Problem (Problem 1)**:** Let F be a field, and for $n \geqslant 1$, let $\mathrm{Mat}_n(F)$ be the set of $n \times n$ matrices with entries in F.

(a) Show that $GL_n(F) := \{x \in \mathrm{Mat}_n(F) \mid \det(x) \neq 0\}$ is a group under matrix multiplication.

(b) Show that $SL_n(F) := \{x \in \mathrm{Mat}_n(F) \mid \det(x) = 1\}$ is a normal subgroup of $GL_n(F)$, and identify the quotient $GL_n(F)/SL_n(F)$.

Solution:

(a) We see that if $a, b \in GL_n(F)$, then since $\det(a) \neq 0$, the properties of the determinant yield $0 \neq \det(a)^{-1} = \det\left(a^{-1}\right)$, meaning that $a^{-1} \in GL_n(F)$, and $0 \neq \det(a)\det(b) = \det(ab)$, meaning that $ab \in GL_n(F)$, since fields have no zero-divisors.

(b) If $a \in SL_n(F)$, then for any $x \in GL_n(F)$, we have

$$\begin{aligned}\det\left(xax^{-1}\right) &= \det(x)\det(a)\det\left(x^{-1}\right)\\ &= \det(x)\det(a)\det(x)^{-1}\\ &= \det(a)\\ &= 1,\end{aligned}$$

meaning that $xax^{-1} \in SL_n(F)$ for any $x \in GL_n(F)$. In particular, we note that the map

$$\det\colon\ GL_n(F) \to F \setminus \{0\},$$

given by $a \mapsto \det(a)$ is a group homomorphism, as has been established by the properties of the determinant, and it is surjective, as the matrix $\mathrm{diag}(a, 1_F, \dots, 1_F)$ has determinant a, for any $a \in F$. Finally, we see that $\det^{-1}(\{1_F\})$ is $SL_n(F)$, meaning that by the First Isomorphism Theorem, $GL_n(F)/SL_n(F) \cong F \setminus \{0\}$.

Problem (Problem 2)**:** Let G be a group, and let $H_1, H_2 \leqslant G$ be subgroups. Show that if $H_1 \cup H_2$ is a subgroup, then either $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$.

Solution: Suppose toward contradiction that there were some $x \in H_1 \setminus H_2$ and $y \in H_2 \setminus H_1$. Since $xy \in H_1 \cup H_2$, it follows that $xy \in H_1$ or $xy \in H_2$. If $xy \in H_1$, then so too is $x^{-1}xy$, meaning $y \in H_1$, which is a contradiction. Similarly, if $xy \in H_2$, then so too is xyy^{-1}, implying $x \in H_2$, again a contradiction. Thus, either $H_1 \setminus H_2$ or $H_2 \setminus H_1$ is empty, so that $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$.

Problem (Problem 3)**:** Let G be a group, and let $H_1, H_2 \leqslant G$ be subgroups.

(a) Show that if H_1 and H_2 are finite, with $\gcd(|H_1|, |H_2|) = 1$, then $H_1 \cap H_2 = \{e\}$.

(b) Show that if both H_1 and H_2 are normal subgroups, and $H_1 \cap H_2 = \{e\}$, then $h_1h_2 = h_2h_1$ for all $h_1 \in H_1$ and $h_2 \in H_2$.

Solution:

(a) Let $g \in H_1 \cap H_2$. Then, we see that $\mathrm{ord}(g) \mid |H_1|$ and $\mathrm{ord}(g) \mid |H_2|$, so $\mathrm{ord}(g) \mid \gcd(|H_1|, |H_2|)$; yet, since $\gcd(|H_1|, |H_2|) = 1$, this means that $\mathrm{ord}(g) = 1$, meaning $g = \{e\}$.

(b) If H_1 and H_2 are normal subgroups, then for $h_1 \in H_1$ and $h_2 \in H_2$, we consider the commutator $c = h_1h_2h_1^{-1}h_2^{-1}$. Notice that by grouping as $\left(h_1h_2h_1^{-1}\right)h_2^{-1}$, since H_2 is a normal subgroup, $c \in H_2$. Similarly, by grouping as $h_1\left(h_2h_1^{-1}h_2^{-1}\right)$, since H_1 is normal, we see that $c \in H_1$. Since $H_1 \cap H_2 = \{e\}$, we see that $h_1h_2h_1^{-1}h_2^{-1} = e$, so $h_1h_2 = h_2h_1$.

