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

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

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 $\#F_{2^4} = 15$ 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 $\phi(15) = \phi(3) \phi(5) = 2 \cdot 4 = 8$ 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 $b, c$, and $d$ 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 $\theta \notin \mathbb{Q}$ 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 $\mathbb{F}_p(\sqrt{D_1}, \sqrt{D_2})/\mathbb{F}_p$ 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 $\theta = \sqrt{2} + \sqrt{3}$. 

\[\square\]

Date: 06/01/2011.
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.

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 $K = \mathbb{F}_p(\alpha) = \mathbb{F}_{p^}\alpha$.

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 $a^q = a$ for all $a \in L$. The polynomial $x^q - x \in \mathbb{F}_q[x]$ 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 $x^q - x$ 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 $a^{q^m} - a = 0$ 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 $\mathbb{F}_q$. 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. 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 $[K : L_c] = p$. 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

\[
\sigma_a(\zeta) = \sigma_a(\zeta_n) = \sigma_a(\zeta_n^b) = (\zeta_n)^b = \zeta_n^{ab} = (\zeta_n)^a = \zeta^a
\]

as desired.

5. Recall that \(\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + 1 = \prod_{i=1}^{p-1} (x - \epsilon_i)\). By comparing the coefficients of \(x^{p-2}\), we see that \(\sum_{i=1}^{p-1} \epsilon_i = -1\). Suppose first that \(p \nmid n\). Let \(\sigma_n\) denote the element of \(\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})\) such that \(\sigma_n(\zeta) = \zeta^n\) for all \(\zeta \in \mu_p\). Then \(\sigma_n(\sum_{i=1}^{p-1} \epsilon_i) = \sum_{i=1}^{p-1} \epsilon_i^n\). But the left hand side is \(\sigma_n(-1) = -1\), giving the desired result. Finally, if \(p \mid n\), then of course \(\epsilon_i^n = 1\), so \(\sum_{i=1}^{p-1} \epsilon_i^n = p - 1\).

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

\[
\overline{\zeta} = e^{2\pi i a/n} = e^{-2\pi i a/n} = \overline{\zeta}^{-1}.
\]

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 \(\sigma_a(\zeta_{p_i}^{n_i}) = \zeta_{p_i}^{an_i}\) follows from \#4. Since \(\zeta_{p_i}^{n_i}\) is a \(p_i^{n_i}\)th root of unity, clearly \(\sigma_a(\zeta_{p_i}^{n_i}) = \zeta_{p_i}^{an_i}\) depends only on \(a\) modulo \(p_i^{n_i}\).

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

References