<table>
<thead>
<tr>
<th>Problem Number</th>
<th>Problem</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>69</td>
<td>Problem 8.2</td>
<td>26</td>
</tr>
<tr>
<td>70</td>
<td>Problem 8.3</td>
<td>26</td>
</tr>
<tr>
<td>71</td>
<td>Problem 8.4</td>
<td>26</td>
</tr>
<tr>
<td>72</td>
<td>Problem 8.5</td>
<td>27</td>
</tr>
<tr>
<td>73</td>
<td>Problem 8.6</td>
<td>28</td>
</tr>
<tr>
<td>74</td>
<td>Problem 8.7</td>
<td>28</td>
</tr>
<tr>
<td>75</td>
<td>Problem 8.8</td>
<td>28</td>
</tr>
<tr>
<td>76</td>
<td>Problem 8.9</td>
<td>29</td>
</tr>
<tr>
<td>77</td>
<td>Problem 8.10</td>
<td>29</td>
</tr>
<tr>
<td>78</td>
<td>Problem 9.1</td>
<td>30</td>
</tr>
<tr>
<td>79</td>
<td>Problem 9.2</td>
<td>30</td>
</tr>
<tr>
<td>80</td>
<td>Problem 9.3</td>
<td>32</td>
</tr>
<tr>
<td>81</td>
<td>Problem 9.4</td>
<td>32</td>
</tr>
<tr>
<td>82</td>
<td>Problem 9.5</td>
<td>32</td>
</tr>
<tr>
<td>83</td>
<td>Problem 9.6</td>
<td>33</td>
</tr>
<tr>
<td>84</td>
<td>Problem 9.7</td>
<td>33</td>
</tr>
<tr>
<td>85</td>
<td>Problem 9.8</td>
<td>34</td>
</tr>
<tr>
<td>86</td>
<td>Problem 9.9</td>
<td>34</td>
</tr>
<tr>
<td>87</td>
<td>Problem 9.10</td>
<td>34</td>
</tr>
</tbody>
</table>
1 Problem 1.2

We give proof by induction. The claim is true for $n = 1$, since $1^2 = 1^3$. Suppose it is true for $n = k > 1$. Then:

$$(1 + 2 + 3 + \cdots + k + (k + 1))^2 = (1 + 2 + 3 + \cdots + k)^2 + 2(1 + 2 + 3 + \cdots + k)(k + 1) + (k + 1)^2$$

By the induction hypothesis,

$$(1 + 2 + 3 + \cdots + k)^2 = 1^3 + 2^3 + \cdots + k^3$$

so it suffices to show that $2(1 + 2 + 3 + \cdots + k)(k + 1) + (k + 1)^2 = (k + 1)^3$. Indeed, one can prove by induction that $1 + 2 + 3 + \cdots + k = \frac{k(k+1)}{2}$, so

$$2(1 + 2 + 3 + \cdots + k)(k + 1) + (k + 1)^2 = 2 \left( \frac{k(k+1)}{2} \right) (k + 1) + (k + 1)^2$$

$$= k(k+1)^2 + (k + 1)^2$$

$$= (k + 1)(k + 1)^2$$

$$= (k + 1)^3$$

so our claim holds for $n = k + 1$, and therefore is true for all $n \in \mathbb{N}$ by induction.

2 Problem 1.3

We prove more generally that for any fixed $a \in \mathbb{N}$, $a - 1$ divides $a^n - 1$ for all $n \in \mathbb{N}$ by induction on $n$. Clearly, $a - 1 \mid a - 1$. Suppose it is true for $n = k > 1$. Then

$$a^{k+1} - 1 = a^{k+1} - a + a - 1 = a(a^k - 1) + (a - 1)$$

Since $a^k - 1$ is divisible by $a - 1$ by the induction hypothesis and $a - 1$ manifestly divides $a - 1$, it follows that $a - 1 \mid a^{k+1} - 1$, which completes the proof. Now take $a = 13$.

3 Problem 1.4

We give proof by contrapositive: i.e., if $a \neq 2$ or $n$ is not prime, then $a^n - 1$ is not prime. Note $1^n - 1 = 0$ is not prime, so suppose $a > 2$. By the previous problem, $a - 1 \mid a^n - 1$, and since $a - 1 \neq 1$ and $a - 1 \neq a^n - 1 \ (n > 1)$, $a - 1$ is a proper divisor of $a^n - 1$, so $a^n - 1$ is composite. If $a = 2$, then suppose $n = xy$ is composite. Then $a^x - 1$ divides $(a^x)^y - 1 = a^n - 1$ by the previous problem. Since $1 < x < n$, $a^x - 1$ is a proper divisor of $a^n - 1$, whence $a^n - 1$ is not prime.

Now, suppose $2^n + 1$ is prime. Note that for $n$ odd, $a^n + 1$ factors as

$$a^n + 1 = (a + 1)(a^{n-1} - a^{n-2} + a^{n-3} + \cdots - a + 1)$$

One can prove this, e.g., by induction on $k$ for $n = 2k + 1$. Alternatively, it is more generally true that $a - b \mid a^n - b^n$ for all $a, b \in \mathbb{Z}, n \in \mathbb{N}$, so one can take $a = a, b = -1$. Hence, let $n = 2^k \cdot m$, where $m$ is odd. Then $2^n = 2^{2^k \cdot m} = (2^{2^k})^m$, so $2^{2^k} + 1$ is a proper divisor of $2^n + 1$ unless $m = 1$. Hence, $n$ must be a power of 2.
4 Problem 1.5

Note that a particular solution is \((x_0, y_0) = (10, -24)\) (one can compute a particular solution by using the euclidean algorithm to find \(x, y \in \mathbb{Z}\) such that \(93x + 39y = 3\), since \(\gcd(93, 39) = 3\)). Using the statement of problem 1.6, the general solution is then given by

\[
x = 10 + 31k, \quad y = -24 - 13k, \quad k \in \mathbb{Z}
\]

5 Problem 1.6

Let \(a, b, c\) be nonzero integers and \(d = \gcd(a, b)\). Suppose \(ax + by = c\) has a solution \((x, y) \in \mathbb{Z}^2\). Since \(d \mid a, d \mid b, d \mid ax + by = c\). On the other hand, suppose \(d \mid c\), i.e. \(c = kd\) for some \(k \in \mathbb{Z}\). By Bezout’s lemma, there exist \(x, y \in \mathbb{Z}\) such that \(ax + by = d\), so \(akx + bky = dk = c\).

Now, suppose that \(x_0, y_0 \in \mathbb{Z}\) satisfies \(ax_0 + by_0 = c\), and let \((x, y)\) be another solution to the equation \(ax + by = c\). One can trivially verify that \(x = x_0 + (b/d)k, y = y_0 - (a/d)k\) is a solution for all \(k \in \mathbb{Z}\). Then \(ax_0 + by_0 = c = ax + by\), so \(a(x_0 - x) = b(y - y_0)\). Letting \(a = a_0d, b = b_0d\), we may divide both sides by \(d\) to obtain \(a_0(x_0 - x) = b_0(y - y_0)\). Since \(b_0\) divides the RHS and \(\gcd(a_0, b_0) = 1, b_0 \mid x_0 - x\), i.e. \(x_0 - x = kb_0\) is \(k(b/d)\) for some \(k \in \mathbb{Z}\). Then \(y - y_0 = a/b(x_0 - x) = (a/d)k\), so \(y_0 - y = -(a/d)k\), which proves the claim.

6 Problem 1.7

Suppose \(ab = n^2\) for some \(n \in \mathbb{N}\) with \(\gcd(a, b) = 1\). By the fundamental theorem of arithmetic, there is a unique factorization

\[
ab = p_1^{k_1} \cdots p_l^{k_l}
\]

for some distinct primes \(p_1, \ldots, p_l\) and positive integers \(k_1, \ldots, k_l\). Furthermore, since \(ab\) is a square, each of \(k_1, \ldots, k_l\) is even (namely, each is twice the exponent of \(p_i\) that appears in the prime decomposition of \(n\)). For each \(i = 1, \ldots, l\), let \(t_i\) be the highest power of \(p_i\) dividing \(a\), and \(r_i\) the higher power of \(p_i\) dividing \(b\). By unique factorization, we have \(t_i + r_i = k_i\); but since \(\gcd(a, b) = 1\), at most one of \(t_i, r_i\) is nonzero, i.e. \(t_i = k_i\) and \(r_i = 0\), or \(t_i = 0\) and \(r_i = k_i\) for each \(i = 1, \ldots, l\). Hence, every power appearing in the prime decomposition of \(a\) is even, so \(a\) is a square; likewise with \(b\).

7 Problem 1.8

Suppose \(\gcd(a, n) = \gcd(b, n) = 1\). By Bezout’s lemma, there exist \(x, y, z, w \in \mathbb{Z}\) such that \(ax + ny = 1, bz + nw = 1\). Hence, \(1 = (ax + ny)(bz + nw) = (xz)ab + (yzb + axw + nyw)n\), whence \(\gcd(ab, n) \mid 1\) by problem 1.6, so \(\gcd(ab, n) = 1\).
8 Problem 1.10
Let \( \{p_1, \ldots, p_n\} \) be any finite nonempty list of primes congruent to 2 mod 3 (such a list exists, e.g. \( \{2\} \)). Consider \( N = 3p_1 \cdots p_n - 1 \). Note that \( N \equiv -1 \equiv 2 \pmod{3} \); further, \( N \equiv -1 \pmod{p_i} \) for each \( i = 1, \ldots, n \), so \( p_i \) does not divide \( N \) for any \( i \). Suppose \( N = q_1 \cdots q_k \) (not necessarily distinct) primes \( q_1, \ldots, q_k \). Then \( [N]_3 = [q_1]_3 \cdots [q_k]_3 = [2]_3 \), so there must be some \( l \in \{1, \ldots, k\} \) such that \( q_l \equiv 2 \pmod{3} \). Since \( q_l \) is a divisor of \( N \), it is not in the list \( \{p_1, \ldots, p_n\} \), so \( \{p_1, \ldots, p_n\} \) is a proper subset of the set of all primes congruent to 2 mod 3. Since this list was arbitrary, this shows that no such finite set contains all primes congruent to 2 mod 3, i.e. there must be infinitely many primes congruent to 2 mod 3.

9 Problem 2.1
Suppose \( b \equiv c \pmod{a} \), i.e. \( b = c + ka \) for some \( k \in \mathbb{Z} \). Let \( d = \gcd(a, b), d' = \gcd(a, c) \). Since \( d \mid a \) and \( d \mid b, d \mid b - ka = c \), so \( d \mid d' \). Symmetrically, one can see that \( d' \mid d \), so \( d = d' \).

10 Problem 2.2
By the binomial theorem, \( (a + b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k} \) so it suffices to show that \( p \) divides \( \binom{p}{k} \) for each \( 1 \leq k \leq p - 1 \). Indeed, if \( \frac{p!}{k!(p-k)!} = n \in \mathbb{N} \), then \( p! = n \cdot k! \cdot (p-k)! \). Since \( p \) divides the LHS, it also divides the RHS, and so by Euclid’s lemma divides one of \( n, k!, (p-k)! \). If \( p \) divides \( k! \), then inductively applying Euclid’s lemma, it divides one of \( 1, 2, \ldots, k \), which is impossible since \( k < p \). Likewise, \( p \) cannot divide \( (p-k)! \), so \( p \) must divide \( n \), which completes the proof.

11 Problem 2.3
(a) Since \( \gcd(7, 300) = 1 \), \( [7] \in (\mathbb{Z}/300\mathbb{Z})^\times \). In particular, one can use the Euclidean algorithm to find \( r, s \in \mathbb{Z} \) such that \( 7r + 300s = 1 \), whence \( [r] = [7]^{-1} \). One may compute \( r = 43, s = -1 \), so that \( [7] \cdot X = [2] \) implies \( x = [2][43] = [86] \).

(b) This is equivalent to the linear Diophantine equation \( 120x + 300y = 80 \), which has no solutions: 3 divides \( 120x + 300y \) for all \( x, y \in \mathbb{Z} \), but 3 does not divide 80.

(c) There are many approaches here: one is via the Chinese Remainder Theorem. Factoring \( 300 = 2^2 \cdot 3 \cdot 5^2 \), consider the associated system of congruences:

\[
\begin{align*}
[9]_4 \cdot [X]_4 &= [48]_4 \implies [1]_4 \cdot [X]_4 &= [0]_4 \implies [X]_4 &= 0 \\
[9]_3 \cdot [X]_3 &= [48]_3 \implies [0]_3 \cdot [X]_3 &= [0]_3
\end{align*}
\]
\[ 9_{25} \cdot [X]_{25} = [48]_{25} = [23]_{25} \]

Since \( \text{gcd}(9, 25) = 1 \), the last equation has a unique solution, which one can determine by computing the inverse of \( [9] \) in \( \mathbb{Z}/25\mathbb{Z} \), e.g. via the Euclidean algorithm. Noting \( 9 \cdot 14 - 25 \cdot 5 = 1 \) shows \( [9]^{-1}_{25} = [14]_{25} \), i.e. the last congruence relation can be rewritten as

\[ [X]_{25} = [23]_{25} [14]_{25} = [322]_{25} = [22]_{25} \]

The second congruence relation is trivially satisfied; the first and third “glue” to a unique simultaneous solution mod 100 by the Chinese Remainder Theorem, which we can identify as follows. WLOG, take the representative \( X \) to be between 0 and 99 inclusive. Then \( [X]_{25} = [22]_{25} \) gives four possible representatives: 22, 47, 72, 97. The simultaneous congruence \( [X]_{4} = [0]_{4} \) implies that the representative \( X \) is divisible by 4, so \( [X]_{100} = [72]_{100} \). Taking translates by 100 yield the other two solutions: the final solution set is given by \{ [72]_{300}, [172]_{300}, [272]_{300} \}.