Problem (Problem 4)**:** Let $g \in G$ be an element with $\mathrm{ord}(g) = n < \infty$.

(a) Show that if $g^m = e$, then $n \mid m$.

(b) If $d \mid n$, then $\mathrm{ord}\left(g^d\right) = n/d$.

(c) Show that for any integer $m \neq 0$, $\langle g^m \rangle = \left\langle g^{\gcd(m,n)} \right\rangle$.

(d) Use (b) and (c) to conclude that $\operatorname{ord}(g^m) = \frac{n}{\gcd(m,n)}$ for any $m \neq 0$.

Solution:

(a) We see that if $g^m = e$, then $g^m = (g^n)^k$, as $\operatorname{ord}(g) = n < \infty$, so that $g^m = g^{nk}$, and thus $n|m$.

(b) Let $d|n$. Then, $n = ad$ for some $a \in \mathbb{Z}$, so $e = g^n = \left(g^d\right)^a$, meaning $\operatorname{ord}\left(g^d\right) = a = n/d$.

(c) The inclusion $\langle g^m \rangle \subseteq \left\langle g^{\gcd(m,n)} \right\rangle$ immediately follows from the fact that $\gcd(m,n)|m$. For the reverse direction, we observe that by the Bezout identity, $\gcd(m,n) = am + bn$ for some $a, b \in \mathbb{Z}$, meaning that if $h \in \left\langle g^{\gcd(m,n)} \right\rangle$, then $h = g^{c \gcd(m,n)}$, so $h = g^{acm}$, so $h \in \langle g^m \rangle$.

(d) Since $\langle g^m \rangle = \left\langle g^{\gcd(m,n)} \right\rangle$, it follows that $\operatorname{ord}(g^m) = \operatorname{ord}\left(g^{\gcd(m,n)}\right)$, so $\operatorname{ord}(g^m) = n/\left(\gcd(m,n)\right)$.

Problem (Problem 5)**:** Let g and h be commuting elements of a group G having finite orders m and n. If m and n are relatively prime, then $\operatorname{ord}(gh) = mn$.

Solution: Let k be such that $(gh)^k = e$, meaning that $g^k h^k = e$, so that $g^k = h^{-k}$. In particular, this means that $h^{-k} \in \langle g \rangle$, implying that $h^k \in \langle g \rangle$, and similarly, $g^k \in \langle h \rangle$.

It follows that g^k and h^k are contained in $\langle g \rangle \cap \langle h \rangle$; yet, since m and n are coprime, we know from Problem 3 that $\langle g \rangle \cap \langle h \rangle = \{e\}$, so that $g^k = e = h^k$. Therefore, $m|k$ and $n|k$, meaning that $\operatorname{lcm}(m,n)|k$. Yet, since m and n are relatively prime, this means $mn|k$. Finally, since $g^{mn}h^{mn} = e$, it follows that $\operatorname{ord}(gh) = mn$.

Problem (Problem 6)**:** Let G be a finite group of even order. Then, G contains an element of order 2.

Solution: Suppose not. Then, for any $e \neq g \in G$, $g \neq g^{-1}$. By pairing off each non-identity g with its corresponding g^{-1}, we see that G can be partitioned as

$$G = \left\{\{e\}, \left\{g_1, g_1^{-1}\right\}, \dots, \left\{g_k, g_k^{-1}\right\}\right\},$$

since G is finite. Yet, this means that G is of odd order, which is a contradiction.

Problem (Problem 7)**:** Let $G = \{g_1, \dots, g_n\}$ be a finite abelian group. Show that the product $g_1 g_2 \cdots g_n$ is an element of order $\leqslant 2$.

Solution: Clearly, $g_1 g_2 \dots g_n$ is an element of G; furthermore, we see that if we square this value, then

$$(g_1 g_2 \cdots g_n)^2 = g_1 g_2 \cdots g_n g_1 g_2 \cdots g_n.$$

Since G is abelian, we may pair each g_i with its corresponding g_j such that $g_i g_j = e_G$. Therefore, we see that $(g_1 g_2 \cdots g_n)^2 = e_G$, so $g_1 g_2 \cdots g_n$ has order at most 2.

Problem (Problem 8)**:** Construct an explicit isomorphism between the group $(\mathbb{R}_{>0}, \cdot)$ of strictly positive real numbers under multiplication and the group $(\mathbb{R}, +)$ of all real numbers under addition.

On the other hand, show that the group $(\mathbb{Q}_{>0}, \cdot)$ of strictly positive rational numbers under multiplication is not isomorphic to the group $(\mathbb{Q}, +)$ of all rational numbers under addition.

