Problem 5 in 3.4. Prove that subgroups and quotient groups of a solvable group are solvable.

Solution. Suppose that $G$ is solvable, and $H$ is a subgroup of $G$. Since $G$ is solvable, it has a filtration: $1 = G_0 \leq G_1 \leq G_2 \leq \cdots \leq G_n = G$, where $G_{i+1}/G_i$ is abelian. Let $H_i = H \cap G_i$. Since $G_i$ is normal in $G_{i+1}$, it is obvious that $H_i$ is normal in $H_{i+1}$.

Lemma 1. $H_{i+1}/H_i$ is isomorphic to a subgroup of $G_{i+1}/G_i$.

Proof. Consider the composite homomorphism $\pi : H_{i+1} \rightarrow G_{i+1} \rightarrow G_{i+1}/G_i$, where the first homomorphism is the inclusion of $H_{i+1}$ as a subgroup of $G_{i+1}$ and the second is the projection of $G_{i+1}$ onto the quotient. The kernel of this map is

$$H_{i+1} \cap G_i = H \cap G_{i+1} \cap G_i = H \cap G_i = H_i.$$

Therefore $\pi(H_{i+1}) \cong H_{i+1}/H_i$ by the First Isomorphism Theorem (Theorem 16 on page 97).

Since $H_{i+1}/H_i$ is a subgroup of an abelian group, it is abelian and $1 = H_0 \leq H_1 \leq H_2 \leq \cdots \leq H_n = H$, proving that $H$ is solvable.

Next suppose that $Q = G/N$ is a quotient of $G$, with $N$ some normal subgroup. Let $\phi : G \rightarrow Q$ be the projection map. Define $Q_i = \phi(G_i)$.

Lemma 2. The subgroup $Q_i$ is normal in $Q_{i+1}$ and $Q_{i+1}/Q_i$ is isomorphic to a quotient of $G_{i+1}/G_i$.

Proof. The normality of $Q_i = \phi(G_i)$ in $Q_{i+1} = \phi(G_{i+1})$ follows from the normality of $G_i$ in $G_{i+1}$.
Let \( \theta : G_{i+1} \longrightarrow Q_{i+1}/Q_i \) be the composition \( G_{i+1} \longrightarrow Q_{i+1} \longrightarrow Q_{i+1}/Q_i \). The first homomorphism here is \( \phi \) restricted to \( G_{i+1} \), and the second homomorphism is the projection onto the quotient. Both of these homomorphisms are surjective, so \( Q_{i+1}/Q_i \) is isomorphic to \( G_{i+1}/\ker(\theta) \). Clearly \( G_{i+1} \subseteq \ker(\theta) \) so \( G_{i+1}/\ker(\theta) \) is isomorphic to a quotient of \( G_{i+1}/G_i \). \( \Box \)

Now \( 1 = Q_0 \trianglelefteq Q_1 \trianglelefteq Q_2 \trianglelefteq \cdots \trianglelefteq Q_n = Q \).

**Problem 12 in 3.4.** Prove that the following are equivalent:

(i) Every group of odd order is solvable;

(ii) The only simple groups of odd order are those of prime order.

These facts were proved in a famous paper of Feit and Thompson in 1963.

This depends on the fact that every finite group has a composition series, that is, a sequence of subgroups \( 1 = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_n = G \) where \( G_{i+1}/G_i \) is simple.

**Lemma 3.** Every finite group \( G \) has a composition series.

This is part of the Jordan-Hölder theorem (Theorem 22) on page 103. Since the authors don’t prove it here is a proof. For a full proof of the important Jordan-Hölder theorem, see Lang’s Algebra, page 22.