12 Problem 2.4

This is equivalent to \( [73]_{m} = [0]_{m}, \) i.e. \( m \mid 73 \), so \( m = 1 \) or \( m = 73 \).

13 Problem 2.5

This amounts to showing that the (multiplicative) order of \( [2] \) in \( (\mathbb{Z}/13\mathbb{Z})^{\times} \cong \mathbb{Z}/12\mathbb{Z} \) is 12. By Lagrange’s theorem, it suffices to check the possible orders 1, 2, 3, 4, 6, 12. One can see \( [2]^{6} = [64] = [-1] \) and \( [2]^{4} = [16] = [3] \), which rules out 1, 2, 3, 4 and 6 as orders, so \( |[2]| = 12 \), as desired.

14 Problem 2.6

This is a straightforward application of the Euclidean algorithm: one can compute that \( [100]^{-1} = [109] \).

15 Problem 2.7

By computing the square of all residue classes mod 11, one can see that solutions are \( X = [4]_{11}, X = [7]_{11} \).

16 Problem 2.8

This boils down to computing the (multiplicative) order of \( [2] \) in \( (\mathbb{Z}/17\mathbb{Z})^{\times} \cong \mathbb{Z}/16\mathbb{Z} \). Furthermore, by Lagrange’s theorem, \( |[2]| \) divides \( |(\mathbb{Z}/17\mathbb{Z})^{\times}| = 16 \), so it suffices to check the possible orders 1, 2, 4, 8, 16. One can see that \( [2]^{4} = [16] = [-1] \) (which rules out 1, 2 as well), so \( [2]^{8} = [1] \) and hence \( |[2]| = 8 \). Therefore, \( [2]^{k} = [1] \) if and only if \( 8 \mid k \).
17 Problem 2.9

Reflexivity and symmetry are obvious: \((a, b) \sim (a, b)\), since \(ab = ba\) for all \(a, b \in \mathbb{R}\), and 
\((a, b) \sim (c, d) \implies ad = bc \implies da = cb \implies (c, d) \sim (a, b)\). Transitivity requires a bit more care: suppose \((a, b) \sim (c, d), (c, d) \sim (e, f)\). Then \(ad = bc, cf = de\), so \(adcf = bcde\). If \(c \neq 0, d \neq 0\), then cancellation implies \(af = be\) as desired. If \(c = 0\), then \(ad = bc\) implies \(a = 0\), since \(d \neq 0\). Similarly, \(cf = de\) implies \(e = 0\), so \(af = be\). Likewise, if \(d = 0\), then \(ad = bc\) implies \(b = 0\), since \(c \neq 0\), and \(cf = de\) implies \(f = 0\), so again \(af = be\). Hence, \(\sim\) is an equivalence relation.

We claim that the equivalence classes of \(\sim\) are lines through the origin (minus the origin) in \(\mathbb{R}^2\). Indeed, the proof of transitivity above shows that \((a, 0) \sim (c, d)\) if and only if \(d = 0\), i.e. \((a, 0)\) and \((c, 0)\) lie on the \(x\)-axis, and similarly that \((0, b) \sim (c, d)\) if and only if \(c = 0\). If \((a, b) \sim (c, d)\) with \(a, b\) both nonzero, then \(c, d\) must both be nonzero as well, and so we may write \(b/a = d/c\). Then \((a, b), (c, d)\) are both points on the line with slope \(b/a\).

18 Problem 2.10

We proceed by induction on \(n\). For the case \(n = 3\), note that every odd integer \(x\) is congruent to 1, 3, 5 or 7 mod 8, so it suffices to verify

\[
[1]_8^2 = [3]_8^2 = [5]_8^2 = [7]_8^2 = [1]_8
\]

Suppose it is true for some \(n = k > 3\). Then for all \(x\) odd, \(x^{2k-2} - 1\) is divisible by \(2^k\); since \(x\) is odd, \(x^{2k-2} + 1\) is even (hence divisible by 2), so

\[
(x^{2k-2} - 1)(x^{2k-2} + 1) = x^{2k-1} - 1
\]

is divisible by \(2 \cdot 2^k = 2^{k+1}\), completing the proof.

19 Problem 3.2

Note that

\[
((ab)c)d = (a(bc))d = a((bc)d) = a(b(cd))
\]

20 Problem 3.3

If \((ab)^2 = a^2b^2\) for all \(a, b \in G\), then

\[
abab = aabb
\]

for all \(a, b \in G\). Left multiplying by \(a^{-1}\) and right multiplying by \(b^{-1}\) gives

\[
ba = ab
\]

so \(G\) is abelian.
21 Problem 3.4

If $3[x]_{18} = [0]_{18}$, then $3x = 18y$ for some $y \in \mathbb{Z}$, i.e. $x = 6y$. The possible equivalence class representatives are therefore $[0]_{18}, [6]_{18}, [12]_{18}$; it’s easy to see that $[0]_{18}$ has order 1, and $[6]_{18}$ and $[12]_{18}$ are elements of order 3.

22 Problem 3.5

Suppose $f : G \rightarrow H, g : H \rightarrow K$ are group homomorphisms. Then for any $x, y \in G$,

$$(g \circ f)(xy) = g(f(xy)) = g(f(x)f(y)) = g(f(x))g(f(y)) = (g \circ f)(x)(g \circ f)(y)$$

so $g \circ f$ is a group homomorphism. Since the composition of two bijections is a bijection, this also shows that the composition of two isomorphisms is an isomorphism (see problem 1.1).

23 Problem 3.6

Note that $(\mathbb{Z}/9\mathbb{Z})^\times = \{[1]_9, [2]_9, [4]_9, [5]_9, [7]_9, [8]_9\}$. Note


so $[2]$ must have order 6 in $(\mathbb{Z}/9\mathbb{Z})^\times$, whence $(\mathbb{Z}/9\mathbb{Z})^\times$ is a cyclic group of order 6, and thus is isomorphic to $\mathbb{Z}/6\mathbb{Z}$.

24 Problem 3.7

Suppose $a, b \in G$ with $|a| = n, |b| = m$ and $\gcd(n, m) = 1$. Since $G$ is abelian,

$$(ab)^{nm} = a^{nm}b^{nm} = (a^n)^m(b^m)^n = e$$

so $|ab|$ divides $nm$. On the other hand, note that $\langle ab \rangle$ contains $\langle a \rangle$; indeed, $(ab)^{m} = a^{m}b^{m} = a^{m}$, and $\langle a^{m} \rangle = \langle a \rangle$ since $m, n$ are coprime. Hence, by Lagrange's theorem, $|\langle a \rangle| = |a| = n$ divides $|\langle ab \rangle| = |ab|$. Similarly, $m$ divides $|ab|$, so $\text{lcm}(n, m) = nm$ divides $|ab|$, whence $|ab| = nm$.

25 Problem 3.8

(a) Let $\mu_n = \{z \mid z \in \mathbb{C}, z^n = 1\}$ be the set of all complex $n^{\text{th}}$ roots of unity. Let $G = (\mu_n, \cdot)$ where $\cdot$ is the standard multiplication operation on $\mathbb{C} \setminus \{0\}$. Let $x, y \in G$. Then as complex multiplication is commutative,

$$(xy^{-1})^n = x^n(y^{-1})^n = 1 \cdot y^{-n} = (y^n)^{-1} = 1^{-1} = 1$$
so $G$ is a subgroup of $\langle \mathbb{C} \setminus \{0\}, \cdot \rangle$ by the subgroup test, whence $\mu_n$ forms a group with respect to complex multiplication.

Note that the elements of $\mu_n$ are precisely the distinct roots of the polynomial $f(X) = X^n - 1 \in \mathbb{C}[X]$. Since $e^{2\pi i} = 1$, it is clear $e^{(2\pi i k)/n} \in \mathbb{C}$ is a root of $f(X)$ for each $k \in \{1, \ldots, n\}$. Further, $e^{(2\pi i k_1)/n} \neq e^{(2\pi i k_2)/n}$ for any $k_1 \neq k_2 \in \{1, 2, \ldots, n\}$, so there are $n$ roots of $f(X)$ of this form. Since there are exactly $n$ roots of $f(X)$ over $\mathbb{C}$, we must have

$$\mu_n = \{e^{(2\pi i k)/n} \mid k \in \{1, \ldots, n\}\}$$

whence $(\mu_n, \cdot)$ is cyclic with generator $e^{(2\pi i)/n}$.

(b) Let $G = \langle x \rangle$ be a cyclic group of order $n$. We first prove that every subgroup of $G$ is cyclic.

Suppose $H$ is a subgroup of $G$. If $H = \{e\} = \{x^0\}$, the claim is trivially true. Suppose $H$ is nontrivial, i.e. there exists $g \neq e \in H$. Since $G$ is cyclic, every nonidentity element of $H$ is of the form $x^k$ for some positive integer $k$ between 1 and $n - 1$. By the well-ordering principle, there is a least such integer; call this $l$. Since $H$ is a subgroup, it is clear $\langle x^l \rangle \subseteq H$. Let $x^k \in H$. Using Euclidean division, write $k = ql + r$ for some $0 \leq r < l$. Then $x^k = x^{ql+r} = (x^l)^qx^r$, so $x^r = (x^l)^{-q}x^k$. Since $H$ is a subgroup, it follows $x^r \in H$; but $r < l$, so by the minimality of $l$, we must have $r = 0$, whence $k = ql$, so $H \subseteq \langle x^l \rangle$.

Now let $n = kd$ for positive integers $k, d$. Then $x^d$ has order $k$, i.e. $\langle x^d \rangle \subseteq G$ has order $k$, so $G$ has at least one subgroup of order $k$. Consider the subset $H$ of $G$ consisting of all elements of order dividing $k$, i.e. $H = \{x \in G \mid x^k = e\}$. Note that $e \in H$, and since $G$ is cyclic (hence abelian), for any $g_1, g_2 \in H$, we have $(g_1g_2)^k = g_1^k g_2^k = ee = e$, so $g_1g_2 \in K$. Finally, note that if $g \in H$, then $(g^{-1})^k = g^{-k} = (g^k)^{-1} = e^{-1} = e$, so $g^{-1} \in H$. Hence, $H$ is a subgroup of $G$.

Since $H$ is a subgroup of $G$ and $G$ is cyclic, it follows that $H$ is cyclic. Since every element of $H$ has order dividing $k$, it follows that the generator of $H$ has at most order $k$, so $H$ has at most $k$ elements.

Conversely, let $H'$ be any subgroup of $G$ which has order $k$ (by the above, at least one must exist). Then $H'$ is cyclic, and is generated by an element $h \in G$ of order $k$. But then $h \in H$, so $\langle h \rangle = H' \subseteq H$, so in particular, $H$ has exactly $k$ elements, and $H' = H$.

26 Problem 3.9

Let $G$ be a finite group of even order $2n$. Let $\Gamma = \{a \mid a \in G, a \neq a^{-1}\}$, i.e. let $\Gamma$ be the subset of $G$ of elements which do not have order 1 or 2. Note that if $x \in \Gamma$, then $x^{-1}$ is also in $\Gamma$ and is distinct from $x$. Hence, $\Gamma$ must have even order, so $G \setminus \Gamma$ also has even order.

Since $e \in G \setminus \Gamma$, $G \setminus \Gamma$ has at least two elements, so $G$ must have an element of order 2 (the only element of order 1 in $G$ is $e$).
27 Problem 3.10

Note that a matrix \( A \in \text{GL}_n(\mathbb{Z}/p\mathbb{Z}) \) if and only if the columns of \( A \) are linearly independent over \( \mathbb{Z}/p\mathbb{Z} \). We count the number of ways one can construct such \( A \). There are \( p^n - 1 \) choices for the first column \( c_1 \) of \( A \), since the only restriction is that \( c_1 \) is not the zero vector. There are \( p^n - p \) choices for the second column \( c_2 \) of \( A \); we must only avoid the \( p \) distinct multiples of the first column \( c_1 \). In general, there are \( p^n - p^{j-1} \) choices for the \( j^{\text{th}} \) column \( c_j \), since there are \( p^{j-1} \) distinct linear combinations \( k_1c_1 + k_2c_2 + \cdots + k_{j-1}c_{j-1}, k_i \in \mathbb{Z}/p\mathbb{Z} \) (note that each linear combination is distinct, or else there would be a nontrivial linear dependence among the columns). Hence,

\[
|\text{GL}_2(\mathbb{Z}/p\mathbb{Z})| = \prod_{i=0}^{n-1} p^n - p^i
\]

28 Problem 4.1

Suppose \( \gcd(m_i, m_j) = 1 \) for each \( i \neq j \), and let \( m = \prod_{i=1}^{k} m_i \). Then by the Chinese Remainder Theorem,

\[
\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z}
\]

so \( \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z} \) is cyclic. Alternatively, the order of \((1,1,\ldots,1)\) in \( \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z} \) is \( \text{lcm}(m_1,m_2,\ldots,m_k) = m \), so one can see directly that \( \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z} \) is cyclic. Suppose that \( \gcd(m_i, m_j) > 1 \) for some \( i \neq j \), and let \( n = \text{lcm}(m_1,m_2,\ldots,m_k) \); note that \( n < m \). But \( n(a_1,\ldots,a_k) = (na_1,\ldots,na_k) = 0 \) for all \((a_1,\ldots,a_k) \in \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z} \), since any multiple of \( m_i \) annihilates every element of \( \mathbb{Z}/m_i\mathbb{Z} \). Hence, every element of \( \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z} \) has order dividing \( n < m \), so in particular, no element has order \( m \), i.e. \( \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z} \) is not cyclic.

