Solutions to
Abstract Algebra

Chapter 13 - Field Theory
David S. Dummit & Richard M. Foote

Solutions by positrón0802
`https://positron0802.wordpress.com`

1 January 2021

Contents

13 Field Theory

13.1 Basic Theory and Field Extensions

Exercise 13.1.1. The polynomial $p(x) = x^3 + 9x + 6$ is irreducible in $\mathbb{Z}[x]$ by Eisenstein Criterion with $p = 3$. By Gauss Lemma, it is thien rreducible in $\mathbb{Q}[x]$. To find $(1 + \theta)^{-1}$, we apply the Euclidean algorithm to $p(x)$ and $1 + x$ to find

$$x^3 + 9x + 6 = (1 + x)(x^2 - x + 10) - 4.$$

Evaluating at θ, we have $(1 + \theta)(\theta^2 - \theta + 10) = 4$. Therefore

$$(1 + \theta)^{-1} = \frac{\theta^2 - \theta + 10}{4}.$$

Exercise 13.1.2. Let $f(x) = x^3 - 2x - 2$. The polynomial f is irreducible over $\mathbb{Z}$ by Eisenstein Criterion with $p = 2$, hence over $\mathbb{Q}$ by Gauss Lemma. Now, if θ is a root of f, then $\theta^3 = 2\theta + 2$, so that

$$(1+\theta)(1+\theta+\theta^2) = 1 + 2\theta + 2\theta^2 + \theta^3 = 3 + 4\theta + 2\theta^2.$$

For computing $\dfrac{1+\theta}{1+\theta+\theta^2}$, first we compute $(1+\theta+\theta^2)^{-1}$. Applying the Euclidean algorithm, we obtain

$$x^3 - 2x - 2 = (x^2 + x + 1)(x - 1) - 2x - 1$$

and

$$x^3 - 2x - 2 = (2x + 1)\left(\frac{x^2}{2} - \frac{x}{4} - \frac{7}{8}\right) - \frac{9}{8}.$$

Evaluating at θ, from these equalities it follows that

$$(\theta^2 + \theta + 1)(\theta - 1) = 2\theta + 1 \quad \text{and} \quad (2\theta + 1)^{-1} = \frac{8}{9}\left(\frac{\theta^2}{2} - \frac{\theta}{4} - \frac{7}{8}\right),$$

so that

$$\frac{8}{9}(\theta^2 + \theta + 1)(\theta - 1)(\frac{\theta^2}{2} - \frac{\theta}{4} - \frac{7}{8}) = 1.$$

Then

$$(\theta^2 + \theta + 1)^{-1} = \frac{8}{9}(\theta - 1)\left(\frac{\theta^2}{2} - \frac{\theta}{4} - \frac{7}{8}\right) = -\frac{2\theta^2}{3} + \frac{\theta}{3} + \frac{5}{3},$$

where we used $\theta^3 = 2\theta + 2$ again. It follows that

$$\frac{1+\theta}{1+\theta+\theta^2} = (1+\theta)\left(-\frac{2\theta^2}{3} + \frac{\theta}{3} + \frac{5}{3}\right) = -\frac{\theta^2}{3} + \frac{2\theta}{3} + \frac{1}{3}.$$

Exercise 13.1.3. Since $0^3 + 0 + 1 = 1$ and $1^1 + 1 + 1 = 1$ in $\mathbb{F}_2$, it follows that $x^3 + x + 1$ is irreducible over $\mathbb{F}_2$. Since θ is root of $x^3 + x + 1$, we have $\theta^3 = -\theta - 1 = \theta + 1$. Hence, the powers of θ in $\mathbb{F}_2(\theta)$ are

$$\theta, \ \ \theta^2, \ \ \theta^3 = \theta + 1, \ \ \theta^4 = \theta^2 + \theta, \ \ \theta^5 = \theta^2 + \theta + 1, \ \ \theta^6 = \theta^2 + 1, \ \text{ and } \ \theta^7 = 1.$$

