5 Separable and Inseparable Extensions

1.

## 13.6 Cyclotomic Polynomials and Extensions

1.

# Chapter 14

# Galois Theory

## 14.1 Basic Definitions

1.

## 14.2 The Fundamental Theorem of Galois Theory

1.

## 14.3 Finite Fields

1.

## 14.4 Composite Extensions and Simple Extensions

1.

## 14.5 Cyclotomic Extensions and Abelian Extensions over $\mathbb{Q}$

1.

## 14.6 Galois Groups of Polynomials

1.

## 14.7 Solvable and Radical Extensions: Insolvability of the Quintic

1.

## 14.8 Computation of Galois Groups over $\mathbb{Q}$

1.

## 14.9 Transcedental Extensions. Inseparable Extensions, Infinite Galois Groups

1.

# Part V

# An Introduction to Commutative Rings, Algebraic Geometry, and Homological Algebra

# Chapter 15

# Commutative Rings and Algebraic Geometry

## 15.1 Noetherian Rings and Affine Algebraic Sets

1.

## 15.2 Radicals and Affine Varieties

1.

## 15.3 Integral Extensions and Hilbert's Nullstellensatz

1.

## 15.4 Localization

1.

## 15.5 The Prime Spectrum of a Ring

1.

# Chapter 16

# Artinian Rings, Discrete Valuation Rings, and Dedekind Domains

## 16.1 Artinian Rings

1.

## 16.2 Discrete Valuation Rings

1.

## 16.3 Dedekind Domains

1.

# Chapter 17

# Introduction to Homological Algebra and Group Cohomology

## 17.1 Introduction to Homological Algebra–Ext and Tor

1.

## 17.2 The Cohomology of Groups

1.

## 17.3 Crossed Homomorphisms and $H^1(G, A)$

1.

## 17.4 Group Extensions, Factor Sets and $H^2(G, A)$

# Part VI

# Introduction to the Representation Theory of Finite Groups

# Chapter 18

# Representation Theory and Character Theory

## 18.1 Linear Actions and Modules over Group Rings

1.

## 18.2 Wedderburn's Theorem and Some Consequences

1.

## 18.3 Character Theory and the Orthogonality Relations

1.

# Chapter 19

# Examples and Applications of Character Theory

## 19.1 Characters of Groups of Small Order

1.

## 19.2 Theorems of Burnside and Hall

1.

## 19.3 Introduction to the Theory of Induced Characters

1.