**Proof.** Let \( H \) be a proper normal subgroup that is as large as possible. By induction on \( |G| \), \( H \) has a composition series \( 1 = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_{n-1} = H \) where \( G_{i+1}/G_i \) is simple. Now we can can complete this to a composition series for \( G \) by taking \( G_n = G \). We have only to check that \( G_n/G_{n-1} = G/H \) is simple. But if \( G/H \) is not simple, it has a nontrivial normal subgroup. By Theorem 20 on page 99, part (5), this subgroup must be of the form \( K/H \) where \( K \) is a normal subgroup of \( G \) that is proper but larger than \( H \). This contradicts the way \( H \) was chosen. \( \Box \)

**Solution.** First let us check (i) implies (ii). Assume every group of odd order, and let \( G \) be a simple group of odd order. Then \( G \) is solvable, so it has a filtration \( 1 = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_n = G \) where \( G_{i+1}/G_i \) is abelian. Because \( G \) is simple, \( G_1 \) can only be 1 or \( G \), and this filtration has length 2. This means that \( G = G/1 = G_1/G_0 \) is abelian. But an abelian simple group is cyclic of prime order, proving (i) \( \Rightarrow \) (ii).

Let us check that (ii) implies (i). Let \( G \) be a group of odd order. Find a composition series \( 1 = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_n = G \). The quotients \( G_{i+1}/G_i \) are solvable by Problem 5.
Problem 8 in 5.5. Construct a nonabelian group of order 75. Classify all groups of order 75. (There are three of them.)

Solution. If $G$ is an abelian group of order 75, then $G$ is the direct product of its Sylow subgroups. The 3-Sylow must be $Z_3$ while the 5-Sylow may be $Z_{25}$ or $Z_5 \times Z_5$, so

$$G \cong Z_3 \times Z_{25} \cong Z_{75} \quad \text{or} \quad G \cong Z_3 \times Z_5 \times Z_5 \cong Z_{15} \times Z_5.$$ 

It remains to consider the nonabelian groups of order 75. Let $G$ be nonabelian, and consider the 5-Sylow subgroup $P$. By the Sylow theorems, its order must divide 75 and be $\equiv 1 \mod 5$. This means that $P \triangleleft G$. If $Q$ is the 3-Sylow, then $PQ$ is a subgroup of $G$ (by Theorem 16 on page 187) whose order is a multiple of 25 and of 3. Therefore $PQ = G$. On the other hand, $P \cap Q$ is trivial, so Theorem 12 on page 180 applies, and $G$ is the semidirect product $P \rtimes Q$ with respect to some homomorphism $\varphi : Q \rightarrow \text{Aut}(P)$. The semidirect product can be nonabelian only if $\varphi$ is nontrivial, so $\text{Aut}(P)$ must have order a multiple of 3.

If $P \cong Z_{25}$ then $\text{Aut}(P) \cong (\mathbb{Z}/25\mathbb{Z})^\times$ by Proposition 16 on page 135. Thus the order of $\text{Aut}(P)$ is $\phi(25) = 20$. This is not a multiple of 3, so this case is impossible.

We are left with the case $P \cong Z_5 \times Z_5$. The automorphism group of this is $\text{GL}(2, \mathbb{F}_5)$ by part (3) of Proposition 17 on page 136. (Think of $Z_5 \times Z_5$, written additively, as a 2-dimensional vector space over $\mathbb{F}_5$. Its automorphisms are linear transformations, so $\text{Aut}(P)$ is isomorphic to the ring of $2 \times 2$ invertible matrices.) In this case $| \text{GL}(2, \mathbb{F}_q) | = (q^2 - 1)(q^2 - q)$ by the Example on page 413 of Dummit and Foote. If $q = 5$, this is $24 \cdot 20 = 2^3 \cdot 3 \cdot 5$. Hence $\phi$ can be any homomorphism of $Q = Z_3$ onto the Sylow subgroup of $\text{GL}(2, \mathbb{F}_5) = \text{Aut}(P)$.

To make this group more explicit, let us exhibit a particular automorphism of order 3. We start with the matrix

$$M = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \in \text{GL}(2, \mathbb{F}_5).$$

We may check that $M^3 = 1$. To interpret this as an automorphism, write $P \cong Z_5 \times Z_5$ additively. It has generators $x$ and $y$ corresponding to the column vectors $x = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $y = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ and $M$ sends $x$ to $-x + y$, and $y$ to $-x$. 