Exercise 13.1.4. Denote this map by φ. Then

$$\varphi(a + b\sqrt{2} + c + d\sqrt{2}) = a + c - b\sqrt{2} - d\sqrt{2} = \varphi(a + b\sqrt{2}) + \varphi(c + d\sqrt{2})$$

and

$$\begin{aligned}\varphi((a + b\sqrt{2}) \cdot (c + d\sqrt{2})) &= \varphi(ac + 2bd + (ad + bc)\sqrt{2}) \\ &= ac + 2bd - (ad + bc)\sqrt{2} \\ &= (a - b\sqrt{2})(c - d\sqrt{2}) \\ &= \varphi(a + b\sqrt{2})\varphi(c + d\sqrt{2}),\end{aligned}$$

so φ is an homomorphism. If $\varphi(a+b\sqrt{2}) = \varphi(c+d\sqrt{2})$, then $a-b\sqrt{2} = c-d\sqrt{2}$; as $\sqrt{2} \notin \mathbb{Q}$, this implies $a = b$ and $c = d$. Thus φ is injective. Furthermore, given $a+b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, we have $\varphi(a-b\sqrt{2}) = a+b\sqrt{2}$, so φ is surjective. Therefore φ is an isomorphism of $\mathbb{Q}(\sqrt{2})$ with itself.

Exercise 13.1.5. Let $\alpha = p/q$ be a root of a monic polynomial $p(x) = x^n + \cdots + a_1x + a_0$ over $\mathbb{Z}$, with $\gcd(p,q) = 1$. Then

$$\left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \cdots + a_1\frac{p}{q} + a_0 = 0,$$

so that

$$q(a_{n-1}p^{n-1} + \cdots + a_1pq^{n-2} + a_0q^{n-1}) = -p^n.$$

Thus, every prime that divides q must divide p^n as well, so divides p. Since $\gcd(p,q) = 1$, there is no prime dividing q, hence $q = \pm 1$. The result follows.

Exercise 13.1.6. This is straightforward. If

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0,$$

then

$$\begin{aligned}
&(a_n\alpha)^n + a_{n-1}(a_n\alpha)^{n-1} + a_na_{n-2}(a_n\alpha)^{n-2} + \cdots + a_n^{n-2}a_1(a_n\alpha) + a_n^{n-1}a_0 \\
&= a_n^n\alpha^n + a_n^{n-1}a_{n-1}\alpha^{n-1} + a_n^{n-1}a_{n-2}\alpha^{n-2} + \cdots + a_n^{n-1}a_1\alpha + a_n^{n-1}a_0 \\
&= a_n^{n-1}(a_n\alpha^n + a_{n-1}\alpha^{n-1} + a_{n-2}\alpha^{n-2} + \cdots + a_1\alpha + a_0) = 0.
\end{aligned}$$

Exercise 13.1.7. Suppose $x^3 - nx + 2$ is reducible; then it must have a linear factor, hence a root. By the Rational Root Theorem, if α is a root of $x^3 - nx + 2$, then α must divide 2, so that $\alpha = \pm 1, \pm 2$. If $\alpha = -1$ or 2, then $n = 3$; if $\alpha = -1$, then $n = 1$; and if $\alpha = 2$, then $n = 5$. Therefore $x^3 - nx + 2$ is irreducible for $n \neq -1, 3, 5$.

Exercise 13.1.8. We subdivide this exercise in cases and subcases.

If $x^5 - ax - 1$ is reducible then it has a root (linear factor) or is a product of two irreducible polynomials of degrees 2 and 3 respectively.

Case 1. If $x^5 - ax - 1$ has a root, then, by the Rational Root Theorem, it must be $\alpha = \pm 1$. If $\alpha = 1$ is a root, then $a = 0$. If $\alpha = -1$ is a root, then $a = 2$.

Case 2. Now, assume that there exist $f(x)$ and $g(x)$ irreducible monic polynomials over $\mathbb{Z}$ of degrees 2 and 3 respectively, such that $x^5 - ax - 1 = f(x)g(x)$. Write $f(x) = x^2 + bx + c$ and $g(x) = x^3 + rx^2 + sx + t$, where $b, c, r, s, t \in \mathbb{Z}$. Then

$$\begin{aligned}
x^5 - ax - 1 &= (x^2 + bx + c)(x^3 + rx^2 + sx + t) \\
&= x^5 + (b+r)x^4 + (br + c + s)x^3 + (bs + cr + t)x^2 + (bt + cs) + tc.
\end{aligned}$$

Equating coefficients leads to

$$\begin{aligned} b + r &= 0, \\ br + c + s &= 0, \\ bs + cr + t &= 0, \\ bt + cs &= -a, \\ ct &= -1. \end{aligned}$$

From $ct = -1$ we deduce $(c, t) = (-1, 1)$ or $(c, t) = (1, -1)$, which gives us two cases.

