1. Section 14.3

4. Construct the finite field of 16 elements and find a generator for the multiplicative group. How many generators are there?

To construct the finite field of 16 elements, we begin with $\mathbb{F}_2$ and adjoin a root with a minimum polynomial of degree four. One such degree four irreducible polynomial is $x^4 + x + 1$ (0 and 1 are not roots, and the only irreducible polynomial of degree 2, namely $x^2 + x + 1$, does not divide it). As such, the field

$$\mathbb{F}_{24} = \mathbb{F}_2[x]/(x^4 + x + 1)$$

is a field with 16 elements, and has a basis over $\mathbb{F}_2$ given by $1, x, x^2, x^3$.

It follows by Lagrange’s Theorem and the observation $\#\mathbb{F}_{24} = 15$ that $x$ generates the unit group. Indeed, $x^3 \neq 1$ and $x^5 = x \cdot x^4 = x \cdot (x + 1) = x^2 + x \neq 1$.

There are $\varphi(15) = \varphi(3)\varphi(5) = 2 \cdot 4 = 8$ generators.

6. Suppose $K = \mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{D_1}, \sqrt{D_2})$ with $D_1, D_2 \in \mathbb{Z}$, is a biquadratic extension and that $\theta = a + b\sqrt{D_1} + c\sqrt{D_2} + d\sqrt{D_1D_2}$ where $a, b, c, d \in \mathbb{Z}$ are integers, and at least two of $b, c, d$ are nonzero. Prove that the minimum polynomial $m_\theta(x)$ for $\theta$ over $\mathbb{Q}$ is irreducible of degree 4 over $\mathbb{Q}$ but is reducible modulo every prime $p$. In particular, show that the polynomial $x^4 - 10x^2 + 1$ is irreducible in $\mathbb{Z}[x]$ but is reducible modulo every prime.

Proof: The problem as stated in the book is missing a condition that we have included above: we need that at least two of $b, c, d$ are nonzero, so let us suppose that this is the case.

The minimal polynomial of $\theta$ is of course irreducible; we must show it has degree 4. If not, then since $[K : \mathbb{Q}] = 4$, we would have $\theta \in \mathbb{Q}$ or $[\mathbb{Q}(\theta) : \mathbb{Q}] = 2$. Since $1, \sqrt{D_1}, \sqrt{D_2}, \sqrt{D_1D_2}$ form a basis of $K$ over $\mathbb{Q}$, we have $\theta \not\in \mathbb{Q}$ as long as at least one of $b, c, d$ and $d$ is nonzero. If $[\mathbb{Q}(\theta) : \mathbb{Q}] = 2$, then $\theta$ is fixed by a nontrivial element of $\text{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. The elements of $\text{Gal}(K/\mathbb{Q})$ are the automorphisms given by

$$\sqrt{D_1} \mapsto \pm \sqrt{D_1}, \quad \sqrt{D_2} \mapsto \pm \sqrt{D_2}$$

for all 4 possible choices of $\pm$. For each of the nontrivial automorphisms $\sigma$, we find that $\sigma(\theta) = \theta$ implies that at least two of $b, c, d$ are zero. For example, if $\sigma : \sqrt{D_1} \mapsto \sqrt{D_1}, \sqrt{D_2} \mapsto -\sqrt{D_2}$, then $\sigma(\theta) = \theta$ implies

$$a + b\sqrt{D_1} - c\sqrt{D_2} - d\sqrt{D_1D_2} = a + b\sqrt{D_1} + c\sqrt{D_2} + d\sqrt{D_1D_2},$$

which implies that $c = d = 0$. The other two cases are similar. Therefore, we see $K = \mathbb{Q}(\theta)$ and hence that $m_\theta(x)$ has degree 4.

Suppose that $m_\theta(x)$ is irreducible modulo a prime $p$. Let $\alpha$ be a root of $m_\theta(x)$ in $\overline{\mathbb{F}}_p$, so $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = 4$. Yet clearly $\alpha \in \mathbb{F}_p(\sqrt{D_1}, \sqrt{D_2})$. Since $\mathbb{F}_p(\sqrt{D_1}, \sqrt{D_2})^2$ has size 2, it follows that at least one of $D_1, D_2$, or $D_1D_2$ is a square (possibly zero). Thus $[\mathbb{F}_p(\sqrt{D_1}, \sqrt{D_2}) : \mathbb{F}_p] \leq 2$, giving a contradiction.

