Problem 1 (6.1). *1. If $K \trianglelefteq G$ and G/K are solvable, then G is solvable.*

2. Prove that S_n is not solvable for $n \geq 5$.

Proof. 1. Let $K \trianglelefteq G$ such that G/K and K are both solvable. Then there is a solvability series $G_0' \trianglelefteq \ldots \trianglelefteq G_n' = G/K$. Next define G_i as $G_i' = G_i/K$. Since $K \trianglelefteq G$ and $G_i/K \trianglelefteq G_{i+1}/K$ we have that $G_i \trianglelefteq G_{i+1}$. We know that G_{i+1}/G_i is abelian because $G_{i+1}/G_i \cong (G_{i+1}/K)/(G_i/K) = G_{i+1}'/G_i'$ which are abelian. Since K has a solvability series $H_0 \trianglelefteq \ldots \trianglelefteq H_m = K$ we can stitch them together to get

$$\{e\} = H_0 \trianglelefteq \ldots \trianglelefteq H_m = K = G_0 \trianglelefteq \ldots \trianglelefteq$$

which is a solvability series for G.

Therefore the group G is solvable.

2. Since A_n for $n \geq 5$ is simple and not Abelian we know that A_n is not solvable. Since A_n is the only nontrivial subgroup of S_n and S_n is not abelian for $n \geq 5$ any solvability series of S_n would be required to include A_n. However since A_n is not solvable this cannot occur.

Therefore S_n is not solvable for $n \geq 5$.

□

Problem 2 (6.2). *A finite group G is solvable if, and only if, every composition factor of a composition series of G is cyclic of prime order.*

Proof. Suppose that there is a composition series for G such that every factor of the composition series is cyclic of prime order. Then this composition series fulfills the condition to show that G is solvable as cyclic groups are abelian.

Otherwise suppose that G is solvable. Then there is a normal series $\{e\} = G_0 \trianglelefteq \ldots \trianglelefteq G_n = G$ such that the factors are finite and abelian. We can assume that the factors are not trivial as this would signify that $G_i = G_{i+1}$ for some i and then we could remove G_{i+1} and the normal series would still witness solvability. Now suppose that G_{i+1}/G_i was not simple. Then there would exist a normal subgroup $K' = K/G_i \trianglelefteq G_{i+1}/G_i$. This implies that $G_i \trianglelefteq K$ and that $K \trianglelefteq G_{i+1}$. Since K/G_i is a subgroup of an abelian group we know that it is abelian and G_{i+1}/K will also be abelian because $G_i \leq K$ and this implies that K contains the commutator. Thus we have a new series $G_o \trianglelefteq \ldots \trianglelefteq G_i \trianglelefteq K \trianglelefteq G_{i+1} \trianglelefteq \ldots \trianglelefteq G_n$. Now we can repeat this process until there are no non-simple factors left in our series. This process will terminate as G is finite.

This gives us a normal series $H_0 \trianglelefteq \ldots \trianglelefteq H_m$ wherein the factors are finite, abelian, non-trivial, and simple. Since the factors are non-trivial and simple this normal series is in fact a composition series. Moreover finite, abelian, and simple imply cyclic of prime order. Which means that all of the factors of this normal series are cyclic of prime order.

Therefore a group G is solvable if and only if there is a composition series wherein every factor is cyclic of prime order. □

Problem 3 (6.3). *1. Let G be a group and $\phi : M(X) \to G$ a monoid homomorphism which satisfies*

$$\phi(s^{-1}) = \phi(s)^{-1} \text{ for all } s \in S$$

then for any $w \in M(X)$, $\phi(w) = \phi(r(w))$

2. *Let S be a set, R a subset of $F(S)$, G a group, $\phi : S \to G$ a function and $\widetilde{\phi} : F(S) \to G$ the induced group homomorphism. If $\widetilde{\phi}(r) = e$ for all $r \in R$, then there exists a homomorphism $\overline{\phi}$ from $\langle S|R\rangle$ to G such that $\overline{\phi} \circ \pi \circ i = \phi$ where $i : S \to F(S)$ is the inclusion map, $\pi : F(S) \to \langle S|R\rangle$ is the natural surjection, and $\widetilde{\phi} : F(S) \to G$ is the homomorphism satisfying $\widetilde{\phi} \circ i = \phi$.*

Proof. 1. We will prove this statement by induction. Suppose that $|w| = 0$. Then the only valid word is ϵ for which $\epsilon = r(\epsilon)$ and as such $\phi(\epsilon) = \phi(r(\epsilon))$.