29 Problem 4.2

The claim is clear if \( K \subset H \) or \( H \subset K \), since then \( H \cup K = H \) or \( H \cup K = K \), which are both subgroups of \( G \). Suppose neither \( K \subset H \) nor \( H \subset K \). Then there exists \( k \in K \setminus H, h \in H \setminus K \). If \( kh \in K \), i.e. \( kh = k' \) for some \( k' \in K \), then \( h = k^{-1}k' \in K \), which is not the case by hypothesis. Similarly, \( kh \notin H \), so \( kh \notin K \cup H \), so \( K \cup H \) is not a subgroup.

30 Problem 4.3

Let \( G \) be a group, and let \( K, H \) be finite subgroups of \( G \) with relatively prime orders \( k \) and \( n \), respectively. Note \( K \cap H \) is a subgroup of both \( K \) and \( H \), so by Lagrange, the order of \( K \cap H \) divides both \( k \) and \( n \), and hence divides \( \gcd(k, n) = 1 \). Thus, \( |K \cap H| = 1 \), and since \( e \in K \) and \( e \in H \), we must have \( K \cap H = \{e\} \).
31 Problem 4.4

Let $G$ be a group with finitely many subgroups. Note that every element of $G$ has finite order; if there were $x \in G$ with infinite order, each of the cyclic subgroups $\langle x \rangle, \langle x^2 \rangle, \langle x^3 \rangle \ldots$ would be distinct subgroups of $G$, a contradiction. Let $\Omega = \{\langle a \rangle \mid a \in G\}$, i.e. let $\Omega$ be the collection of all cyclic subgroups of $G$ generated by elements of $G$. Since $G$ is the union of the cyclic subgroups generated by each of its elements, we have

$$G = \bigcup_{X \in \Omega} X$$

Since $G$ has finitely many subgroups, it is clear $\Omega$ is finite. Further, since every element of $G$ has finite order, every element of $\Omega$ is finite. Hence, $G$ is a finite union of finite subgroups, whence $G$ is finite.

32 Problem 4.5

Suppose $|x| = |G|$ for some $x \in G$. Then $|\langle x \rangle| = |x| = |G|$. Since $G$ is finite, and $\langle x \rangle \subset G$, this means $\langle x \rangle = G$, i.e. $G$ is cyclic.

33 Problem 4.6

The only group of order 1 up to isomorphism is the trivial group. All groups of prime order are cyclic; indeed, if $|G| = p$ for some prime $p$, then any non-identity element $g \in G$ generates a cyclic subgroup $\langle g \rangle$ whose order divides $|G| = p$, and hence must be all of $G$. Thus, all groups of order 2, 3 are cyclic. By problem 4.1, the group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is not cyclic, so this is a non-cyclic group of the smallest order.

34 Problem 4.7

Let $S_3 = \{e, (1, 2), (2, 3), (1, 3), (1, 2, 3), (1, 3, 2)\}$. Each transposition of $S_3$ generates a distinct cyclic subgroup of order 2, and each 3-cycle generates the same cyclic subgroup of order 3. We claim that (in addition to the trivial subgroup and $S_3$) these are all subgroups of $S_3$. Indeed, let $H$ be a subgroup of $S_3$. If $H$ contains a transposition and a 3-cycle, then by Lagrange $H$ is divisible by both 2 and 3, hence by 6, so $H = S_3$. One may compute

$$(1, 2)(2, 3) = (1, 2, 3); (1, 2)(1, 3) = (1, 3, 2); (1, 3)(2, 3) = (1, 3, 2)$$

so if $H$ contains two distinct transpositions, it also contains a 3-cycle and hence must be all of $S_3$. Thus, the subgroups of $S_3$ are:

$$\{e\}, \langle (1, 2) \rangle, \langle (2, 3) \rangle, \langle (1, 3) \rangle, \langle (1, 2, 3) \rangle, S_3$$

One can compute directly that $\langle (1, 2, 3) \rangle$ is a normal subgroup of $S_3$. Alternatively, $\langle (1, 2, 3) \rangle$ is a subgroup of index 2 in $S_3$, hence normal (see problem 5.6). However, note that

$$(1, 2)(1, 3)(1, 2)^{-1} = (1, 2)(1, 3)(1, 2) = (1, 2)(1, 2, 3) = (2, 3)$$
\((1, 2)(2, 3)(1, 2)^{-1} = (1, 2)(2, 3)(1, 2) = (1, 2)(1, 3, 2) = (1, 3)\)
\((1, 3)(1, 2)(1, 3)^{-1} = (1, 3)(1, 2)(1, 3) = (1, 3)(1, 2, 3) = (1, 2)\)

So \(\{e\}, \{(1, 2, 3)\}\), \(S_3\) are the only normal subgroups of \(S_3\).

### 35 Problem 4.8

Recall that for any group \(G\) and subset \(S \subseteq G\), the subgroup \(\langle S \rangle\) generated by \(S\) consists of all strings (of arbitrary length \(n\)) of the form \(s_1^{\varepsilon_1}s_2^{\varepsilon_2}\cdots s_n^{\varepsilon_n}\), where \(\varepsilon_i \in \{1, -1\}\) for each \(i = 1, \ldots, n\). Let \(H\) be a subgroup of \(G\). Then clearly, \(H \subseteq \langle H \rangle\), so it remains to show the inclusion \(\langle H \rangle \subset H\). We do so by induction on \(n\), the length of the string. For \(n = 1\), it is clear, since \(h^1\) and \(h^{-1}\) are in \(H\) for all \(h \in H\), as \(H\) is a subgroup of \(G\). Suppose it is true for \(n = k > 1\). Consider a string of symbols \(h_1^{\varepsilon_1}h_2^{\varepsilon_2}\cdots h_{k+1}^{\varepsilon_{k+1}}\) where \(h_i \in H\) for each \(i = 1, \ldots, k+1\); by associativity, we can write this as \(h_1^{\varepsilon_1}(h_2^{\varepsilon_2}\cdots h_{k+1}^{\varepsilon_{k+1}})\). By the induction hypothesis \((h_2^{\varepsilon_2}\cdots h_{k+1}^{\varepsilon_{k+1}}) \in H\), and clearly \(h_1^{\varepsilon_1} \in H\). Since \(H\) is a subgroup, it follows \((h_1^{\varepsilon_1}(h_2^{\varepsilon_2}\cdots h_{k+1}^{\varepsilon_{k+1}}) \in H\), completing the proof that \(\langle H \rangle \subset H\) by induction.

### 36 Problem 4.9

First, we enumerate the elements of \(\text{GL}_2(\mathbb{Z}/2\mathbb{Z})\). If \(A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}_2(\mathbb{Z}/2\mathbb{Z})\), then \(\det(A) = ad - bc \neq 0\), i.e. \(ad \neq bc\). If \(a = 0\) or \(d = 0\), then \(b = c = 1\); and likewise, if \(a = d = 1\), then \(b = 0\) or \(c = 0\), so this gives six elements:

\[
\text{GL}_2(\mathbb{Z}/2\mathbb{Z}) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}
\]

Now, by writing down the group tables for \(\text{GL}_2(\mathbb{Z}/z\mathbb{Z})\) and \(S_3\), one can check that the assignments

\[
\begin{align*}
(1, 2) & \mapsto e; \quad (1, 3) \mapsto (1, 2); \quad (2, 3) \mapsto (2, 3); \quad (0, 1) \mapsto (1, 3) \\
(1, 1) & \mapsto (1, 2, 3); \quad (0, 1) \mapsto (1, 3, 2)
\end{align*}
\]

define a group isomorphism \(\text{GL}_2(\mathbb{Z}/2\mathbb{Z}) \to S_3\). Later, we will have a more efficient approach to this problem: one can show that there are only two groups of order 6 up to isomorphism, namely \(S_3\) and \(\mathbb{Z}/6\mathbb{Z}\).

### 37 Problem 4.10

Let \(f : \mathbb{Q} \to \mathbb{Z}/m\mathbb{Z}\) be a group homomorphism. For any \(p/q \in \mathbb{Q}\), we may write \(p/q\) as \(m(p/qm) = \), where multiplication by \(m\) corresponds with repeating the group operation \(m\)
times. Thus, since \( f \) is a homomorphism,

\[
f \left( \frac{p}{q} \right) = f \left( m \left( \frac{p}{mq} \right) \right) = mf \left( \frac{p}{qm} \right) = [0]_m
\]
since multiplication by \( m \) is trivial on \( \mathbb{Z}/m\mathbb{Z} \).

### 38 Problem 5.1

1. \( H \) is the image of the inclusion homomorphism \( H \hookrightarrow G \).

2. \( N \) is the kernel of the projection homomorphism \( G \to G/N \).

### 39 Problem 5.2

Let \( n \) be a natural number, and let \( f : \mathbb{Q}/\mathbb{Z} \to \mathbb{Q}/\mathbb{Z} \) be the map given by \( f(a+\mathbb{Z}) = na+\mathbb{Z} \).

Let \( a \in \mathbb{Q} \). Then for any \( k \in \mathbb{Z} \),

\[
f(a + k + \mathbb{Z}) = n(a + k) + \mathbb{Z} = na + nk + \mathbb{Z} = na + \mathbb{Z} = f(a + \mathbb{Z})
\]

Hence, \( f \) is well-defined. Let \( a + \mathbb{Z}, b + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z} \). Then

\[
f(a + b + \mathbb{Z}) = f(a+b+\mathbb{Z}) = n(a+b)+\mathbb{Z} = na+nb+\mathbb{Z} = (na+\mathbb{Z})+(nb+\mathbb{Z}) = f(a)+f(b)
\]

so \( f \) is a group homomorphism. Note that if \( p/q + \mathbb{Z} \in \mathbb{Q} \) such that \( p/q + \mathbb{Z} \in \ker(f) \), then

\[
f \left( \frac{p}{q} + \mathbb{Z} \right) = \frac{np}{q} + \mathbb{Z} = 0 + \mathbb{Z}
\]

i.e. \( np/q \in \mathbb{Z} \). Hence \( p/q + \mathbb{Z} \in \ker(\varphi) \) if and only if \( q \mid n \), so \( \ker(f) = \{ p/q + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z} \mid \ q \text{ divides } n \} = \langle q/n + \mathbb{Z} \rangle \). Let \( a + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z} \). Then note

\[
f \left( \frac{a}{n} + \mathbb{Z} \right) = n \left( \frac{a}{n} \right) + \mathbb{Z} = a + \mathbb{Z}
\]

so \( f \) is surjective, i.e. \( \text{Im}(f) = \mathbb{Q}/\mathbb{Z} \). Note that this problem shows that \( \mathbb{Q}/\mathbb{Z} \) is isomorphic to a proper quotient of itself.

### 40 Problem 5.3

Let \( K \subset H \subset G \) be subgroups such that \([G : K] = n < \infty\). Note that the index of \( K \) in \( H \) must be finite, since the cosets of \( K \) in \( H \) are cosets of \( K \) in \( G \), namely those whose representatives are elements of \( H \). Furthermore, the index of \( H \) in \( G \) must be finite; indeed, there is an injective map from the cosets of \( H \) in \( G \) to the cosets of \( K \) in \( G \) given by \( gH \mapsto gK \), since if \( g_1K = g_2K \), then \( g_2^{-1}g_1 \in K \subset H \), so \( g_1H = g_2H \). With this information, let \([G : H] = m < \infty, [H : K] = s < \infty\), and let \( \{ g_1H, g_2H, \ldots, g_mH \} \) and
Let \( \{h_1K, \ldots, h_sK\} \) be a complete list of cosets of \( H \) in \( G \) and a complete list of cosets of \( K \) in \( H \) respectively. We claim that \( \Omega := \{g_hj_hK\}_{1 \leq i \leq m, 1 \leq j \leq s} \) is a complete list of cosets of \( K \) in \( G \), whence \( [G : K] = ms = [G : H][H : K] \).

Indeed, for any \( g \in G \), \( g \in g_iH \) for some \( 1 \leq i \leq m \), since the cosets of \( H \) in \( G \) partition \( G \). Then \( g = g_ih \) for some \( h \in H \), and because the cosets of \( K \) in \( H \) likewise partition \( H \), there is some \( 1 \leq j \leq s \) so that \( h \in h_jK \), i.e. \( h = h_jk \) for some \( k \in K \). Then \( g = g_ih_jk \), i.e. \( g \in g_ih_jK \), so the elements of \( \Omega \) cover \( G \). Furthermore, each of these cosets are distinct. Suppose \( i \neq i' \). Then \( g_ih_jK \subset g_iH \) and likewise \( g_i'h_j'K \subset g_i'H \), and since \( g_iH \cap g_i'H = \emptyset \), this shows \( g_ih_jK \neq g_i'h_j'K \). Suppose \( g_ih_jK = g_i'h_j'K \). Then \( h_jK = h_j'K \), so \( j = j' \); thus, all elements of \( \Omega \) are distinct cosets of \( K \) in \( G \), completing the proof.

### 41 Problem 5.4

Let \( \Omega \) be the set of left cosets of \( H \) in \( G \), and let \( \Gamma \) be the set of right cosets of \( H \) in \( G \). Let \( \varphi: \Gamma \to \Omega \) be the map given by \( \varphi(Ha) = a^{-1}H \). Suppose \( Ha = Ha' \), i.e. \( a'a^{-1} \in H \). Since \( H \) is a subgroup, \( (a'a^{-1})^{-1} = aa'^{-1} \in H \), hence \( aa'^{-1}H = H \), so \( \varphi(Ha) = a^{-1}H = a'^{-1}H = \varphi(Ha') \). Thus, \( \varphi \) is well-defined.