3
However we would like to write $P$ multiplicatively. So let us translate this automorphism from additive to multiplicative notation. Let

$$P = \langle x, y | x^5 = y^5 = 1, xy = yx \rangle$$

Then $M$ represents an automorphism $\mu$ of $P$ such that $\mu(x) = x^{-1}y$, $\mu(y) = x^{-1}$. It is easy to check that it has order 3. Let $Q = \mathbb{Z}_3$ with generator $z$. Then we have a homomorphism $\phi: Q \to \text{Aut}(P)$ such that $\phi(z) = \mu$. The semidirect product $P \rtimes_\phi Q$ is the unique nonabelian group of order 75.

In terms of generators and relations, it may be described thus:

$$\langle x, y, z | x^5 = y^5 = z^3 = 1, xy = yx, zxz^{-1} = x^{-1}y, zyz^{-1} = x^{-1} \rangle.$$

Problem 1 in 14.6. Show that a cubic with a multiple root has a linear factor. Is the same true for quartics?

Solution. The wording of the problem seems slightly unclear. He means that if $f \in F[x]$ has a multiple root in an extension field $E$, then it has a linear factor in $F[x]$. The key insight is that it does not matter whether we take the greatest common divisor of $f$ and $f'$ in $F[x]$ or in $E[x]$. We will digress to discuss this point. As I mentioned, you must assume that the characteristic is not 3.

We remind the reader that although the notion of greatest common divisor is useful for unique factorization domains, it is particularly simple over principal ideal domains.

If $R$ is a principal ideal domain and $f, g \in R$, then the greatest common divisor of $f$ and $g$ may be characterized as a generator $\delta$ of the ideal $I = Rf + Rg$. It has the property that $\delta$ divides both $f$ and $g$, and that $\delta$ can be written as $\delta = mf + ng$, $m, n \in R$.

Lemma 4. Let $R \subseteq S$ be principal ideal domains and let $f, g \in R$. Let $\delta$ be the greatest common divisor of $f$ and $g$ as an element of $R$. Then $\delta$ is also the greatest common divisor of $f$ and $g$ as an element of $S$.

Proof. We have $\delta$ dividing $f$ and $g$ (in $R$) and $\delta = mf + ng$ for $m, n \in R$. These facts remain true in $S$, so $\delta$ is the greatest common divisor of $f$ and $g$ as an element of $S$. \qed

Now we may finish the proof. Let $h$ be the greatest common divisor of $f$ and $f'$ in $F[x]$. Because $f$ has a multiple root, the degree of $h$ is at least 1.
But it is at most 2 since \( f' \) has degree 2. Therefore \( h \) is a polynomial in \( F[x] \) of degree 1 or 2 that divides \( f \). Thus either \( h \) or \( f/h \) is linear, proving that \( f \) has a linear factor.

We are asked whether the statement remains true when \( f \) is quartic. The answer is no. For example, we could take \( f(x) = g(x)^2 \), where \( g(x) \) is an irreducible quadratic. This has two multiple roots in the splitting field, namely the roots of \( g(x) \). But \( f(x) \) has no linear factors.

**Problem 2 in 14.6.** Determine the Galois groups of the following polynomials:

(a) \( x^3 - x^2 - 4 \)

(b) \( x^3 - 2x + 4 \)

(c) \( x^3 - x + 1 \)

(d) \( x^3 + x^2 - 2x - 1 \).

**Solution.** We recall that the discriminant of \( f(x) = x^3 + bx + c \) is \( -(27c^2 + 4b^3) \).

(a): \( f(x) = x^3 - x^2 - 4 \). Make the substitution \( x \mapsto x + \frac{1}{3} \) to transform the polynomial into \( x^3 - \frac{1}{3}x - \frac{110}{27} \). This does not change the discriminant, which is therefore

\[
D = -27 \left( \frac{-110}{27} \right)^2 - 4 \left( -\frac{1}{3} \right)^3 = -448.
\]

Since the discriminant is negative, it is not a square over \( \mathbb{Q} \), and so the Galois group is \( S_3 \). The polynomial is irreducible. The field contains \( \mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{-7}) \).