Case 2.1. First suppose $(c, t) = (-1, 1)$. Then the system of equations reduces to

$$\begin{aligned} b + r &= 0, \\ br - 1 + s &= 0, \\ bs - r + 1 &= 0, \\ b - s &= -a. \end{aligned}$$

Put $b = -r$ into the second and third equations to obtain $-r^2 - 1 + s = 0$ and $-rs - r + 1 = 0$, that is, $r^2 + 1 - s = 0$ and $rs + r - 1 = 0$. Adding these last two equations we obtain $r^2 + rs + r - s = 0$. Thus $r^2 + rs + r + s = 2s$, so that $(r + 1)(r + s) = 2s$. Now, from $r^2 + 1 - s = 0$ we have $r^2 = s - 1$, so $r^2 + rs + r - s = 0$ becomes $rs + r = 1$, that is, $r(s + 1) = 1$. Hence, $r = 1$ and $s = 0$, or $r = -1$ and $s = -2$. If $r = 1$ and $s = 0$, then $(r + 1)(r + s) = 2s$ leads to $2 = 0$, a contradiction. If $r = -1$ and $s = -2$, it leads to $0 = -4$, another contradiction.

We deduce that $(c, t) = (-1, 1)$ is impossible.

Case 2.2. Suppose that $(c, t) = (1, -1)$. The system of equations reduces to

$$\begin{aligned} b + r &= 0, \\ br + 1 + s &= 0, \\ bs + r - 1 &= 0, \\ -b + s &= -a. \end{aligned}$$

Adding the second and third equation we obtain $b(r + s) + r + s = 0$, so that $(b + 1)(r + s) = 0$. Then $b = -1$ or $r = -s$, so one more time we have two cases. If $r = -s$, then $br + 1 + s = 0$ becomes $br + 1 - r = 0$. Hence, $b = -r$ and $br + 1 - r = 0$ gives $r^2 + r - 1 = 0$. By the Rational Root Theorem, this equation has no roots in $\mathbb{Z}$. Since $r \in \mathbb{Z}$, we have a contradiction. Now suppose $b = -1$. From $b = -r$ we obtain $r = 1$; thus, from $br + 1 + s = 0$ we obtain $s = 0$. Finally, from $-b + s = -a$ it follows that $a = -1$. Therefore, we find the consistent solution $(b, c, r, s, t) = (-1, 1, 1, 0, -1)$ and the factorisation

$$x^5 - ax - 1 = (x^2 + bx + c)(x^3 + rx^2 + sx + t) = (x^2 - x + 1)(x^3 + x^2 - 1).$$

13.2 Algebraic Extensions

Exercise 13.2.1. Since the characteristic of $\mathbb{F}$ is p, its prime subfield is (isomorphic to) $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Then $\mathbb{F}$ is a vector space over $\mathbb{F}_p$. Since $\mathbb{F}$ is finite, we have $[\mathbb{F} : \mathbb{F}_p] = n$ for some $n \in \mathbb{Z}^+$. It follows that

$$|\mathbb{F}| = |\mathbb{F}_p|^{[\mathbb{F}:\mathbb{F}_p]} = p^n.$$

Exercise 13.2.2. Note that g and h are irreducible over both $\mathbb{F}_2$ and $\mathbb{F}_3$. If θ is a root of g, then $\mathbb{F}_2(\theta) \cong \mathbb{F}_2/(g(x))$ has 4 elements and $\mathbb{F}_3(\theta) \cong \mathbb{F}_3/(g(x))$ has 9 elements. Furthermore, is θ_2 if a root of h, then $\mathbb{F}_2(\theta_2) \cong \mathbb{F}_2/(h(x))$ has 8 elements and $\mathbb{F}_3(\theta_2) \cong \mathbb{F}_3/(h(x))$ has 27 elements.

The multiplication table for $\mathbb{F}_2/(g(x))$ is

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	x
$x+1$	0	$x+1$	x	x

The multiplication table for $\mathbb{F}_3/(g(x))$ is

$\cdot$	0	1	2	x	$x+1$	$x+2$	$2x$	$2x{+}1$	$2x{+}2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$x+1$	$x+2$	$2x$	$2x{+}1$	$2x{+}2$
2	0	2	1	$2x$	$2x{+}2$	$2x{+}1$	x	$x+2$	$x+1$
x	0	x	$2x$	$2x{+}1$	1	$x+1$	$x+2$	$2x{+}2$	2
$x+1$	0	$x+1$	$2x{+}2$	1	$x+2$	$2x$	2	x	$2x{+}1$
$x+2$	0	$x+2$	$2x{+}1$	$x+1$	$2x$	2	$2x{+}2$	1	x
$2x$	0	$2x$	x	$x+2$	2	$2x{+}2$	$2x{+}1$	$x+1$	1
$2x{+}1$	0	$2x{+}1$	$x+2$	$2x{+}2$	x	1	$x+1$	2	$2x$
$2x{+}2$	0	$2x{+}2$	$x+1$	2	$2x{+}1$	x	1	$2x$	$x+2$

In both cases, x is a generator of the cyclic group of non-zero elements.