Suppose \( \varphi(Ha) = \varphi(Hb) \) for some \( Ha, Hb \in \Gamma \), i.e. \( a^{-1}H = b^{-1}H \). Then \( ba^{-1}H = H \), so \( ba^{-1} \in H \), whence \( H = Hba^{-1} \), i.e. \( Ha = Hb \). Hence \( \varphi \) is injective.

Further, for any left coset \( gH \in \Omega \), \( \varphi(Hg^{-1}) = (g^{-1})^{-1}H = gH \), so \( \varphi \) is surjective. Hence, \( \varphi \) is a well-defined bijection between \( \Gamma \) and \( \Omega \).

### 42 Problem 5.5

Let \( f: G \to H \) be a surjective group homomorphism.

(a) Let \( H' \) be a subgroup of \( H \), and let \( G' = f^{-1}(H') \). Since \( H' \) is a subgroup of \( H \), \( e_H \in H' \), so \( f^{-1}(e_H) = e_G \in G' \). Further, let \( g_1, g_2 \in G' \). Then \( f(g_1g_2) = f(g_1)f(g_2) \in H' \), since \( f(g_1), f(g_2) \in H' \), and \( H' \) is a subgroup of \( H \), so \( g_1g_2 \in G' \). Finally, note that for any \( g \in G' \), \( f(g^{-1}) = f(g)^{-1} \in H' \), so \( g^{-1} \in G' \). Hence, \( G' \) is a subgroup of \( G \).

Let \( \Omega \) be the set of subgroups of \( H \), \( \xi \) be the set of all subgroups of \( G \), and let \( \Gamma \) be the set of all subgroups of \( G \) containing \( \ker(f) \). Let the map \( \psi: \Omega \to \xi \) be given by \( \psi(H') = f^{-1}(H') \). Since \( e_H \in H' \) for every \( H' \in \Omega \), \( \ker(f) = f^{-1}(e_H) \subseteq f^{-1}(H) = \psi(H') \)

for all \( H' \in \Omega \), so \( \Im(\psi) \subseteq \Gamma \).

Suppose \( \psi(H_1) = f^{-1}(H_1) = f^{-1}(H_2) = \psi(H_2) \) for some \( H_1, H_2 \in \Omega \). Then since \( f \) is surjective, \( H_1 = f(f^{-1}(H_1)) = f(f^{-1}(H_2)) = H_2 \), so \( \psi \) is injective.

Let \( G' \in \Gamma \). We want to find \( H' \in \Omega \) such that \( G' = \psi(H') = f^{-1}(H') \). Note \( f(G') \) is a subgroup of \( H \), so put \( H' = f(G') \); we want to show \( G' = \psi(H') = f^{-1}(f(G')) \). The inclusion \( G' \subseteq f^{-1}(f(G')) \) is clear. Suppose \( h = f(g) \in f(G') \) for \( g \in G \). Then \( f(g) = f(g') \) for some \( g \in G' \). Then \( k = g(g')^{-1} \in \ker(f) \subseteq G' \), so \( g = kg' \in G' \).

Hence \( f^{-1}(f(G')) \subseteq G' \), so \( f^{-1}(f(G')) = G' \), i.e. \( \psi \) is surjective. Hence, \( \psi: \Omega \to \Gamma \) is a bijection.

(b) Let \( H' \) be a normal subgroup of \( H \), and let \( \pi: H \to H/H' \) be the canonical projection homomorphism. Since \( \pi \) and \( f \) are both surjective homomorphisms, \( \pi \circ f: G \to H/H' \)
is also a surjective homomorphism. The kernel of $\pi \circ f$ is precisely the preimage of the kernel of $\pi$ under $f$, i.e. $G' = \ker(\pi \circ f) = f^{-1}(\ker(\pi)) = f^{-1}(H)$. Hence, by the first isomorphism theorem,

$$G/G' \cong H/H'$$

Finally, since $G'$ is the kernel of $\pi \circ f : G \to H/H'$, it is a normal subgroup of $G$. Let $\psi : \Omega \to \Gamma$ be the bijection given above. Let $\Omega'$ be the set of all normal subgroups of $H'$, and let $\Gamma'$ be the set of all normal subgroups of $G$ containing $\ker(f)$. We showed above that $\operatorname{Im}(\psi|_{\Omega'})$ (the image of $\psi$ restricted to $\Omega'$) lies in $\Gamma'$. Further, the exact proof given above which shows $\psi : \Omega \to \Gamma$ is a bijection in fact shows $\psi|_{\Omega'} : \Omega' \to \Gamma'$ is a bijection.

43 Problem 5.6

Let $G$ be a group, and let $H$ be a subgroup of $G$ of index 2. Then there are precisely two left cosets of $H$ in $G$, $H$ and $aH$ for some $a \in G$ such that $a \notin H$. Similarly, there are two right cosets of $H$ in $G$, $H$ and $Ha$. Since the (left and right) cosets of $H$ in $G$ partition $G$, we must have $aH = G \setminus H = Ha$. Thus, the left and right cosets of $H$ in $G$ coincide, so $H$ is normal in $G$.

44 Problem 5.7

Let $H \subset G$ be a subgroup. Suppose for any $a \in G$, there exists $b \in G$ such that $aH = Hb$, i.e. $aHb^{-1} = H$. Then in particular, $Hb \supset eb = b = ah \in aH$ for some $h \in H$, so

$$aHb^{-1} = aH(a^{-1})^{-1} = aHh^{-1}a = aHa^{-1} = H$$

for all $a \in G$. Hence, $H \trianglelefteq G$.

45 Problem 5.8

Let $m > 1$. Note that $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ can be generated by 3 elements, namely $([1]_m, [0]_m, [0]_m), ([0]_m, [1]_m, [0]_m), ([0]_m, [0]_m, [1]_m)$. Now, for any prime $p$, note that $(\mathbb{Z}/p\mathbb{Z})^k$ cannot be generated by fewer than $k$ elements; indeed, $(\mathbb{Z}/p\mathbb{Z})^k$ is a $\mathbb{Z}/p\mathbb{Z}$-vector space, and so any (linear) generating set over $\mathbb{Z}/p\mathbb{Z}$ has at least $k$ elements; since generating $(\mathbb{Z}/p\mathbb{Z})^k$ as a group is an stronger condition, any generating set for $(\mathbb{Z}/p\mathbb{Z})^k$ has at least $k$ elements. For any prime $p$ dividing $m$, there is a well-defined surjective homomorphism $(\mathbb{Z}/m\mathbb{Z})^3 \to (\mathbb{Z}/p\mathbb{Z})^3$ given by reduction mod $p$ in each component, and so any set of generators for $(\mathbb{Z}/m\mathbb{Z})^3$ must map to a set of generators of $(\mathbb{Z}/p\mathbb{Z})^3$. In particular, if $(\mathbb{Z}/m\mathbb{Z})^3$ could be generated by two elements, then so could $(\mathbb{Z}/p\mathbb{Z})^3$, a contradiction.

46 Problem 5.9

Let $p$ be an odd prime. Note that $x^2 \equiv -1 \pmod{p}$ if and only if $(\mathbb{Z}/p\mathbb{Z})^\times$ has an element of order 4. Indeed, if $x^2 \equiv -1 \pmod{p}$, then $x^4 \equiv 1 \pmod{p}$, so $[x]_p$ has order 4. On the other
hand, \((\mathbb{Z}/p\mathbb{Z})^\times\) is a cyclic group of order \(p - 1\), and hence has a unique (cyclic) subgroup of order 2 by problem 3.8(b). In particular, \((\mathbb{Z}/p\mathbb{Z})^\times\) has a unique element of order 2, since each distinct element of order 2 generates a distinct cyclic subgroup of order 2. Since \([-1]_p\) is an element of \((\mathbb{Z}/p\mathbb{Z})^\times\) of order 2, this must be the unique element of order 2. Thus, if \([x]_p\) is an element of order 4 in \((\mathbb{Z}/p\mathbb{Z})^\times\), then \([x^2]_p\) is an element of order 2, and hence must be \([-1]_p\). Now, since \((\mathbb{Z}/p\mathbb{Z})^\times\) is cyclic of order \(p - 1\), it has an element of order 4 (that is, a cyclic subgroup of order 4) if and only if \(4 | p - 1\), i.e. \(p \equiv 1 \pmod{4}\).

47 Problem 5.10

Let \(H \neq G\) be a subgroup of \(G\) of finite index, i.e. \(|G/H| = n\). If \(G\) is trivial, then the claim is clearly true, so assume \(G\) is nontrivial.

Let \(\varphi : G \to S(G/H)\) be the group homomorphism given by \(x \mapsto f_x\), where \(f_x(aH) = xaH\) (i.e., let \(\varphi\) represent the action of \(G\) by left translation on the left cosets \(G/H\)). Then \(\ker(\varphi)\) is a normal subgroup of \(G\), and by the first isomorphism theorem, \(G/\ker(\varphi) \cong \operatorname{Im}(\varphi) \subseteq S(G/H)\). Since \(S(G/H)\) is finite, it follows that \(G/\ker(\varphi)\) is finite, so \(\ker(\varphi)\) has finite index in \(G\). It remains to show that \(\ker(\varphi)\) is not all of \(G\).

To see this, let \(x \in G\) such that \(x \notin H\). Then in particular, \(\varphi(x)(H) = f_x(H) = xH \neq H\), so \(x \notin \ker(\varphi)\).

48 Problem 6.1

Let \(G\) be a group, and let \(S \subset G\). Suppose \(S\) satisfies \(gSg^{-1} \subset S\) for all \(g \in G\). Let \(\langle S \rangle\) be the subgroup generated by \(S\). Let \(s \in S\), i.e. \(s = s_1^{\varepsilon_1} s_2^{\varepsilon_2} \cdots s_n^{\varepsilon_n}\), where \(s_1, s_2, \ldots, s_n \in S\), \(\varepsilon_i \in \{-1, 1\}\) for each \(i\). Then

\[
gs g^{-1} = g s_1^{\varepsilon_1} s_2^{\varepsilon_2} \cdots s_n^{\varepsilon_n} g^{-1} = (g s_1^{\varepsilon_1}) (g s_2^{\varepsilon_2}) \cdots (g s_n^{\varepsilon_n}) g^{-1} = (g s_1 g^{-1})^{\varepsilon_1} (g s_2 g^{-1})^{\varepsilon_2} \cdots (g s_n g^{-1})^{\varepsilon_n}\]

(technically, one should prove the above by induction, but this is not hard to show.) Since \(gs_i g^{-1} \in S\) for each \(i\) by hypothesis, it follows that \((gs_i g^{-1})^{\varepsilon_i} \in \langle S \rangle\) for each \(i\), whence \(gs g^{-1} = \prod_{i=1}^n (g s_i g^{-1})^{\varepsilon_i} \in \langle S \rangle\). Hence, \(g \langle S \rangle g^{-1} \subseteq \langle S \rangle\) for each \(g \in G\), so \(\langle S \rangle \leq G\). Note that in our proof that, in fact showed that if \(g S g^{-1} \subseteq \langle S \rangle\) for all \(g \in G\), then \(\langle S \rangle \leq G\) (with the trivial modification that the line beginning “Since \(gs_i g^{-1} \in S\)...” should instead read “Since \(gs_i g^{-1} \in \langle S \rangle\)...”).

49 Problem 6.2

It is clear that \(\mathbb{Q}/\mathbb{Z}\) has a cyclic subgroup of order \(n\) for each \(n \in \mathbb{N}\), namely \(H_n = \langle \frac{1}{n} + \mathbb{Z} \rangle\). Suppose \(\langle p/q + \mathbb{Z} \rangle \subset \mathbb{Q}/\mathbb{Z}\) is a cyclic subgroup of order \(n\); as always, we may assume \(\gcd(p, q) = 1\). Then \(n(p/q) \in \mathbb{Z}\), i.e. \(np = qk\) for some \(k \in \mathbb{Z}\). Since \(\gcd(p, q) = 1\), \(q \mid n\), so
n = qd for some d ∈ ℤ. Then p/q = pd/qd = pd/n, so ⟨p/q + ℤ⟩ = ⟨pd/n + ℤ⟩ ⊆ Hₙ. Since ⟨p/q + ℤ⟩ and Hₙ both have order n, ⟨p/q + ℤ⟩ = Hₙ.

50 Problem 6.3

Consider the homomorphism f: G → G given by f(x) = nx. In problem 5.2, we showed that this map is a well-defined surjective group homomorphism, so G/ker(f) ≅ G by the first isomorphism theorem. In problem 5.2, we also identified ker(f) = Hₙ, so this proves the claim.

51 Problem 6.4

Suppose r + ℤ ∈ ℜ/ℤ has finite order, i.e. n(r + ℤ) = nr + ℤ = ℤ for some n ∈ ℕ. Then nr ∈ ℤ, so nr = k for some k ∈ ℤ, whence r = k/n, so r ∈ ℚ/ℤ ⊆ ℜ/ℤ. It’s clear that every element p/q + ℤ ∈ ℚ/ℤ has order dividing |q| ∈ ℤ, so the set of torsion elements of ℜ/ℤ is precisely ℚ/ℤ.