The polynomial $x^4 - 10x^2 + 1$ is the special case of $\theta = \sqrt{2} + \sqrt{3}$. \qed
8. Determine the splitting field of \( x^p - x + a \) over \( \mathbb{F}_p \), where \( a \neq 0, a \in \mathbb{F}_p \). Show explicitly that the Galois group is cyclic. Such an extension is called an Artin-Schreier extension.

\[ \text{Proof.} \] Let \( K \) be the splitting field of \( x^p - x + a \) over \( \mathbb{F}_p \). We have seen already in problem 13.5.5 (assignment 6) that \( x^p - x + a \) is irreducible and separable over \( \mathbb{F}_p \). Notice that if \( \alpha \) is a root of \( x^p - x + a \) and \( k \in \mathbb{F}_p \), then

\[ (\alpha + k)^p - (\alpha + k) = \alpha^p + k^p - \alpha - k + a = \alpha^p - \alpha + a = 0, \]

since \( k^p = k \). Therefore, the roots of \( x^p - x + a \) in \( K \) are precisely \( \alpha + k \) for \( k \in \mathbb{F}_p \), and \( K = \mathbb{F}_p(\alpha) = \mathbb{F}_{p^m} \).

Since the Galois group is transitive on the roots, we furthermore have a bijection

\[ \text{Gal}(K/\mathbb{F}_p) \cong \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \]

given by \( \sigma \mapsto k \) such that \( \sigma(\alpha) = \alpha + k \). It is easy to verify that this bijection is in fact a group homomorphism, hence a group isomorphism:

\[ \sigma(\alpha) = \alpha + k_1, \quad \tau(\alpha) = \alpha + k_2 \]

implies

\[ \sigma \tau(\alpha) = \sigma(\alpha + k_2) = \sigma(\alpha) + \sigma(k_2) = \alpha + k_1 + k_2. \]

\[ \square \]

9. (a) If \( x \in \mathbb{F}_q \), then \( \sigma_q(x) = x^q = x \), so \( \sigma_q \) fixes \( \mathbb{F}_q \).

(b) Let \( L \) be a finite extension of \( \mathbb{F}_q \) of degree \( n \). Then \( L \) has \( q^n \) elements, so by Lagrange’s theorem \( a^{q^n-1} = 1 \) for all \( a \in L^* \), and hence \( a^{q^n} = a \) for all \( a \in L \). The polynomial \( x^{q^n} - x \in \mathbb{F}_q[x] \) can have at most \( q^n \) roots in any extension field, and we’ve demonstrated this many in \( L \) already, namely the \( q^n \) distinct elements of \( L \). Therefore \( x^{q^n} - x \) splits completely into linear factors over \( L \), and not over any subfield (since every element of \( L \) is a root). Since splitting fields are unique up to isomorphism, we see that any two field extensions of \( \mathbb{F}_q \) of degree \( n \) are isomorphic via an isomorphism fixing \( \mathbb{F}_q \).

(c) We saw in (a) that the automorphism \( \sigma_q \) fixes \( \mathbb{F}_q \) and hence is an element of \( \text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \). Furthermore, if \( \sigma_q^m \) is the identity, then \( a^{q^n} - a = 0 \) for all \( a \in \mathbb{F}_{q^n} \). Since the polynomial \( x^{q^n} - x \) can have at most \( q^n \) roots, we must therefore have \( m \geq n \). Furthermore, every element \( a \in \mathbb{F}_{q^n} \) does satisfy \( a^{q^n} - a = 0 \) as noted above, so \( \sigma_q^n = 1 \) in \( \text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \). Therefore, the order of \( \sigma_q \) in \( \text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \) is \( n \); since this is the size of the Galois group, we see that \( \text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \) is the cyclic group of size \( n \) generated by \( \sigma_q \).

(d) If \( \mathbb{F}_{q^d} \subset \mathbb{F}_{q^n} \), then \( \mathbb{F}_{q^d} \) is vector space over \( \mathbb{F}_{q^d} \). By counting sizes, we see that \( q^n \) is a power of \( q^d \); in other words, \( d \) divides \( n \). Conversely, if \( d \) divides \( n \) then \( x^{q^d} - x \) divides \( x^{q^n} - x \), and hence the splitting field of \( x^{q^d} - x \) is contained in the splitting field of \( x^{q^n} - x \), i.e. \( \mathbb{F}_q^{d} \subset \mathbb{F}_q^{n} \).