(b): \( f(x) = x^3 - 2x + 4 \). The discriminant is \(-400\). Even though \( 400 = 20^2 \) is a square, \(-400\) is not a square in \( \mathbb{Q} \) because it is negative. The Galois group is again \( S_3 \) and the field contains \( \mathbb{Q}(i) \).

(c): The discriminant is \(-23\). This is negative, so the Galois group is \( S_3 \).

(d): You may remember this as the irreducible polynomial satisfied by \( \zeta_7 + \zeta_7^{-1} = 2 \cos \left( \frac{2\pi}{7} \right) \). So it generates the unique cubic subfield inside \( \mathbb{Q}(\zeta_7) \), which is abelian over \( \mathbb{Q} \). So the Galois group is cyclic, \( Z_3 \). Alternatively, let us compute the discriminant. Making the change of variables \( x \mapsto x - \frac{1}{3} \).
gives the polynomial \( x^3 - \frac{7}{3} x - \frac{7}{27} \) so the discriminant is

\[
-27 \left( -\frac{7}{27} \right)^2 - 4 \left( \frac{7}{3} \right)^3 = 49.
\]

Since \( 49 = 7^2 \) this is a square over \( \mathbb{Q} \), so the Galois group is \( Z_3 \). If you know some algebraic number theory, the 7 will tell you to look for it inside the cyclotomic field of 7-th roots of unity.

**Problem 3 in 14.6.** Prove that for any \( a, b \in \mathbb{F}_p \) if \( x^3 + ax + b \) is irreducible then \(-4a^3 - 26b^2\) is a square in \( \mathbb{F}_p \). \( 1 = G_0 \subseteq G_1 \subseteq G_2 \subseteq \cdots \subseteq G_n = G \)

**Solution.** We will write \( q = p^n \). Let \( \alpha, \beta, \gamma \) be the roots of \( f(x) = x^3 + ax + b \). Because \( f \) is assumed to be irreducible, these lie in the unique cubic extension field \( E = \mathbb{F}_q \). Therefore \( r = (\alpha - \beta)(\alpha - \gamma)(\beta - \gamma) \in E \). The square \( r^2 \) is the discriminant \( D(f) \), which is in \( F = \mathbb{F}_q \). Since \( r^2 \in F, r \) lies in the unique quadratic extension of \( F \). But this field is not contained in \( E \). Both fields \( \mathbb{F}_q^2 \) and \( \mathbb{F}_q^3 \) are contained in \( \mathbb{F}_q^4 \), so we can take their intersection, but this intersection is just \( \mathbb{F}_q \). Since \( r \in \mathbb{F}_q^3 \cap \mathbb{F}_q^2 = \mathbb{F}_q \), we see that \( D(f) = r^2 \) is a square in \( \mathbb{F}_q \).

**Problem 4 in 14.6.** Determine the Galois group of \( x^4 - 25 \).

**Solution.** This polynomial is reducible over \( \mathbb{Q} \):

\[
x^4 - 25 = (x^2 - 5)(x^3 + 5).
\]

So the roots are \( \pm \sqrt{5} \) and \( \pm \sqrt{5}i \). Clearly the splitting field is \( \mathbb{Q}(\sqrt{5}, i) \). It has degree 4 over \( \mathbb{Q} \) and every automorphism sends \( \sqrt{5} \) to \( \pm \sqrt{5} \) and \( i \) to \( \pm i \), so the Galois group is \( Z_2 \times Z_2 \).

**Problem 44 in 14.6.** Let \( \alpha_1, \alpha_2, \alpha_3, \alpha_4 \) be the roots of a quartic polynomial \( f(x) \) over \( \mathbb{Q} \). Show that the quantities \( \alpha_1 \alpha_2 + \alpha_3 \alpha_4, \alpha_1 \alpha_3 + \alpha_2 \alpha_4 \) and \( \alpha_1 \alpha_4 + \alpha_2 \alpha_3 \) are permuted by the Galois group of \( f(x) \). Conclude that these elements are the roots of a cubic polynomial with coefficients in \( \mathbb{Q} \) (sometimes called the cubic resolvent of \( f(x) \)).