52 Problem 6.5

Let ϕ ∈ Aut(ℤ). Since 1 ∈ ℤ generates ℤ as a group, ϕ is determined by the value of ϕ(1); indeed, for n ∈ ℕ,

ϕ(n) = ϕ(1 + 1 + ⋯ + 1) = ϕ(1) + ϕ(1) + ⋯ + ϕ(1) = nϕ(1)

and

ϕ(n) = −ϕ(n) = −nϕ(1)

Furthermore, since ϕ is an automorphism, ϕ(1) must generate ℤ as an abelian group, so ϕ(1) ∈ {±1}, and thus |Aut(ℤ)| ≤ 2. It is straightforward to check that the assignment ϕ(1) = −1, corresponding to the “global” map ϕ(n) = −n defines an automorphism of ℤ (of order 2), which proves the claim.

Note that Inn(G) is trivial for any abelian group. Indeed, the conjugation automorphism ρₔ: G → G sends h to ghg⁻¹ = gg⁻¹h = h, so ρₔ = Idₙ for all g ∈ G. Applying this result to G = ℤ, we find Inn(ℤ) = {e}.

53 Problem 6.6

For each g ∈ G, let ρₔ: G → G be defined by ρₔ(h) = ghg⁻¹. To show that Inn(G) is a normal subgroup of Aut(G), it suffices to show that ϕ Inn(G)ϕ⁻¹ = Inn(G) for each ϕ ∈ Aut(G). For any ρₔ ∈ Inn(G),

(ϕ o ρₔ o ϕ⁻¹)(h) = ϕ(ρₔ(ϕ⁻¹(h))) = ϕ(ϕ⁻¹(h)g) = ϕ(ϕ⁻¹(h))(ϕ(g))⁻¹ = ϕ(g)hϕ(g⁻¹)⁻¹

for all h ∈ G, so ϕ o ρₔ o ϕ⁻¹ = ρₔϕ(ϕ) ∈ Inn(G). Hence, ϕ Inn(G)ϕ⁻¹ ⊆ Inn(G). Since ϕ: G → G is a bijection, ϕ Inn(G)ϕ⁻¹ = Inn(G) as desired.
54 Problem 6.7

As noted in discussion, every group automorphism of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is simultaneously a vector space isomorphism of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and hence $\text{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong \text{GL}_2(\mathbb{Z}/2\mathbb{Z})$. As shown in problem 4.9, $\text{GL}_2(\mathbb{Z}/2\mathbb{Z}) \cong S_3$.

55 Problem 6.8

Let $n \geq 3$. We claim $S_n$ has trivial center. Let $\sigma \neq e \in S_n$. Let $i \in \{1, \ldots, n\}$ such that $\sigma(i) = j \neq i$ for some $j \in \{1, \ldots, n\}$. Since $\sigma$ is a bijection, $\sigma(l) \neq j$ for any $l \neq i$. Let $\gamma \in S_n$ be the transposition which interchanges $i$ and some $k \neq j$; this is possible since $n \geq 3$. Then note that

$$\sigma(\gamma(i)) = \sigma(k) \neq j$$

but

$$\gamma(\sigma(i)) = \gamma(j) = j$$

Since $(\sigma \circ \gamma)(i) \neq (\gamma \circ \sigma)(i)$, it follows $\gamma \sigma \neq \sigma \gamma$. Hence, no nontrivial element of $S_n$ commutes with every element of $S_n$, so $Z(S_n) = \{e\}$.

56 Problem 6.9

(a) Suppose $H$ is characteristic in $G$. Then $f(H) = H$ for every $f \in \text{Aut}(G)$. In particular, $f(H) = H$ for every $f \in \text{Inn}(G) \subseteq \text{Aut}(G)$. Let $f_g \in \text{Inn}(G)$ be the map $x \mapsto gxg^{-1}$. Then $f_g(H) = H$ for every $g \in G$, i.e. $gHg^{-1} = H$ for every $g \in G$, so $H$ is normal in $G$.

(b) Suppose $K$ is a characteristic subgroup of $H$, and $H$ is a characteristic subgroup of $G$. Let $f \in \text{Aut}(G)$. Then $f(H) = H$, so $f$ restricts to an automorphism of $H$, i.e. $f|_H \in \text{Aut}(H)$. Hence, since $K$ is a characteristic subgroup of $H$, $f(K) = f|_H(K) = K$, so $K$ is a characteristic subgroup of $G$.

(c) The proof is essentially identical to part (b). Suppose $K$ is a characteristic subgroup of $H$, and $H$ is a normal subgroup of $G$. Let $f \in \text{Inn}(G)$. Then $f(H) = H$, so $f$ restricts to an automorphism of $H$, i.e. $f|_H \in \text{Aut}(H)$. Hence, since $K$ is a characteristic subgroup of $H$, $f(K) = f|_H(K) = K$, so $K$ is a normal subgroup of $G$.

57 Problem 6.10

Let $G$ be a finite group, and let $N$ be an abelian normal subgroup of $G$. Suppose that the orders $|G/N|$ and $|\text{Aut}(N)|$ are relatively prime (note $\text{Aut}(N)$ is finite, since $N$ is finite). Since $N$ is a normal subgroup of $G$, there is a homomorphism from $G$ to $\text{Aut}(N)$ induced by the action of $G$ on $N$ by conjugation. More specifically, there is a homomorphism $\varphi: G \to \text{Aut}(N)$ given by $\varphi(g) = f_g$, where $f_g(n) = gng^{-1}$ for each $n \in N$.

Note that $\ker(\varphi) = \{g \in G \mid f_g(n) = n \text{ for all } n \in N\} = \{g \in G \mid gng^{-1} = n \text{ for all } n \in N\}$.
\[ \{ g \in G \mid gn = ng \text{ for all } n \in N \} \], i.e., \( \ker(\varphi) \) is the set of elements of \( G \) which commute with every element of \( N \). Since \( N \) is abelian, we clearly have \( N \subseteq \ker(\varphi) \). Put \( H = \text{Im}(\varphi) \); note \( H \) is a subgroup of \( \text{Aut}(N) \). By the first isomorphism theorem, we have \( G/\ker(\varphi) \cong H \). By Lagrange, \( |H| \mid |\text{Aut}(N)| \), so \( |G/\ker(\varphi)| \mid |\text{Aut}(N)| \). However, since \( N \subseteq \ker(\varphi) \), by the third isomorphism theorem,

\[ (G/N)/(\ker(\varphi)/N) \cong G/\ker(\varphi) \]

so in particular,

\[ |G/N| = |G/\ker(\varphi)| \cdot |\ker(\varphi)/N| \]

Hence, \( |G/\ker(\varphi)| \mid |G/N| \). Since \( |G/N| \) and \( |\text{Aut}(N)| \) are relatively prime by hypothesis, we must have \( |G/\ker(\varphi)| = 1 \), i.e., \( G = \ker(\varphi) \). But then every element of \( N \) commutes with every element of \( G \), so \( N \subseteq Z(G) \).

58 Problem 7.1

Note that \( (456)(145) \) sends 1 to 5, 2 to 2, 3 to 3, 4 to 6, 5 to 1, and 6 to 4, and so can be written as \( (15)(46) \). Similarly, \( (1234)(15)(46) \) sends 1 to 5, 2 to 3, 3 to 4, 4 to 6, 5 to 2, and 6 to 1, and so can be written as \( (152346) \).

59 Problem 7.2

1. Using (c) (or computing by hand), \( |(1234)(567)| = \text{lcm}(3, 4) = 12 \).

2. The order of any \( k \)-cycle is \( k \). Indeed, it is clear that the order of \( \sigma := (a_1, \ldots, a_k) \) divides \( k \). However, one can prove by induction that \( \sigma^n \) sends \( a_1 \) to \( a_n \) for each \( 1 \leq n < k \), so \( \sigma^n \) does not have order \( < k \). Note that we cannot use (c) to answer this question: we are going to use it to prove (c)!

3. Let \( \sigma \in S_n \) be the unique product of disjoint cycles \( \tau_1 \tau_2 \cdots \tau_r \) of lengths \( k_1, \ldots, k_r \), and let \( k = \text{lcm}(k_1, \ldots, k_r) \). Since the cycles \( \tau_1, \ldots, \tau_r \) are disjoint, they commute, so for any \( n \in \mathbb{N} \),

\[ \sigma^n = (\tau_1 \tau_2 \cdots \tau_r)^n = \tau_1^n \tau_2^n \cdots \tau_r^n \]

Further, one can prove by induction on \( n \) that for any \( n \in \mathbb{N} \), if two cycles \( \gamma, \rho \) are disjoint, then so are \( \gamma^n, \rho^n \). Intuitively, this is obvious: \( \gamma \) and \( \rho \) permute different subsets of numbers, so their powers must as well; more rigorously, if \( \gamma \) fixes every element which \( \rho \) permutes, then so does every power of \( \gamma \), and vice versa. Hence, it follows that

\[ \sigma^n = \tau_1^n \tau_2^n \cdots \tau_r^n = e \iff \tau_1^n = \tau_2^n = \cdots = \tau_r^n = e \]

Let \( m \) be the order of \( \sigma \). By (b) and the preceding line, \( k_i \) divides \( m \) for each \( i = 1, \ldots, r \), so \( k \) divides \( m \). On the other hand, it is clear that \( \sigma^k = e \), so \( m \) divides \( k \), whence \( k = m \).
Problem 7.3

Every element $\sigma \in S_5$ can be uniquely written as a product of disjoint cycles $\tau_1 \tau_2 \cdots \tau_r$ with cycle lengths $k_1, \ldots, k_r > 0$ satisfying $k_1 + \cdots + k_r = 5$. By the preceding problem, the order of $\sigma$ is given by $\text{lcm}(k_1, \ldots, k_r)$, so it is sufficient to compute all distinct partitions $(k_1, \ldots, k_r)$ of 5 and find the partition that maximizes $\text{lcm}(k_1, \ldots, k_r)$ (it is clear that for each such partition of 5, there is a product of $r$ disjoint cycles of lengths $k_1, \ldots, k_r$ in $S_5$). We list the partitions of 5 and their associated lcms here:

<table>
<thead>
<tr>
<th>Partitions</th>
<th>LCMs</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 + 1 + 1 + 1 + 1 = 5</td>
<td>$\text{lcm}(1, 1, 1, 1) = 5$</td>
</tr>
<tr>
<td>1 + 1 + 1 + 2 = 5</td>
<td>$\text{lcm}(1, 1, 1, 2) = 2$</td>
</tr>
<tr>
<td>1 + 2 + 2 = 5</td>
<td>$\text{lcm}(1, 2, 2) = 2$</td>
</tr>
<tr>
<td>1 + 1 + 3 = 5</td>
<td>$\text{lcm}(1, 1, 3) = 3$</td>
</tr>
<tr>
<td>1 + 4 = 5</td>
<td>$\text{lcm}(1, 4) = 4$</td>
</tr>
<tr>
<td>2 + 3 = 5</td>
<td>$\text{lcm}(2, 3) = 6$</td>
</tr>
<tr>
<td>5 = 5</td>
<td>$\text{lcm}(5) = 5$</td>
</tr>
</tbody>
</table>

Hence, the largest order an element of $S_5$ can have is 6, which corresponds to the disjoint product of a 2-cycle with a 3-cycle, e.g. $(12)(345)$.

Problem 7.4

Let $\sigma \in S_5$ commute with $\tau = (123)$. Then $\tau \sigma$ sends 4 to $\tau(\sigma(4))$, whereas $\sigma(\tau(4)) = \sigma(4)$, so $\sigma(4)$ is fixed by $\tau$, i.e. $\sigma(4) \in \{4, 5\}$. By a similar argument $\sigma(5)$ is fixed by $\tau$, so $\sigma(5) \in \{4, 5\}$. Since $\sigma$ is a bijection, $\sigma$ either fixes both 4 and 5, or $\sigma$ interchanges 4 and 5. This also means that $\sigma|_{\{1,2,3\}} \in S(\{1,2,3\})$. Performing similar computations on 1, 2, 3, we get the following constraints:

\[
\begin{align*}
\tau(\sigma(1)) &= \sigma(2) \\
\tau(\sigma(2)) &= \sigma(3) \\
\tau(\sigma(3)) &= \sigma(1)
\end{align*}
\]

If $\sigma(1) = 1$, then $\sigma(2) = \tau(1) = 2, \sigma(3) = \tau(2) = 3$. If $\sigma(1) = 2$, then $\sigma(2) = \tau(2) = 3, \sigma(3) = \tau(3) = 1$. If $\sigma(1) = 3$, then $\sigma(2) = \tau(3) = 1, \sigma(3) = \tau(1) = 2$. Hence, the set of elements of $S_5$ which commute with $(123)$ are a subset of

\[S := \{e, (123), (132), (45), (123)(45), (132)(45)\}\]

and it is easy to see that every element of $S$ commutes with $(123)$, so in fact $S$ is exactly the subset of $S_5$ which commutes with $(123)$.

Remark 61.0.1. Another way to make this computation is the following. The condition $\sigma \tau = \tau \sigma$ is equivalent to $\sigma \tau \sigma^{-1} = \tau$; since $\sigma \tau \sigma^{-1} = (\sigma(1), \sigma(2), \sigma(3)) = (123)$, it follows that $\sigma|_{\{1,2,3\}} \in \langle \tau \rangle \subset S_3$. Everything above can now be deduced.
62 Problem 7.5

(a) Let $G$ be a group, and define a relation on $G$ by $a \sim b$ if there exists $g \in G$ such that $a = gb^{-1}$. Then $a = eae^{-1}$, so $\sim$ is reflexive; if $a = gb^{-1}$, then $b = g^{-1}ag = g^{-1}a(g^{-1})^{-1}$, so $\sim$ is symmetric; and if $a = gb^{-1}, b = hch^{-1}$, then $a = ghch^{-1}g^{-1} = ghc(gh)^{-1}$, so $\sim$ is transitive. Hence, conjugacy is an equivalence relation on $G$.