2. \textbf{Section 14.4}

1. The minimal polynomial of the element \( \alpha = \sqrt{1 + \sqrt{2}} \) is \( f(x) = (x^2 - 1)^2 - 2 \), which has degree 4. The roots of this polynomial are \( \pm \alpha \) and \( \pm \beta \), where \( \beta = \sqrt{1 - \sqrt{2}} \). So the Galois closure of \( K = \mathbb{Q}(\alpha) \) over \( \mathbb{Q} \) is \( \mathbb{Q}(\alpha, \beta) \), which has degree 2 over \( K \) and degree 8 over \( \mathbb{Q} \).

3. By the Theorem of Primitive Element, \( F = \mathbb{Q}(\alpha) \) for some \( \alpha \in F \). To prove that \( [F : \mathbb{Q}] \leq n \), it suffices to prove that the minimal polynomial of \( \alpha \) over \( \mathbb{Q} \) has degree at most \( n \). By the Cayley-Hamilton Theorem, \( \alpha \) satisfies its characteristic polynomial, which has degree \( n \). Therefore the minimal polynomial of \( \alpha \) has degree at most \( n \), as desired.

6. Let \( K = \mathbb{F}_p(x, y) \) and \( F = \mathbb{F}_p(x^p, y^p) \). For each \( c \in F \), let \( L_c = \mathbb{F}_p(x + cy) \). Since \( (x + cy)^p = x^p + c^py^p \in F \), we have \([L_c : F] \leq p \). However since clearly \( K = L_c(y) \) and \( y \) has degree \( p \) over \( F \), we have \([K : L_c] \leq p \).

Since \([K : F] = p^2 \), we must therefore have \([K : L_c] = [L_c : F] = p \).

Suppose now that \( L_c = L_{c'} \) for distinct \( c, c' \in F \). Let \( L = L_c = L_{c'} \). Since \( x + cy, x + c' y \in L \), we obtain by subtracting that \( (c - c')y \in L \), so \( y \in L \) since \( c, c' \in F \subset L \). Then clearly \( x \in L \) as well, so \( L = K \), a contradiction to the calculation above. Therefore the fields \( L_c \) are distinct, and there are infinitely many since they are indexed by \( c \in F \), and \( F \) is infinite.
3. Section 14.5

4. Since $\zeta_n$ is a primitive $n$th root of unity, any primitive $n$th root of unity can be written $\zeta = \zeta_n^b$ for some integer $b$. Then

$$\sigma_a(\zeta) = \sigma_a(\zeta_n^b) = \sigma_a(\zeta_n)^b = (\zeta_n^b)^b = \zeta_n = (\zeta_n^b)^a = \zeta^a$$

as desired.

5. Recall that $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + 1 = \prod_{i=1}^{p-1}(x - \zeta_i)$. By comparing the coefficients of $x^{p-2}$, we see that $\sum_{i=1}^{p-1} \zeta_i = -1$. Suppose first that $p \not| n$. Let $\sigma_n$ denote the element of $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ such that $\sigma_n(\zeta) = \zeta^n$ for all $\zeta \in \mu_p$. Then $\sigma_n(\sum_{i=1}^{p-1} \zeta_i) = \sum_{i=1}^{p-1} \zeta_i^n$. But the left hand side is $\sigma_n(-1) = -1$, giving the desired result. Finally, if $p \mid n$, then of course $\zeta^n = 1$, so $\sum_{i=1}^{p-1} \zeta_i^n = p - 1$.

7. In $\mathbb{C}$, any $n$th root of unity has the form $\zeta = e^{2\pi i a/n}$, and so

$$\zeta = e^{2\pi i a/n} = e^{−2\pi i a/n} = \zeta^{-1}.$$  

Therefore complex conjugation restricts to the automorphism $\sigma_{−1}$ on $\mathbb{Q}(\zeta)$. The subfield of real elements of $\mathbb{Q}(\zeta)$, denoted $\mathbb{Q}(\zeta)^+$, is therefore the fixed field of $\sigma_{−1}$. Since $\sigma_{−1}$ has order 2, we see that $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta)^+] = 2$.  