**Solution.** If \( \sigma \in \text{Gal}(E/\mathbb{Q}) \), where \( E \) is the splitting field of \( f \), then \( \sigma(\alpha_1), \sigma(\alpha_2), \sigma(\alpha_3) \) and \( \sigma(\alpha_4) \) are \( \alpha_1, \alpha_2, \alpha_3, \alpha_4 \) in some order, and it is therefore clear that \( \sigma(\alpha_1 \alpha_2 + \alpha_3 \alpha_4) = \sigma(\alpha_1)\sigma(\alpha_2) + \sigma(\alpha_3)\sigma(\alpha_4) \) is one of \( \beta_1 = \alpha_1 \alpha_2 + \alpha_3 \alpha_4, \beta_2 = \alpha_1 \alpha_3 + \alpha_2 \alpha_4 \) and \( \beta_3 = \alpha_1 \alpha_4 + \alpha_2 \alpha_3 \), and so forth. Since \( \sigma \)
permutes $\beta_1, \beta_2$ and $\beta_3$, the symmetric functions in $\beta_1, \beta_2$ and $\beta_3$ are invariant under $\sigma$. In particular, $\sigma$ fixes $a, b, c$ where
\[
x^3 + ax^2 + bx + c = (x - \beta_1)(x - \beta_2)(x - \beta_3),
\]
so
\[
a = -(\beta_1 + \beta_2 + \beta_3), \quad b = \beta_1\beta_2 + \beta_2\beta_3 + \beta_3\beta_1, \quad c = \beta_1\beta_2\beta_3.
\]
Thus $a, b, c$ are in $\mathbb{Q}$, and the cubic resolvent (1) is in $\mathbb{Q}[x]$.

**Problem 49 in 14.6.** Prove that the Galois group over $\mathbb{Q}$ of $x^6 - 4x^3 + 1$ is isomorphic to the dihedral group of order 12. (**Hint:** Observe that the two real roots are inverses of each other.)

**Solution.** We will prove that $\text{Gal}(E/\mathbb{Q}) \cong S_3 \times Z_2$, where $E$ is the splitting field of $f(x) = x^6 - 4x^3 + 1$. Then we will point out that $D_{12} \cong S_3 \times Z_2$.

If $\alpha$ is a root of this, then $\alpha^3$ is a root of $x^2 - 4x + 1$, that is, $\alpha^3 = 2 \pm \sqrt{3}$. Hence the splitting field $E$ contains $\sqrt{3}$. Over the subfield $\mathbb{Q}(\sqrt{3})$, we may factor the polynomial
\[
x^6 - 4x^3 + 1 = \left(x^3 - 2 - \sqrt{3}\right) \left(x^3 - 2 + \sqrt{3}\right).
\]
Note that $2 + \sqrt{3}$ and $2 - \sqrt{3}$ are inverses, so $\alpha^{-1}$ is a root of $x^3 - 2 + \sqrt{3}$. Therefore we may completely factor the polynomial
\[
x^6 - 4x^3 + 1 = (x - \alpha)(x - \rho\alpha)(x - \rho^2\alpha)(x - \alpha^{-1})(x - (\rho\alpha)^{-1})(x - (\rho^2\alpha)^{-1}).
\]
It is clear that the splitting field $E = \mathbb{Q}(\alpha, \rho)$ where $\rho = e^{2\pi i/3}$, and since $\mathbb{Q}(\rho) = \mathbb{Q}(\sqrt{3})$, $E$ contains the biquadratic field $\mathbb{Q}(\sqrt{3}, \sqrt{-3})$.