(b) Recall that any two elements of $S_n$ are conjugate if and only if they have the same cycle type. It therefore suffices to enumerate the cycle types of $S_n$ for $n = 3, 4$, and the elements of $S_n$ which have this cycle type.

(1) $S_3$: Note $S_3 = \{e, (12), (23), (13), (123), (132)\}$, so the only possible cycle types are the identity, transpositions, and 3-cycles, each sharing their own conjugacy class. Therefore, the possible conjugacy classes are:

$$c_1 = \{e\}, c_2 = \{(12), (23), (13)\}, c_3 = \{(123), (132)\}$$

(2) $S_4$: The possible elements of $S_4$ are $k$-cycles for $1 \leq k \leq 4$, and products of disjoint transpositions. Hence, the possible cycle types are (1), (2), (3), (4), and (2, 2). This gives 5 conjugacy classes, which we enumerate explicitly below:

$$c_1 = \{e\}; c_2 = \{(12), (13), (14), (23), (24), (34)\}$$

$$c_3 = \{(123), (134), (132), (143), (234), (243), (242), (342)\}$$

$$c_4 = \{(1234), (1432), (1324), (1342), (1423), (1243)\}$$

$$c_{2,2} = \{(12)(34), (14)(23), (13)(24)\}$$

(c) As noted in part (b), the number of conjugacy classes in $S_5$ corresponds with the number of distinct cycle types, which are (1), (2), (3), (4), (5), (2)(2), (2)(3). Hence, there are 7 conjugacy classes in $S_5$.

63 Problem 7.6

(a) Since every element of $S_n$ can be written as a product of transpositions, it follows that $S_n$ is generated by the set of all transpositions. Hence, it suffices to show that every transposition is in the subgroup $S$ generated by $(1, 2), (1, 3), (1, 4), \ldots, (1, n)$. Every transposition of the form $(1, k)$ is clearly in $S$, so it remains to show that any transposition of the form $(i, j) \in S$ for $i \neq j$ and $i \neq j \neq 1$. We see that

$$(1, i)(1, j)(1, i) = (1, i)(1, i, j) = (i, j)$$

so the transposition $(i, j)$ is in the $S$, which completes the proof.
(b) We claim that \((1, j) \in H\) for all \(2 \leq j \leq n\), proceeding by induction. The case \(j = 2\) is clear, so suppose our hypothesis is true \(j > 2\); we want to show the hypothesis is true for the case \(j + 1\). Note that \((1, j) \in H\) by hypothesis, so

\[(1, j)(j, j + 1)(1j) = (1, j + 1) \in H\]

This completes the induction. Hence, by (a), \(H = S_n\).

(c) Let \(K\) be the subgroup of \(S_n\) generated by the cycles \((1, 2)\) and \((1, 2, \ldots, n)\). We want to show \(K = S_n\). By (b), it suffices to show that \((i, i + 1) \in K\) for each \(i \in \{1, \ldots, n - 1\}\). We claim that for all \(k \in \{0, \ldots, n - 2\}\),

\[(1, 2, \ldots, n)^k(1, 2)(1, 2, \ldots, n)^{-k} = (k + 1, k + 2)\]

We proceed by induction. The base case is clear, as

\[(1, 2, \ldots, n)^0(1, 2)(1, 2, \ldots, n)^{-0} = e(1, 2)e = (1, 2) = (0 + 1, 0 + 2)\]

Suppose the claim is true for \(k > 0\); we want to show the hypothesis is true for the case \(k + 1\). By the induction hypothesis, we see

\[(1, 2, \ldots, n)^{k+1}(1, 2)(1, 2, \ldots, n)^{-(k+1)} = (1, 2, \ldots, n)^1(k+1, k+2)(1, 2, \ldots, n)^{-1} = (k+2, k+3)\]

which completes the induction. Hence, \(K = S_n\), as desired.

64 Problem 7.7

For \(S_n, n \geq 3\), see problem 6.8. Let \(n \geq 4\). We claim \(A_n\) has trivial center. Let \(\sigma \neq e \in A_n\). Let \(i \in \{1, \ldots, n\}\) such that \(\sigma(i) = j \neq i\) for some \(j \in \{1, \ldots, n\}\). Put \(l = \sigma^{-1}(i) \in \{1, \ldots, n\}\), and let \(k \in \{1, \ldots, n\}\) such that \(k \neq l, i, j\); this is possible since \(n \geq 4\). Since \(\sigma\) is a bijection, \(\sigma(k) \neq i\) since \(k \neq l\). Put \(\gamma = (i, k, j) \in A_n\). Then

\[\gamma(\sigma(i)) = \gamma(j) = i\]

but

\[\sigma(\gamma(i)) = \sigma(k) \neq i\]

since \(k \neq l\). Since \((\sigma \circ \gamma)(i) \neq (\gamma \circ \sigma)(i)\), it follows \(\gamma \sigma \neq \sigma \gamma\). Hence, no nontrivial element of \(A_n\) commutes with every element of \(A_n\), so \(Z(A_n) = \{e\}\).

65 Problem 7.8

Let \(f \in \text{Aut}(S_3)\). By problem 7.6(c), \((12), (123)\) generated \(S_3\), so every automorphism of \(S_3\) is determined by the images of \((12), (123)\). Since automorphisms preserve order, it follows that \(f((123))\) is a 3-cycle and \(f((12))\) is a 2-cycle. Since there are two 3-cycles in \(S_3\) and three 2-cycles in \(S_3\), it follows that \(|\text{Aut}(S_3)| \leq 6\). By problem 7.7, \(Z(S_3) = \{e\}\), so \(S_3/Z(S_3) \cong \text{Inn}(S_3) \cong S_3\). Hence, \(|\text{Inn}(S_3)| = 6\), and since \(\text{Inn}(S_3) \subseteq \text{Aut}(S_3)\), we have \(\text{Aut}(S_3) = \text{Inn}(S_3) \cong S_3\).
66 Problem 7.9

Let \( N = \{e, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\} \subset S_4 \). Note that the subset \( N' \) of nonidentity elements of \( N \) consists of all products of disjoint transpositions of \( S_4 \), and hence contains all elements with cycle type \( (2, 2) \). Hence, \( \sigma N' \sigma^{-1} \subset N' \) for all \( \sigma \in S_4 \), so \( S_4 \) acts by conjugation on \( N' \). Consider the homomorphism \( \varphi: S_4 \to S(N') \) induced by this action; since \( |N'| = 3 \), note \( S(N') \cong S_3 \). Let \( \tau \in \ker(\varphi) \). We have

\[
\begin{align*}
\tau(1, 2)(3, 4)\tau^{-1} &= \tau(1, 2)\tau^{-1}\tau(3, 4)\tau^{-1} = (\tau(1), \tau(2))(\tau(3), \tau(4)) = (1, 2)(3, 4) \\
\tau(1, 3)(2, 4)\tau^{-1} &= (\tau(1), \tau(3))(\tau(2), \tau(4)) = (1, 3)(2, 4) \\
\tau(1, 4)(2, 3)\tau^{-1} &= (\tau(1), \tau(4))(\tau(2), \tau(3)) = (1, 4)(2, 3)
\end{align*}
\]

Hence, we can classify what \( \tau \) can (and in fact must) be based on the value of \( \tau(1) \). Suppose \( \tau(1) = 1 \). Then \( \tau(2) = 2 \), \( \tau(3) = 3 \), and \( \tau(4) = 4 \), so \( \tau = e \). Suppose \( \tau(1) = 2 \). Then \( \tau(2) = 1 \), \( \tau(3) = 4 \), \( \tau(4) = 3 \), so \( \tau = (1, 2)(3, 4) \). Suppose \( \tau(1) = 3 \). Then \( \tau(2) = 4 \), \( \tau(3) = 1 \) and \( \tau(4) = 2 \), so \( \tau = (1, 3)(2, 4) \). Finally, suppose \( \tau(1) = 4 \). Then \( \tau(2) = 3 \), \( \tau(3) = 2 \) and \( \tau(4) = 1 \), so \( \tau = (1, 4)(2, 3) \).

This shows simultaneously that \( \ker(\varphi) \subseteq N \) and \( N \subseteq \ker(\varphi) \), so we have \( N = \ker(\varphi) \). By the first isomorphism theorem, we then have

\[
S_4/N \cong S(N') = S_3
\]

67 Problem 7.10

Let \( \pi: S_4 \to S_4/N \) be the canonical quotient map. In problem 9, we proved that \( S_4/N \cong S_3 \). Note that there are several isomorphic copies of \( S_3 \) inside of \( S_4 \). Indeed, it is not hard to prove that for each \( i \in \{1, 2, 3, 4\} \), the subgroup of permutations in \( S_4 \) which fix \( i \) is isomorphic to \( S_3 \). Then in particular, there is an embedding of \( S_3 \) into \( S_4 \) which maps \( S_3 \) onto one of these isomorphic subgroups. The idea in building a homomorphism \( \varphi: S_4/N \to S_4 \) such that \( \pi \circ \varphi = \text{Id}_{S_4/N} \) is to consider the composition \( S_4/N \xrightarrow{\sim} S_3 \xhookrightarrow{} S_4 \), where the first arrow is the isomorphism from Problem 7.9 and the second arrow is one such embedding of \( S_3 \) into \( S_4 \). Of course, we still need to prove that this satisfies the desired composition rule. We will do so constructively, and in the process offer another solution to Problem 7.9. Consider the elements \( e, (12), (13), (23), (123), (132) \in S_4 \). We claim that

\[
\]

Since \( S_4/N \) is a group of order 6, it suffices to show each of these cosets is distinct. This is a straightforward but tedious exercise, and I omit it here.

Now we can write down the obvious map. Let \( \varphi: S_4 \) be defined explicitly by

\[
\begin{align*}
eN &\mapsto e & (12)N &\mapsto (12) & (23)N &\mapsto (23) \\
(13)N &\mapsto (13) & (123)N &\mapsto (123) & (132)N &\mapsto (132)
\end{align*}
\]
There is no issue of well-definedness, since \( \varphi \) is not defined using coset representatives. Furthermore, \( \varphi \) is a homomorphism by construction; indeed, the group law in \( S_4/N \) is defined on cosets by \( gNhN = ghN \). (For example, \( \varphi(\langle 12 \rangle N \langle 23 \rangle N) = \varphi(\langle 12 \rangle \langle 23 \rangle N) = \varphi(\langle 123 \rangle N) = (123) = (12) \langle 23 \rangle = \varphi(\langle 12 \rangle N) \varphi(\langle 23 \rangle N) \); one can check the other cases similarly.) Finally, it is obvious that \( \pi \circ \varphi = \text{Id}_{S_4/N} \) by construction, so we’re done.

68 Problem 8.1

Let \( G \) act on a set \( X \), and suppose \( x, y \in X \) satisfy \( ax = y \) for some \( a \in G \). Suppose \( g \in G_x \). Then

\[
(aga^{-1})y = ag(a^{-1}y) = agx = ax = y
\]

so \( aga^{-1} \in G_y \), whence \( aG_xa^{-1} \subseteq G_y \). Likewise, suppose \( g \in G_y \). Then

\[
(a^{-1}ga)x = ag(ax) = agy = a^{-1}y = x
\]

so \( a^{-1}ga \in G_x \), whence \( a^{-1}G_ya \subseteq G_x \), i.e. \( G_y \subseteq aG_xa^{-1} \). Hence, \( G_y = aG_xa^{-1} \).

69 Problem 8.2

Let \( G \) be a group, \( a \in G \). Denote the conjugacy class \( \{bab^{-1}, b \in G \} \) by \( C(a) \). Let \( G \) act on itself by conjugation; then \( C(a) \) is the orbit of \( a \) under the action of \( G \). By the orbit stabilizer theorem, \( |C(a)| = [G : G_a] \), and hence must be a divisor of \( G \).

70 Problem 8.3

Suppose \( G \) acts on \( X \) doubly transitively, and let \( \Delta X := \{(x, x) \mid x \in X \} \subset X \times X \). There is an action of \( G \) on \( X \times X \) given by \( g \cdot (x, y) = (gx, gy) \). If \( |X| = 1 \), then the conclusion is trivial, so we may assume \( |X| > 1 \). Let \( x_1, x_2 \in X \) be distinct elements. Since \( G \) acts doubly transitively on \( X \), for any \( y_1 \neq y_2 \) in \( X \), there is an \( a \in G \) such that \( ax_1 = y_1, ax_2 = y_2 \), i.e. \( a(x_1, x_2) = (y_1, y_2) \). In other words, the orbit of \( (x_1, x_2) \) under the action of \( G \) contains \( (X \times X) \setminus \Delta X \). Since \( |\Delta X| = |X| \), this means \( |\text{orb}((x_1, x_2))| \geq |(X \times X) \setminus \Delta X| = |X|^2 - |X| \). We thus obtain the inequality

\[
|G| = |G_{(x_1, x_2)}|[G : G_{(x_1, x_2)}] \geq [G : G_{(x_1, x_2)}] = |\text{orb}((x_1, x_2))| \geq |X|^2 - |X|
\]

where the middle equality follows from Orbit-Stabilizer.