It is clear that $\zeta + \zeta^{-1}$ is fixed by $\sigma_{−1}$, since $\sigma_{−1}$ swaps $\zeta$ and $\zeta^{-1}$. Therefore $\mathbb{Q}(\zeta + \zeta^{-1}) \subset \mathbb{Q}(\zeta)^+$. On the other hand, the element $\zeta$ satisfies the polynomial

$$(x − \zeta)(x − \zeta^{-1}) = x^2 − (\zeta + \zeta^{-1})x + 1 \in \mathbb{Q}(\zeta + \zeta^{-1})[x].$$

Therefore $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})] \leq 2$, so we must have equality and we must have $\mathbb{Q}(\zeta)^+ = \mathbb{Q}(\zeta + \zeta^{-1})$.

13. (a) The fact that $\sigma_a(\zeta_{p^i}^n) = \zeta_{p^i}^a$, follows from #4. Since $\zeta_{p^i}^n$ is a $p^n$th root of unity, clearly $\sigma_a(\zeta_{p^i}^n) = \zeta_{p^i}^{na}$, depends only on $a$ modulo $p^i$.

(b) The map $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \prod_i \text{Gal}(\mathbb{Q}(\zeta_{p^i}^n)/\mathbb{Q})$ is just the restriction map $\sigma_a \mapsto (\sigma_a \mod p_i^i)$, discussed in part (a). In the Chinese Remainder Theorem, the isomorphism $(\mathbb{Z}/n\mathbb{Z})^* \cong \prod_i (\mathbb{Z}/p_i^i \mathbb{Z})^*$ is simply given by reduction modulo $p_i^n$ for each $i$, i.e. $a \mapsto (a \mod p_i^n)^i$. The result follows.

4. Section 14.6

2. (a) Factors as $x^3 − x^2 − 4 = (x − 2)(x^2 + x + 2)$. Galois group is $\mathbb{Z}/2\mathbb{Z}$.
(b) Factors as $x^3 − 2x + 4 = (x^2 + 2x + 2)$ (x^2 + 2x + 2). Galois group is $\mathbb{Z}/2\mathbb{Z}$.
(c) Irreducible. (Rational root theorem implies only possible roots are ±1, easy to check these aren’t roots.) By equation (14.18),

$$\text{Discriminant} = -4(-1)^3 - 27(1)^2 = -23.$$  

This is not a square, so the Galois group is $S_3$.
(d) Irreducible using same method as in (c). Calculate

$$p = (−6−1)/3 = −7/3, \quad q = (2 + 18 − 27)/27 = 20/27.$$  

$$\text{Discriminant} = -4(-7/3)^3 - 27(20/27)^2 = 36.$$  

This is a square, so Galois group is $\mathbb{Z}/3\mathbb{Z}$.

9. First we show that the polynomial $x^4 + 4x − 1$ is irreducible. There are many ways to do this; here is one. It is easy to check that ±1 are not roots, so the only possible factorization is into two quadratics. From the constant term, such a factorization would necessarily have the form $x^4 + 4x − 1 = (x^2 + ax + 1)(x^2 + bx − 1)$. From the $x$ coefficient we see that $b − a = 4$ and from the $x^3$ coefficient we see that $a + b = 0$. Hence $b = 2$ and $a = −2$. But then the $x^2$ coefficient on the right is −4 rather than 4, so there is no such factorization. Therefore $x^4 + 4x − 1$ is irreducible.

From the formulas on page 614, the resolvent cubic is $h(x) = x^3 + 4x + 16$ and the discriminant is $D = −27(4)^4 + 256(−1)^3 = −531697$. Now $h(x)$ factors as $h(x) = (x + 2)(x^2 − 2x + 8)$. We therefore have $G ≅ D_8$ or $G ≅ \mathbb{Z}/4\mathbb{Z}$. By #19(c), we see that $G ≅ \mathbb{Z}/4\mathbb{Z}$ is not possible since $D < 0$, so $G ≅ D_8$. 