Now assume that for $|w| = n$ that $\phi(w) = \phi(r(w))$. Then let $|w| = n + 1$. Decompose $w = sw_1$. Then we have

$$\phi(w) = \phi(sw_1) = \phi(s)\phi(w_1)$$

From our inductive hypothesis we get

$$\phi(s)\phi(w_1) = \phi(s)\phi(r(w_1))$$

There are two cases to consider. Either $r(w_1) = s^{-1}w_2$ or it does not. In the latter case we can simply recombine to get

$$\phi(s)\phi(r(w_1)) = \phi(sr(w_1)) = \phi(r(sw_1)) = \phi(r(w))$$

completing the proof in that case. Otherwise we get

$$\phi(s)\phi(r(s^{-1}w_2)) = \phi(s)\phi(s^{-1}r(w_2)) = \phi(s)\phi(s)^{-1}\phi(r(w_2)) = \phi(r(w_2)) = \phi(r(w))$$

completing the proof in that direction as well.

Therefore $\phi(w) = \phi(r(w))$.

2. First note that $\langle S|R\rangle \cong F(S)/N(R)$ where $N(R)$ denotes the normalizer of R. Then define $\overline{\phi}(sN(R)) := \tilde{\phi}(s)$. Now we show that $\overline{\phi} \circ \pi \circ i = \phi$. First note that $N(R) \subseteq \ker \phi$ as the kernel is a normal subgroup. Thus

$$\overline{\phi} \circ \pi \circ i(s) = \overline{\phi}(i(s)N(R)) = \tilde{\phi} \circ i(s)$$

and by definition of the free group we know that $\tilde{\phi} \circ i(s) = \phi$ completing the proof.

□

Problem 4 (6.5.1)**.** *Using the Todd-Coxeter algorithm to determine and identify the group*

$$G = \langle x, y | x^2 = 1, y^2 = 1, xyx = yxy\rangle$$

First let $H = \langle y\rangle := 1$. Then $y \cdot 1 = 1$ and we'll say that $x \cdot 1 = 2$. Since both x and y are either order 1 or 2 we have that

	y	y	
1		1	1
2		a	2

where we say that $y \cdot 2 = a$ and

	x	x	
1		2	1
2		1	2
a		b	a

However using the last relation of G we have that

$$x \cdot a = (x(yx \cdot 1)) = yxy \cdot 1$$

implying that $b = a$. If we let $3 := a$. Then we can denote $y = (2\ 3)$ and $x = (1\ 2)$. The group generated by x, y is S_3.

Therefore $G \cong S_3$.

Problem 5 (7.2). *1. Prove that R^X is a group under the multiplication of R.*

2. Prove that $Z(R) \cap R^X = \emptyset$.

Proof. 1. We will show that R^X is closed, has identity, is associative, and contains inverses.

- For closure let $a, b \in R^X$. Then $ab \in R^X$ as $(ab) \cdot (b^{-1}a^{-1}) = e$.
- For identity $1 = 1 \cdot 1 = 1 \cdot 1^{-1}$ which implies that $1 \in R^X$. Since R is a multiplicative identity and $0 \notin R^X$ this will be the identity for R^X.
- For associativity we have that for $a, b, c \in R^X$ that $a(bc) = (ab)c$ as a property inherited from the overlying ring.
- Finally given $a \in R^X$ we let the inverse its inverse in the ring.

Therefore since R^X is closed, has identity, is associative, and contains inverses it is a group.

2. Suppose that $a \in R^X$ and that there exists a $b \in R \setminus \{0\}$ such that $ab = 0$ or $ba = 0$. Without loss of generality assume that it is the former. Then we have

$$b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}0 = 0$$

which is a contradiction.

Therefore $Z(R) \cap R^X = \emptyset$.

□

Problem 6 (7.3). *1. Find the set of all zero divisors of the commutative ring $C([0,1])$ defined in example 7.3. Determine the $C([0,1])^X$.*

2. Let $D \in \mathcal{Q}$ such that the equation $x^2 = D$ has no solution $x \in \mathcal{Q}$. Prove that the set

$$\mathcal{Q}(\sqrt{D}) = \{a + b\sqrt{D} | a, b \in \mathcal{Q}\}$$

forms a field under the ordinary addition and multiplication of complex numbers.