71 Problem 8.4

(a) Let \( H \subset G \) be a subgroup, and let \( \Omega \) be the set of conjugate subgroups of \( H \) in \( G \). Note that \( G \) acts on \( \Omega \) by conjugation, and in particular, this action is transitive: \( \Omega = \text{orb}(H) \). By Orbit-Stabilizer, \( |\text{orb}(H)| = [G : G_H] \), where \( G_H \) is the stabilizer subgroup of \( H \)
under this action of \( G \). Clearly, \( G_H \) contains \( H \), so \([G : H] = [G : G_H][G_H : H]\) by Problem 5.3, whence

\[
|\Omega| = |\text{orb}(H)| = [G : G_H] \leq [G : G_H][G_H : H] = [G : H]
\]

(b) Suppose \( G \) is the union of conjugates of a subgroup \( H \subset G \). Let \( \Omega \) be the set of conjugate subgroups of \( H \) in \( G \). Each element of \( \Omega \) has order \(|H|\), and the intersection of any two elements of \( \Omega \) contains the identity; since \(|\Omega| \leq [G : H]\), we obtain the inequalities:

\[
|G| = |\bigcup_{K \in \Omega} K| \leq 1 + (|H| - 1) \cdot [G : H] = 1 + |H|[G : H] - [G : H] = |G| + 1 - [G : H]
\]

Hence, the only way this inequality can hold is if \([G : H] = 1\), in which case \( H = G \).

(c) Suppose \( G \) acts transitively on a set of \( X \) which has at least two elements. For any \( x \in X \), the stabilizer \( G_x \) of \( x \) is not equal to \( G \), since \( G \) acts transitively on \( X \), and so \( x \) cannot belong to its own orbit if \(|X| \geq 2\). Furthermore, since \( G \) acts transitively on \( X \), Problem 8.1 implies \( G_x, G_y \) are conjugate for every \( x, y \in G \). Hence, \( \bigcup_{x \in X} G_x \neq G \) by part (b), whence there exists some \( g \in G \) which belongs to no stabilizer, i.e. \( g \) does not fix any element of \( X \).

72 Problem 8.5

We begin by factoring \(|A_5| = 60 = 2^2 \cdot 3 \cdot 5\). By the Sylow theorems, the number \( N_5 \) of Sylow 5-subgroups divides 12 and is congruent to 1 mod 5; since \( A_5 \) is simple, it follows that \( N_5 = 6 \). Each Sylow 5-subgroup is cyclic, generated by one of the 24 distinct 5 cycles in \( A_5 \). Likewise, the number \( N_3 \) of Sylow 3-subgroups divides 20 and is congruent to 1 mod 3; again, since \( A_5 \) is simple, it follows that \( N_3 = 4 \) or \( N_3 = 10 \). Each Sylow 3-subgroup is cyclic, generated by one of the 3-cycles in \( A_5 \). If \( N_3 = 4 \), then \( A_5 \) would only have \( 4 \cdot (3 - 1) = 8 \) elements of order 3; since one can clearly list more than 8 3-cycles, we must have \( N_3 = 10 \), i.e. there are 20 distinct 3-cycles in \( A_5 \).

The above work implies that \( A_5 \) has 24 elements of order 5, and 20 elements of order 3, leaving 15 nonidentity elements of \( A_5 \) unaccounted for. The number \( N_2 \) of Sylow 2-subgroups divides 15 and is congruent to 1 mod 2; since \( A_5 \) is simple, it follows that \( N_2 = 3, 5 \) or 15. The intersection of any two distinct Sylow 2-subgroups has order at most 2, so each subgroup contributes at least 2 distinct elements. We can thus rule out the case \( N_2 = 15 \), since this would produce at least \( 15 \cdot 2 = 30 \) distinct elements, exceeding the order of \( A_5 \). Similarly, we can rule out the case of \( N_2 = 3 \), since each Sylow 2-subgroup contributes at most 3 distinct nonidentity elements, and \( 3 \cdot 3 = 9 \) falls short of the 15 unaccounted for nonidentity elements.

Hence, we conclude \( N_2 = 5 \). Since every 4-cycle is odd, each Sylow 2-subgroup must be isomorphic to the Klein 4-group. One such example is \( V_4 = \{e, (12)(34), (13)(24), (14)(23)\} \subset A_5 \). One can easily compute the other four Sylow 2-subgroups by conjugating \( V_4 \) by different elements of \( A_5 \), or writing down the other possible double transpositions into the appropriate groupings.
73  Problem 8.6

Since the highest power of \( p \) dividing \( p! \) is \( p \), every Sylow \( p \)-subgroup of \( S_p \) is of order \( p \), hence cyclic generated by some element of order \( p \). Furthermore, every element of order \( p \) in \( S_p \) must be a \( p \)-cycle, since the order of any element of a symmetric group is the least common multiple of the cycle lengths in its disjoint cycle decomposition. Note that a \( p \)-cycle \( \sigma \) generates the same subgroup of \( S_p \) as a \( p \)-cycle \( \tau \) if and only if (WLOG) \( \tau \) is a (nontrivial) power of \( \sigma \). Hence, to count the number of subgroups of order \( p \) in \( S_p \), it suffices to count the number of \( p \)-cycles and divide by \( p - 1 \), the number of nontrivial powers of each \( p \)-cycle.

We prove the following more general counting result.

Let \( \Omega \) be the set of \( n \)-cycles in \( S_n \). Any element \( \alpha \in \Omega \) can be cyclically permuted so that \( 1 \) is the first element of the cycle, so let \( \alpha \) be the \( n \)-cycle \( (1, k_2, k_3, \ldots, k_n) \). Since \( \alpha \) is an \( n \)-cycle, \( \{k_2, k_3, \ldots, k_n\} = \{2, 3, \ldots, n\} \), so we can define a map \( \phi : \Omega \to S_{n-1} \) by

\[
(1, k_2, k_3, \ldots, k_n) \mapsto \beta
\]

where \( \beta \) is the element of \( S_{n-1} \) such that \( \beta(i) = k_i \). This map is clearly a bijection, whence

\[
|\Omega| = |S_{n-1}| = (n - 1)!
\]

Hence, there are \((p - 1)!/(p - 1) = (p - 2)!\) Sylow \( p \)-subgroups of \( S_p \).

74  Problem 8.7

Let \( H \) be a subgroup of a finite group \( G \) with \( H \neq G \), and suppose that \(|G|\) does not divide \([G : H]!\). Let \( G \) act on the set \( X \) of left cosets \( G/H \) by left translation. This action induces a homomorphism \( \varphi : G \to S(X) \); note that \(|S(X)| = [G : H]!\). Note that if \( g \in \ker(\varphi) \), then \( g \) must fix every element of \( X \) under left translation. In particular, we must have \( gH = H \), so \( g \in H \), i.e. \( \ker(\varphi) \subseteq H \). Suppose \( \ker(\varphi) = \{e\} \); then \( G \cong \text{Im}(G) \subset S(X) \) by the first isomorphism theorem. But \( \text{Im}(G) \) is a subgroup of \( S(X) \), and so \(|\text{Im}(G)| = |G|\) must divide \(|S(X)| = [G : H]!\) by Lagrange’s theorem, a contradiction. Hence, \( N = \ker(\varphi) \) is a proper nontrivial normal subgroup of \( G \) such that \( N \) is a subgroup of \( H \), as desired.

75  Problem 8.8

Let \( G \) be a finite group of order \( 2p^n \) for some prime \( p \) and \( n \geq 1 \). Then by the 1st Sylow theorem, \( G \) has a subgroup \( P \) of order \( p^n \), whence \([G : P] = 2\), so \( P \leq G \). Since \( P \neq \{e\} \) and \( P \neq G \), it follows that \( G \) is not simple.

Let \( G \) be a finite group order \( 3p^n \) for some prime \( p \) and \( n \geq 1 \). By the 1st Sylow theorem, \( G \) has a subgroup \( P \) of order \( p^n \), so \([G : P]! = 3! = 6\). Note that \(|G|\) does not divide 6 unless \( n = 1 \) and \( p = 2 \), so by Problem 8.7, \( G \) is not simple if this is not the case. If \( n = 1 \) and \( p = 2 \), then \(|G| = 6\), and the Sylow-3 subgroup of \( G \) is of index 2, hence normal, so \( G \) is not simple.
76 Problem 8.9

(a) Let \( G \) be a group, and let \( H \) be a subgroup in the center \( Z(G) \) of \( G \). Note that for any \( g \in G \), \( gh = hg \) for all \( h \in N \), i.e. \( ghg^{-1} = h \) for all \( g \in G \), \( h \in N \). Hence, \( gHg^{-1} = H \) for each \( g \in G \), so \( H \) is normal in \( G \).

Suppose \( G/H \) is cyclic. Then \( G/H = \langle xH \rangle \) for some \( x \in G \), i.e. \( g = x^kh_g \) for some \( k \in \mathbb{N}, h_g \in H \) for each \( g \in G \). Let \( g_1, g_2 \in G \). Write \( g_1 = x^{k_1}h_{g_1}, g_2 = x^{k_2}h_{g_2} \) for some \( k_1, k_2 \in \mathbb{N}, h_{g_1}, h_{g_2} \in H \). Then since \( h_{g_1}, h_{g_2} \in Z(G) \),

\[
g_1g_2 = x^{k_1}h_{g_1}x^{k_2}h_{g_2} = x^{k_1}x^{k_2}h_{g_1}h_{g_2} = x^{k_2}x^{k_1}h_{g_2}h_{g_1} = x^{k_2}h_{g_2}x^{k_1}h_{g_1} = g_2g_1
\]

i.e. \( G \) is abelian.

(b) Let \( G \) be a group of order \( p^2 \). By Lagrange, since \( Z(G) \) is a subgroup of \( G \), \( |Z(G)| \) divides \( |G| \), so we must have \( |Z(G)| = 1, |Z(G)| = p \) or \( |Z(G)| = p^2 \). By the class equation, we have

\[
|G| = |Z(G)| + \sum_{i=1}^{n} |G : C_g(x_i)|
\]

where \( x_1, \ldots, x_n \) are representatives of the distinct non-central conjugacy classes. Since \( x_i \notin Z(G) \) for each \( i \), \( [G : C_g(x_i)] > 1 \), so \( p \mid [G : C_g(x_i)] \) for each \( i \). Since \( p \mid |G| \), we must have \( p \mid |Z(G)| \), so \( |Z(G)| = 1 \).

If \( |Z(G)| = p \), then \( |G/Z(G)| = |G|/|Z(G)| = p \), whence \( G/Z(G) \) must be cyclic. By part (a), this implies \( G \) is abelian, a contradiction (since \( G \) is abelian if and only if \( G = Z(G) \)).

If \( |Z(G)| = p^2 \), then \( Z(G) = G \), so \( G \) is abelian.

77 Problem 8.10

Note that the claim is trivial for the cases \( n = 1,2,3 \), as the only subgroup of index \( n \) in \( A_n \) is \( \{e\} \) for \( n = 1,2,3 \). The claim is true for \( n = 4 \), as any subgroup of index 4 in \( A_4 \) has order 3, and hence is isomorphic to \( A_3 \), since all groups of order 3 are cyclic. Hence, it suffices to take \( n \geq 5 \). Let \( H \) be a subgroup of \( A_n \) of index \( n \), and consider the homomorphism \( \varphi: A_n \rightarrow S(X) \) given by the left action of \( A_n \) on the set \( X = A_n/H \) of cosets of \( H \) in \( A_n \). Suppose \( g \in \ker(\varphi) \). Then we must have \( \varphi(g)(H) = gH = H \), i.e. \( g \in H \), so \( \ker(\varphi) \subseteq H \neq A_n \). Since \( A_n \) is simple for \( n \geq 5 \), it follows that \( \ker(\varphi) \) is trivial, whence \( \varphi \) is injective. Hence, \( \varphi(A_n) \) is a subgroup of \( S(X) \cong S_n \) of index 2, and hence must be isomorphic to \( A_n \). Restricting \( \varphi \) to \( H \), it follows that \( H \) is isomorphic to its image under \( \varphi \). Note that \( \varphi(g)(H) = gH = H \) if and only if \( g \in H \), so \( \varphi(H) \) is precisely the set of elements of \( A_n \subset S(X) \) which fix the element \( H \in X \). The subgroup of elements of \( A_n \) which fix a particular element is isomorphic to \( A_{n-1} \), so \( H \cong \varphi(H) \cong A_{n-1} \).
Let $H \subset G = \mathbb{Z} \times \mathbb{Z}$ be the cyclic subgroup generated by the element $(2, 4)$. As suggested by the hint, the factor group $G/H$ is not isomorphic to $\mathbb{Z}$. Indeed, the only torsion element of $\mathbb{Z}$ is 0, whereas $(1, 2)$ is a nontrivial torsion element of $G/H$. Since the image of any torsion element under a homomorphism is also torsion, this means any map $G/H \to \mathbb{Z}$ must send $(1, 2)$ to 0, and hence has nontrivial kernel.

As always, $\{e\}$ and $A_4$ are trivially subgroups of $A_4$. Note that $A_4 = \{e, (12)(34), (13)(24), (14)(23), (123), (132), (124), (142), (134), (143), (234), (243)\}$

Each element of order 2, i.e. the products of disjoint transpositions, generates a unique cyclic subgroup of $A_4$ of order 2. The 3-cycles generate 4 unique cyclic subgroups of order 3, namely $\langle (123) \rangle$, $\langle (124) \rangle$, $\langle (134) \rangle$, and $\langle (234) \rangle$. Finally, a small number of multiplications shows that the set of all products of disjoint transpositions, $V = \{e, (12)(34), (13)(24), (14)(23)\}$ form a subgroup of $A_4$ of order 4 (in fact, since conjugation preserves cycle type, $V$ is in fact a normal subgroup of $A_4$). We can think of $V$ as the subgroup of $A_4$ generated by any two distinct double transpositions. We claim that these are the only proper subgroups of $A_4$, and in particular that $A_4$ has no subgroup of order 6.