18. Let \( \theta \) be a root of \( f(x) = x^3 - 3x + 1 \). The discriminant is \( D = -4(-3)^3 - 27(1)^2 = 81 \), which is a square, so the splitting field is \( \mathbb{Q}(\theta) \) and the Galois group is isomorphic to \( \mathbb{Z}/3\mathbb{Z} \).

Suppose our polynomial factors as \( f(x) = (x - \theta)(x - \alpha)(x - \beta) \). From the \( x^2 \) coefficient, we see that \( \alpha + \beta = -\theta \). Furthermore, the discriminant \( D \) satisfies
\[
\sqrt{D} = 9 = (\theta - \alpha)(\theta - \beta)(\alpha - \beta)
\]
for some ordering of \( \alpha, \beta \). Since \( f'(\theta) = (\theta - \alpha)(\theta - \beta) \), we obtain
\[
9 = (3\theta^2 - 3)(\alpha - \beta), \quad \text{hence} \quad \alpha - \beta = \frac{3}{\theta^2 - 1}.
\]

One method to calculate the inverse of \( \theta^2 - 1 \) is to use matrices. View \( \mathbb{Q}(\theta) = \mathbb{Q}(\theta, \theta^2) \) as a 3-dimensional vector space over \( \mathbb{Q} \) with basis 1, \( \theta, \theta^2 \). The matrix for multiplication by \( \theta \), viewed as a \( \mathbb{Q} \)-linear transformation of \( \mathbb{Q}(\theta) \), is given with respect to this basis as
\[
\begin{pmatrix}
0 & 0 & -1 \\
1 & 0 & 3 \\
0 & 1 & 0
\end{pmatrix}
\]
Taking the square of this matrix and subtracting 1, we see that the matrix for multiplication by \( \theta^2 - 1 \) is
\[
\begin{pmatrix}
-1 & -1 & 0 \\
0 & 2 & -1 \\
1 & 0 & 2
\end{pmatrix}
\]
The inverse of this matrix times 3 is
\[
\begin{pmatrix}
-4 & -2 & -1 \\
1 & 2 & 1 \\
2 & 1 & 2
\end{pmatrix}
\]
From the first column of this matrix, we see that \( 3/(\theta^2 - 1) = -4 + \theta + 2\theta^2 \). Now it is easy to solve the two linear equations
\[
\begin{align*}
\alpha + \beta &= -\theta \\
\alpha - \beta &= -4 + \theta + 2\theta^2.
\end{align*}
\]
We find \( \alpha = -2 + \theta^2 \) and \( \beta = 2 - \theta - \theta^2 \).

19. (a) Since \( \sqrt{D} \) is the product of the differences of the roots of \( f(x) \), and these roots lie in \( K \), it follows that \( \sqrt{D} \in K \).

(b) The element \( \tau \) has order 2, to \( \tau_K \) has order dividing 2, i.e. order 1 or 2. Now \( \tau_K \) has order 1 if and only if it is trivial, i.e. iff \( K \) is fixed by \( \tau \), i.e. if and only if \( K \subseteq \mathbb{R} \).

(c) Suppose that \( \text{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z} \) and that \( D < 0 \). Since \( \mathbb{Q}(\sqrt{D}) \subseteq K \) and \( \sqrt{D} \notin \mathbb{R} \), it follows from part (b) that \( \tau_K \) has order 2. However, a cyclic group of order 4 has a unique element of order 2, so \( \tau_K \) must be this element; and the fixed field will be the unique subfield of \( K \) of index 2, so this must be \( \mathbb{Q}(\sqrt{D}) \). Therefore \( \tau_K \) fixes \( \mathbb{Q}(\sqrt{D}) \). Yet \( D < 0 \) implies that complex conjugation does not fix \( \sqrt{D} \), so this is a contradiction.

(d) This is the same argument. Let \( K \) be a cyclic quartic field, viewed as a subfield of \( \mathbb{C} \). Suppose that \( \mathbb{Q}(\sqrt{D}) \subseteq K \) with \( D < 0 \). Complex conjugation is an order 2 element of \( \text{Gal}(K/\mathbb{Q}) \) (it is nontrivial because it does not fix \( \sqrt{D} \), since \( D < 0 \)), and hence its fixed field is the unique index 2 subfield of \( K \), namely \( \mathbb{Q}(\sqrt{D}) \). This is a contradiction, since complex conjugation does not fix \( \sqrt{D} \).

References