3. Prove $\mathbb{Z}_n$ is an integral domain if, and only if, n is prime.

Proof. 1. The multiplicative inverse of a function if it exists will be $\frac{1}{f(x)}$. So $C([0,1])^X = \{f | f(x) \neq 0, x \in [0,1]\}$ since this will garentee a well defined inverse.

For zero divisors it will be the set of functions where there is at least one value $x \in [0,1]$ such that $f(x) = 0$ and there is an open neighborhood $x \in (a,b) \subseteq [0,1]$ such that $f(y) = 0$ for all $y \in (a,b)$. If a function is in this form we can define its multiplicand to zero by taking a function that is zero everywhere but the interval and attaching a continuous nonzero portion to the interval. For the other direction suppose that all the zeros of f are isolated. Then any multiplicand to get f to zero would have to be zero everywhere except that isolated point breaking continuity.

Therefore $Z(C[0,1])$ is the set of continuous functions such that at least one zero is not isolated.

2. We will show that $\mathcal{Q}(\sqrt{D})$ is a field by showing that we have additive and multiplicative identities and that the operations are associative, commutative, distribute, and have inverses.

   - For additive identity we have $0 \in \mathcal{Q}$.
   $$0 + (a + b\sqrt{D}) = (a + b\sqrt{D}) + 0 = a + b\sqrt{D}$$
   - For multiplicative identity we have $1 \in \mathcal{Q}$.
   $$1(a + b\sqrt{D}) = (a + b\sqrt{D})1 = a + b\sqrt{D}$$
   - For associativity of addition we have
   $$(a+b\sqrt{D})((c+d\sqrt{D})+(e+f\sqrt{D})) = (a+c+e)+(b+d+f)\sqrt{D} = ((a+b\sqrt{D})+(c+d\sqrt{D}))+(e+f\sqrt{D})$$
   - For commutativity of addition we have
   $$(a+b\sqrt{D})+(c+d\sqrt{D}) = (a+c)+(b+d)\sqrt{D} = (c+a)+(d+b)\sqrt{D} = (c+d\sqrt{D})+(a+b\sqrt{D})$$
   - Additive inverse we have
   $$(a + b\sqrt{D}) + (-a - b\sqrt{D}) = 0$$
   - For associativity of multiplication we have
   $$\begin{aligned}((a + b\sqrt{D})(c + d\sqrt{D}))(e + f\sqrt{D}) &= ((ac + Dbd) + (ad + bc)\sqrt{D})(e + f\sqrt{D}) \\ &= (ace + Dbd + adfD + bcfD) + (ade + bce + acf + Dbdf)\sqrt{D} \\ &= (a + b\sqrt{D})((ce + Ddf) + (cf + de)\sqrt{D}) \\ &= (a + b\sqrt{D})(c + d\sqrt{D})((e + f\sqrt{D}))\end{aligned}$$
   - For commutativity of multiplication we have
   $$(a+b\sqrt{D})(b+d\sqrt{D}) = (ac+Dbd)+(ad+bc)\sqrt{D} = (ca+Ddb)+(da+cb)\sqrt{D} = (b+d\sqrt{D})(a+b\sqrt{D})$$
   - For multiplicative inverse if $a, b \neq 0$ we have
   $$(a + b\sqrt{D})\frac{a - b\sqrt{D}}{a^2 - Db^2} = \frac{a^2 - Db^2 + (ab - ba)\sqrt{D}}{a^2 - Db^2} = \frac{a^2 - Db^2}{a^2 - Db^2} = 1$$

   Therefore $\mathcal{Q}(\sqrt{D})$ is a field.

3. Suppose that n is prime. Then for any $x \in \mathbb{Z}_n \setminus \{0\}$ the $\gcd(x, n) = 1$ which from a prior homework means that $x \in \mathbb{Z}^X$ and as such is not a zero divisor. Thus $\mathbb{Z}_n$ is an integral domain if n is prime.

   Otherwise suppose that n is not prime. Then there exist $ab = n$ such that $a, b \neq 1$ or n. However then $ab \equiv 0 \mod n$ which implies that $a \in \mathbb{Z}_n$ is a zero divisor and thus $\mathbb{Z}_n$ is not an integral domain.

   Therefore $\mathbb{Z}_n$ is an integral domain if and only if n is prime.

□

Problem 7 (7.4). *1. Prove that the set*

$$\mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D} | a, b \in \mathbb{Z}\}$$

is a subring of $\mathcal{Q}(\sqrt{D})$ and $\mathbb{Z}[\sqrt{D}]$ is an integral domain.