Since the polynomial $x^3 - 2 - \sqrt{3}$ has imaginary roots, its discriminant is negative, and so it is irreducible over $\mathbb{Q}(\sqrt{3}) \subseteq \mathbb{R}$, with Galois group $S_3$. This proves that $\text{Gal} \left(E/\mathbb{Q}(\sqrt{3})\right)$ contains Galois automorphisms corresponding to all permutations of the roots $\alpha, \rho\alpha, \rho^2\alpha$ of $x^3 - 2 - \sqrt{3}$. Given such a permutation, the effect on the other roots $\alpha^{-1}, (\rho\alpha)^{-1}$ and $(\rho^2\alpha)^{-1}$ is determined. So $\text{Gal} \left(E/\mathbb{Q}(\sqrt{3})\right)$ is a subgroup isomorphic to $S_3$.

To obtain other elements of $\text{Gal}(E/\mathbb{Q})$, let us extend the automorphism $\sqrt{3} \rightarrow -\sqrt{3}$ of $\text{Gal} \left(\mathbb{Q}(\sqrt{3})/\mathbb{Q}\right)$ to an automorphism $\theta$ of $\text{Gal}(E/\mathbb{Q})$. We have some flexibility in this extension, since we may compose with an arbitrary element of $\text{Gal} \left(E/\mathbb{Q}(\sqrt{3})\right)$, and so we may arrange that $\theta(\alpha) = \alpha^{-1}$, and...
\(\theta(\rho \alpha) = (\rho \alpha)^{-1}\) and \(\theta(\rho^2 \alpha) = (\rho^2 \alpha)^{-1}\). In other words, \(\theta(\gamma) = \gamma^{-1}\) for every root \(\gamma\) of \(f\).

Now let \(\sigma \in \text{Gal}(E/\mathbb{Q}(\sqrt{3}))\). We show that \(\sigma \theta = \theta \sigma\). Indeed, if \(\gamma\) is one of the roots of \(f\) then \(\sigma \theta(\gamma) = \sigma(\gamma^{-1}) = \sigma(\gamma)^{-1} = \theta \sigma(\gamma)\). We see that \(\theta^2 = 1\) and that it commutes with \(\text{Gal}(E/\mathbb{Q}(\sqrt{3})) \cong S_3\). Since \(\text{Gal}(E/\mathbb{Q}(\sqrt{3}))\) is obviously the union of \(S_3\) and the coset \(\theta S_3\), it is clear that \(\text{Gal}(E/\mathbb{Q}(\sqrt{3})) \cong S_3 \times Z_2\).

We have found the Galois group, but it remains to be shown that this group is dihedral. The group \(S_3\) is already dihedral of order 6, so let \(\sigma\) be a 3-cycle and \(\tau\) a transposition. In terms of generators and relations

\[
S_3 = \langle \sigma, \tau | \sigma^3 = \tau^2 = 1, \tau \sigma \tau^{-1} = \sigma^{-1} \rangle,
\]

\[
S_3 \times Z_2 = \langle \sigma, \tau, \theta | \sigma^3 = \tau^2 = \theta^2 = 1, \tau \sigma \tau^{-1} = \sigma^{-1}, \sigma \theta = \theta \sigma, \tau \theta = \theta \tau \rangle.
\]

Now let \(\rho = \sigma \theta\). Then \(\rho\) has order 6, and \(\sigma = \rho^4, \theta = \rho^3\) are both in the cyclic group \(\langle \rho \rangle\). In other words \(\langle \rho \rangle \cong Z_3 \times Z_2 \cong \langle \sigma, \theta \rangle\). We also have \(\tau \rho \tau^{-1} = \rho^{-1}\), so

\[
\langle \sigma, \tau, \theta | \sigma^3 = \tau^2 = \theta^2 = 1, \tau \sigma \tau^{-1} = \sigma^{-1}, \sigma \theta = \theta \sigma, \tau \theta = \theta \tau \rangle = \langle \rho, \tau | \rho^6 = \tau^2 = 1, \tau \rho \tau^{-1} = \rho^{-1} \rangle.
\]

This proves that \(S_3 \times Z_2 \cong D_{12}\).