For this, it suffices to show that any subgroup of $A_4$ containing a double transposition and a 3-cycle must be all of $A_4$. We appeal to Lagrange’s theorem here: any subgroup of $A_4$ must have order dividing $|A_4| = 12$, so if a 3-cycle and a double transposition generate more than 6 elements, any subgroup which contains both must be all of $A_4$. Now, we compute:

$$(123)((12)(34)) = (134)$$
$$(134)((12)(34)) = (124)$$
$$(124)((12)(34)) = (143)$$
$$(143)((12)(34)) = (124)$$
$$(142)((12)(34)) = (243)$$
$$(234)((12)(34)) = (132)$$
$$(132)((12)(34)) = (234)$$
$$(243)((12)(34)) = (134)$$

Hence, the above computations show that if any subgroup of $A_4$ contains any 3-cycle and $(12)(34)$, then it contains all eight 3-cycles, and thus must be all of $A_4$. We make similar computations below:

$$(123)((13)(24)) = (243)$$
$$(134)((13)(24)) = (142)$$
Therefore, if any subgroup of $A_4$ contains any 3-cycle and $(13)(24)$, then it contains all eight 3-cycles, and thus must be all of $A_4$. Finally, we see

$$
(123)((14)(23)) = (142)
$$
$$
(134)((14)(23)) = (243)
$$
$$
(124)((14)(23)) = (234)
$$
$$
(143)((14)(23)) = (132)
$$
$$
(142)((14)(23)) = (123)
$$
$$
(234)((14)(23)) = (124)
$$
$$
(132)((14)(23)) = (143)
$$
$$
(243)((14)(23)) = (134)
$$

Therefore, if any subgroup of $A_4$ contains any 3-cycle and $(14)(23)$, then it contains all eight 3-cycles, and thus must be all of $A_4$. This proves the claim that any subgroup which contains 3-cycle and any double transposition must be all of $A_4$. It remains to show that any subgroup of $A_4$ containing two 3-cycles which generate distinct cyclic subgroups must be all of $A_4$. To this end, we show that the subgroup generated by any two such 3-cycles contains a double transposition, proving the claim and completing the proof. It suffices to do this for the specified generators for each cyclic subgroup of order 3.

$$
(123)(124) = (13)(24)
$$
$$
(123)(134) = (234)
$$
$$
(123)(234) = (12)(34)
$$
$$
(134)(234) = (13)(24)
$$
$$
(124)(134) = (13)(24)
$$
$$
(124)(234) = (123)
$$

Hence, the subgroups of $A_4$ are

$$
\{ \{e\}, \langle (12)(34) \rangle, \langle (13)(24) \rangle, \langle (14)(23) \rangle, \langle (123) \rangle, \langle (124) \rangle, \langle (134) \rangle, \langle (234) \rangle, V, A_4 \} 
$$
80 Problem 9.3

(a) Let \( g \in S_n \) be an odd transformation, and consider the map \( f: A_n \to A_n \) given by \( f(x) = gxg^{-1} \). Note that \( f \) is a homomorphism, as for any \( x, y \in A_n \),

\[
f(xy) = gxyg^{-1} = gx(g^{-1}g)yg^{-1} = f(x)f(y)
\]

Further, \( \text{sgn}(g^{-1}xg) = \text{sgn}(g)^{-1} \text{sgn}(x) \text{sgn}(g) = \text{sgn}(x) \) for any \( x \in A_n \), so \( gxg^{-1} \in A_n \) for all \( x \in A_n \). Let \( x \in A_n \); then \( f(g^{-1}xg) = gg^{-1}xgg^{-1} = x \), so \( f \) is surjective. Since \( A_n \) is finite, \( f \) is also injective, whence \( f \) is an automorphism.

(b) Let \( n \geq 4 \), and suppose \( f \) is an inner automorphism, seeking a contradiction. Then \( f(x) = yxy^{-1} \) for some \( y \in A_n \) for all \( x \in A_n \), so in particular, \( gxg^{-1} = yxy^{-1} \) for all \( x \in A_n \). Equivalently, \( y^{-1}gx = xy^{-1}g \) for all \( x \in A_n \), i.e. \( y^{-1}g \) is in the centralizer of \( A_n \) in \( S_n \). With trivial modifications to Problem 7.7, we see that the centralizer of \( A_n \) in \( S_n \) is trivial since \( \gamma \) is chosen to be in \( A_n \) and \( \sigma \) can be chosen to be any nonidentity element of \( S_n \). Hence, \( y^{-1}g = e \), i.e. \( y = g \), a contradiction as \( g \notin A_n \) by hypothesis.

Suppose \( n = 3 \). Then \( A_3 \) is cyclic, so \( \text{Inn}(A_3) \) is trivial. It suffices then to show that \( f: A_3 \to A_3 \) given by \( f(x) = gxg^{-1} \) is a nontrivial automorphism for any transposition \( g \in S_3 \). This is clear, as

\[
\]

\[
\]

\[
(23)(123)(23)^{-1} = (23)(123)(23) = (23)(12) = (132)
\]

81 Problem 9.4

Let \( x_1, \ldots, x_n \in \mathbb{Q}/\mathbb{Z} \). Every \( x_i \) is of the form \( p_i/q_i + \mathbb{Z} \) for some \( p_i, q_i \in \mathbb{Z} \); put \( q = \prod_{i=1}^{n} q_i \). Then \( p_i/q_i + \mathbb{Z} \) belongs to \( \langle 1/q + \mathbb{Z} \rangle \) for each \( i \), whence \( \langle x_1, \ldots, x_n \rangle \subseteq \langle 1/q + \mathbb{Z} \rangle \). But \( \langle 1/q + \mathbb{Z} \rangle \) is a finite cyclic subgroup of \( \mathbb{Q}/\mathbb{Z} \) of order \(|q|\), and hence cannot be all of \( \mathbb{Q}/\mathbb{Z} \), which is infinite (consider the distinct cosets \( 1/n + \mathbb{Z}, n \in \mathbb{N} \)).

82 Problem 9.5

(a) Certainly, \( 0 \in G_{\text{tors}} \). If \( x_1, x_2 \in G_{\text{tors}} \), then there exist \( n_1, n_2 \in \mathbb{N} \) such that \( n_1x_1 = n_2x_2 = 0 \), then certainly \( n_1n_2(x_1 - x_2) = n_2(n_1x_1) - n_1(n_2x_2) = 0 - 0 = 0 \), so \( x_1 - x_2 \in G_{\text{tors}} \), whence \( G_{\text{tors}} \) is a subgroup of \( G \) by the subgroup test.

(b) We determined that this was \( \mathbb{Q}/\mathbb{Z} \) in Problem 6.4.

(c) Any element of \( \mathbb{Q}^\times \) of finite order \( n \) is a (primitive) root of \( X^n - 1 \) over \( \mathbb{C} \). By the rational root theorem, the only roots of \( X^n - 1 \) over \( \mathbb{Q} \) are 1 and (for some \( n \)) \(-1\). Hence, \( \mathbb{Q}^\times_{\text{tors}} = \{-1, 1\} \).
Let $K$ be a normal subgroup of $S_n$ for $n \geq 5$. We claim $K$ must be $\{e\}$, $A_n$, or $S_n$. Since $K \trianglelefteq S_n$, $K \cap A_n$ is a normal subgroup of $A_n$. By the simplicity of $A_n$ for $n \geq 5$, either $K \cap A_n = 1$ or $K \cap A_n = A_n$. In the latter case, $A_n \subseteq K$, and since $[S_n : A_n] = 2$, this implies $K = A_n$ or $K = S_n$. Suppose $K \cap A_n = 1$. Then if $K$ has at least two distinct nonidentity elements $\sigma, \tau$ which are both odd, either $\sigma^2 \neq e$ or $\sigma \tau \neq e$, both of which are even, a contradiction. Hence, $|K| \leq 2$. But $K \subseteq A_n$; since conjugation always fixes the identity, this means $K \subseteq Z(S_n)$. Since we proved $Z(S_n) = \{e\}$ for $n \geq 3$ in Problem 6.8, we must have $K = \{e\}$.

The possible elements of $S_4$ are $k$-cycles for $1 \leq k \leq 4$, and products of disjoint transpositions. Hence, the possible cycle types are $(1)$, $(2)$, $(3)$, $(4)$, and $(2, 2)$. This gives 5 conjugacy classes, which we enumerate explicitly below:

- $c_1 = \{e\}$
- $c_2 = \{(12), (13), (14), (23), (24), (34)\}$
- $c_3 = \{(123), (134), (132), (143), (234), (243), (124), (142)\}$
- $c_4 = \{(1234), (1432), (1342), (1423), (1243)\}$
- $c_{2,2} = \{(12)(34), (14)(23), (13)(24)\}$

Certainly, conjugacy classes in $A_4$ can only shrink from their counterparts in $S_4$. One can verify by computation* that the conjugacy classes $\{e\}, \{(12)(34), (14)(23), (13)(24)\}$ remain intact, whereas the conjugacy class $\{(123), (134), (132), (143), (234), (243), (124), (142)\}$ splits into the two classes $\{(123), (243), (134), (142)\}$ and $\{(132), (234), (143), (124)\}$.

*: Here are some helpful computations. Let $G = A_4$. Orbit stabilizer says that $|\text{orb}(123)| = [G : G_{(123)}]$, where $G_{(123)}$ is the centralizer of $(123)$ in $G$. Certainly, $G_{(123)}$ contains $\langle (123) \rangle$, so $|\text{orb}((123))| \leq 12/3 = 4$. One can verify that

\[
(124)(123)(124)^{-1} = (124)(123)(142) = (243)
\]
\[
(143)(123)(143)^{-1} = (143)(123)(134) = (142)
\]
\[
(234)(123)(234)^{-1} = (234)(123)(243) = (134)
\]

This shows that $G_{(123)} = G_{(132)}$ has exactly three elements, so $\text{orb}(132)$ also has four elements, namely the other four elements of the conjugacy class $c_3$ above.
85 Problem 9.8

(a) By Problem 6.1, it suffices to show that the conjugate of any commutator \([x, y] = x^{-1}y^{-1}xy\) is another commutator. Let \(g \in G\), and note that \((gxg^{-1})^{-1} = (xg^{-1})^{-1}g^{-1} = (g^{-1})^{-1}x^{-1}g^{-1} = gx^{-1}g^{-1}\) for any \(x \in G\). Then

\[g[x, y]g^{-1} = gx^{-1}(g^{-1}g)y^{-1}(g^{-1})x(g^{-1})yg^{-1} = (gx^{-1}g^{-1})(gy^{-1}g^{-1})(gxg^{-1})(gyg^{-1}) = [gxg^{-1}, gyg^{-1}]\]

which establishes the claim.

(b) Let \(H\) be the commutator subgroup of \(G\), and consider the quotient \(G/H\). For any \(x, y \in G\), we have \(x^{-1}y^{-1}xy \in H\), so \(x^{-1}y^{-1}xyH = H\), i.e. \(xHyH = xyH = yxH = yHxH\) for all \(x, y \in G\).

(c) Suppose \(N\) is a normal subgroup of \(G\) such that \(G/N\) is abelian. Then for any \(x, y \in G\), \(xNyN = (xy)N = (yx)N = yNxN\), so \(x^{-1}y^{-1}xyN = N\), i.e. \(x^{-1}y^{-1}xy \in N\). Hence, every commutator belongs to \(N\), whence the commutator subgroup is a subset of \(N\).

86 Problem 9.9

Let \(G_n = [A_n, A_n]\) for each \(n\); by Problem 9.8 parts (a), (b), \(G_n\) is a normal subgroup of \(A_n\), and \(A_n/G_n\) is abelian. For \(n = 1, 2\), \(A_n = \{e\}\), whence \(A_n = G_n\) and thus \(A_n\) is perfect. For \(n = 3\), \(A_n \cong \mathbb{Z}/3\mathbb{Z}\), and hence \(G_n = \{e\}\), so \(A_n\) is not perfect. For \(n \geq 5\), the simplicity of \(A_n\) implies \(G_n = \{e\}\) or \(G_n = A_n\). If we had \(G_n = \{e\}\), then \(A_n/G_n \cong A_n\) would be abelian, a contradiction, so we must have \(G_n = A_n\), whence \(A_n\) is perfect. For \(n = 4\), note that \(V_4 = \{e, (12)(34), (13)(24), (14)(23)\}\) is a normal subgroup of \(A_4\) with abelian quotient \(A_4/V_4 \cong \mathbb{Z}/3\mathbb{Z}\). By problem 9.8(c), \(G_4 \subseteq V_4\), which implies \(G_4 \neq A_4\), so \(A_4\) is not perfect. Hence, \(A_n\) is perfect for \(n \neq 3, 4\).

87 Problem 9.10

Let \(N\) be a normal subgroup of \(G\) and let \(K\) be a subgroup of \(G\) such that the restriction of the canonical homomorphism \(G \rightarrow G/N\) to \(K\) is an isomorphism \(K \rightarrow G/N\). We have an exact sequence of groups

\[1 \rightarrow N \hookrightarrow G \xrightarrow{\pi} G/N \rightarrow 1\]

which is split by the composition \(G/N \rightarrow K \hookrightarrow G\). Hence, \(G\) is the semidirect product of \(N\) and \(G/N\), whence it is the semidirect product of \(N\) and \(K\) via the isomorphism \(K \cong G/N\).