2. *Define the norm function* $N : \mathcal{Q}(\sqrt{D}) \to \mathcal{Q}$ *by*

$$N(a + b\sqrt{D}) = a^2 - Db^2$$

Prove that $N(\alpha\beta) = N(\alpha)N(\beta)$ *for all* $\alpha, \beta \in \mathcal{Q}(\sqrt{D})$.

3. *Show that for any* $\alpha \in \mathbb{Z}[\sqrt{D}]$, α *is a unit of* $\mathbb{Z}[\sqrt{D}]$ *if, and only if,* $N(\alpha) = \pm 1$.

Proof. 1. Both 0 and 1 are integers so they are contained in $\mathbb{Z}[\sqrt{D}]$. Then if $a, b, c, d \in \mathbb{Z}$ then for addition $(a + b\sqrt{D}) + (c + d\sqrt{D}) = (a + b) + (c + d)\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$.
For multiplication we have $(a+b\sqrt{D})(c+d\sqrt{D}) = (ac+Dbd)+(ad+bc)\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$ Finally if $-a, -b \in \mathbb{Z}$ so it is closed under addition, multiplication, and additive inverses. Therefore $\mathbb{Z}[\sqrt{D}]$ is a subring of $\mathcal{Q}(\sqrt{D})$. Moreover because $\mathcal{Q}(\sqrt{D})$ is a field $\mathbb{Z}[\sqrt{D}]$ there will be no zero divisors. As such $\mathbb{Z}[\sqrt{D}]$ is an integral domain.

2. Let $\alpha = a + b\sqrt{D}$ and $\beta = c + d\sqrt{D}$. Then

$$\begin{aligned}
N(\alpha\beta) &= N((ac + Dbd) + (ad + bc)\sqrt{D}) \\
&= (ac + Dbd)^2 - D(ad + bc)^2 \\
&= a^2c^2 + 2acDbd + D^2b^2d^2 - Da^2d^2 - D2adbc - Db^2c^2 \\
&= (a^2 - Db^2)(c^2 - Dd^2) \\
&= N(\alpha)N(\beta)
\end{aligned}$$

3. Note that if we view $a + b\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$ in $\mathcal{Q}(\sqrt{D})$ then $(a + b\sqrt{D})^{-1} = \frac{a-b\sqrt{D}}{a^2-Db^2}$. Now suppose that $N(a + b\sqrt{D}) = \pm 1$. Then the denominator of $\frac{a-b\sqrt{D}}{a^2-Db^2}$ is ± 1 which means that $(a + b\sqrt{D})^{-1}$ has integer coefficients and as such is a unit.
Otherwise suppose that $(a + b\sqrt{D})$ is a unit. Then $\frac{a}{a^2-Db^2}, \frac{b}{a^2-Db^2} \in \mathbb{Z}$. However this can only occur if the denominator $(a^2 - Db^2) = N(a + b\sqrt{D}) = \pm 1$.
Therefore $a + b\sqrt{D}$ is a unit if and only if $N(a + b\sqrt{D}) = \pm 1$.

□

Problem 8 (7.5)**.** *Let* R *be a ring. For any* $a, b \in R$, *if* $1 - ab$ *is a unit, then so is* $1 - ba$.

Proof. Let $(1 - ab)^{-1} = u$. Then

$$\begin{aligned}
(1 - bua)(1 - ba) &= 1 - ba + bua(1 - ba) \\
&= 1 - ba + bu(a - aba) \\
&= 1 - ba + bu(1 - ab)a \\
&= 1 - ba + ba
\end{aligned}$$

Which means that the inverse of $(1 - ba)^{-1} = 1 + bua$ and as such $1 - ba$ is a unit if $1 - ab$ is. □

Problem 9. *Compute the commutator subgroup of* S_4.

The commutator subgroup of S_4 is A_4. To see this first note that the elements of the commutator are of the form $\sigma\tau\sigma^{-1}\tau^{-1}$ which implies that there are an even number of transpositions since the number will add and any cancellations will occur in pairs. Thus $[S_4, S_4] \subseteq A_4$.

Next note that A_4 is generated by 3-cycles. For a given 3-cycle $(i\ j\ k)$ we can decompose it as $(i\ j)(i\ k)(i\ j)(i\ k)$ which means that $(i\ j\ k) \in [S_4, S_4]$. However this implies that $A_4 \subseteq [S_4, S_4]$ and therefore $A_4 = [S_4, S_4]$.