Solution: To see an isomorphism between $(\mathbb{R}_{>0}, \cdot)$ and $(\mathbb{R}, +)$, we define the map $r \mapsto \ln(r)$. Notice that by the definition of the logarithm, $\ln(pr) = \ln(p) + \ln(r)$ (so ln preserves their respective group structures), and that ln admits an inverse, exp, so we have an isomorphism between $(\mathbb{R}_{>0}, \cdot)$ and $(\mathbb{R}, +)$.

On the other hand, we see that if $\varphi \colon (\mathbb{Q}, +) \to (\mathbb{Q}_{>0}, \cdot)$ is any structure-preserving map, then $\varphi(2a) = \varphi(a)^2$, meaning that $\varphi\left(\frac{1}{2}a\right) = \varphi(a)^{1/2}$. Yet, since $\mathbb{Q}_{>0}$ is not closed under the taking of roots, such a map cannot be a homomorphism.

Problem (Problem 9)**:** Use Zorn's Lemma to prove that every (nontrivial) finitely generated group has a maximal proper subgroup.

Solution: Let $G = \langle g_1, \ldots, g_n \rangle$, and let

$$\mathcal{H} = \left\{ H \leqslant G \;\middle|\; H \text{ is a subgroup, } H \neq G \right\}$$

be ordered by inclusion. We claim that $\mathcal{H}$ satisfies the necessary requirements of Zorn's Lemma. To start, we see that $\{e\}$ is a proper subgroup of G, meaning that $\{e\} \in \mathcal{H}$, so $\mathcal{H}$ is nonempty. Furthermore, if $\mathcal{C} = \{H_i\}_{i \in I}$ is a chain in $\mathcal{H}$, then we claim that

$$H = \bigcup_{i \in I} H_i$$

is an upper bound that lies in $\mathcal{H}$. First, we observe that, since $\mathcal{C}$ is totally ordered by inclusion, the union of an arbitrary number of elements of $\mathcal{H}$ is also a subgroup, as we had shown earlier. Additionally, if it were not the case that $H \in \mathcal{H}$ (i.e., $G = H$), then since G is finitely generated, it would follow that each of its generators, $g_1, \ldots, g_n$ are in H. Therefore, there would be some H_i such that all of $g_1, \ldots, g_n$ are in H_i, which would contradict the fact that $\mathcal{C}$ is a chain in H.

Therefore, the conditions of Zorn's Lemma are satisfied, and so G admits a maximal proper subgroup.

Problem (Problem 10)**:**

(a) Show that only a cyclic group of prime order does not have any proper subgroups, and derive that if H is a maximal proper subgroup of an abelian group G, then the quotient G/H is a cyclic group of prime order.

(b) Use (a) to conclude that the additive group of rationals, $(Q, +)$, does not have any maximal proper subgroups, and hence the finitely generated assumption in the previous problem was necessary.

Solution:

(a) Let $e \neq a \in G$. Then, since G does not admit any nontrivial proper subgroups, it follows that $\langle a \rangle = G$, meaning that G is a cyclic group. We see that this means G must be finite, since else, $G \cong \mathbb{Z}$ by corresponding powers of a to the integers, and the integers contain proper subgroups. This implies that $\text{ord}(a) = n < \infty$, meaning that for any $m \neq 0$, $\text{ord}(a^m) = \frac{n}{\gcd(m,n)}$ from an earlier problem; yet, since $\langle a^m \rangle = G$ as well, it follows that $\gcd(m, n) = 1$ for any $m \neq 0$, so that n is prime.

From the fourth isomorphism theorem, it follows that if H is a maximal proper subgroup of an abelian group G, then G/H cannot contain any proper subgroups (or else there would be a proper subgroup of G containing H, which would contradict maximality).

(b) If $H \leqslant \mathbb{Q}$ is a proper subgroup, then there is some $\frac{m}{n} \notin H$, so that $\frac{m}{n} + H \in \mathbb{Q}/H$. This implies that $\frac{1}{n}\mathbb{Z} + H \subseteq \mathbb{Q}/H$, meaning that $\mathbb{Q}/H$ is infinite for any proper subgroup of H. Since all quotients of $\mathbb{Q}$ by proper subgroups are infinite, it follows that none of them can be isomorphic to $\mathbb{Z}/p\mathbb{Z}$ for any prime p, so that $\mathbb{Q}$ does not have any maximal proper subgroups.