Exercise 13.2.3. Since $1+i \notin \mathbb{Q}$, its minimal polynomial is of degree at least 2. We try conjugation, and obtain

$$(x - (1 + i))(x - (1 - i)) = x^2 - 2x + 2,$$

which is irreducible by Eisenstein with $p = 2$. Therefore, the minimal polynomial of $1 + i$ over $\mathbb{Q}$ is $x^2 - 2x + 2$.

Exercise 13.2.4. First, note that $(2 + \sqrt{3})^2 = 4 + 4\sqrt{3} + 3 = 7 + 4\sqrt{3}$. Let $\theta = 2 + \sqrt{3}$. Then $\theta^2 - 4\theta = 7 + 4\sqrt{3} - 8 - 4\sqrt{3} = -1$, so θ is a root of $x^2 - 4x + 1$. Moreover, $x^2 - 4x + 1$ is irreducible over $\mathbb{Q}$ (because $\theta \notin \mathbb{Q}$), so $x^2 - 4x + 1$ is the minimal polynomial of $2 + \sqrt{3}$. Thus $2 + \sqrt{3}$ has degree 2 over $\mathbb{Q}$.

Now let $\alpha = \sqrt[3]{2}$ and $\beta = 1 + \alpha + \alpha^2$. Then $\beta \in \mathbb{Q}(\alpha)$, so $\mathbb{Q} \subset \mathbb{Q}(\beta) \subset \mathbb{Q}(\alpha)$. We have $[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\beta)][\mathbb{Q}(\beta) : \mathbb{Q}]$. Note that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ since α has minimal polynomial $x^3 - 2$ over $\mathbb{Q}$, so $[\mathbb{Q}(\beta) : \mathbb{Q}]$ is either 1 or 3. For the sake of a contradiction suppose $[\mathbb{Q}(\beta) : \mathbb{Q}] = 1$, so that $\beta \in \mathbb{Q}$. Then

$$\beta^2 = (1 + \alpha + \alpha^2)^2 = 1 + 2\alpha + 3\alpha^2 + 2\alpha^3 + \alpha^4 = 5 + 4\alpha + 3\alpha^2,$$

where we used $\alpha^3 = 2$, and therefore

$$\beta^2 - 3\beta = 5 + 4\alpha + 3\alpha^2 - 3(1 + \alpha + \alpha^2) = 2 + \alpha.$$

But then $\alpha = -\beta^2 + 3\beta - 2 \in \mathbb{Q}(\beta) = \mathbb{Q}$, a contradiction. It follows that $[\mathbb{Q}(\beta) : \mathbb{Q}] = 3$.

Exercise 13.2.5. Since the polynomials have degree 3, if they were reducible they would have a linear factor, hence a root in F. Note that every element of F has the form $a + bi$, where $a, b \in \mathbb{Q}$. The roots of $x^3 - 2$ are $\sqrt[3]{2}, \zeta\sqrt[3]{2}$ and $\zeta^2\sqrt[3]{2}$, where ζ is the primitive 3rd root of unity, i.e., $\zeta = \exp(2\pi i/3) = \cos(2\pi/3) + i\sin(2\pi/3) = -\frac{1}{2} + \frac{\sqrt{3}}{2}$. Since $\sqrt{3} \notin \mathbb{Q}$, none of these elements belong to F, so $x^3 - 2$ is irreducible over F. Similarly, the roots of $x^3 - 3$ are $\sqrt[3]{3}, \zeta\sqrt[3]{3}$ and $\zeta^2\sqrt[3]{3}$, and by the same argument none of these elements belong to F. Hence $x^3 - 3$ is irreducible over F.

Exercise 13.2.6. We have to prove that $F(\alpha_1, \ldots, \alpha_n)$ is the smallest field containing $F(\alpha_1), \ldots, F(\alpha_n)$. Clearly $F(\alpha_i) \subset F(\alpha_1, \ldots, \alpha_n)$ for all $1 \leq i \leq n$. Now let K be a field such that $F(\alpha_i) \subset K$ for all i. If θ is an element of $F(\alpha_1, \ldots, \alpha_n)$, it has the form $\theta = a_1\alpha_1 + \cdots + a_n\alpha_n$, where $a_1, \ldots, a_n \in F$. As every $a_i\alpha_i$ belongs to K, we have $\theta \in K$. Thus $F(\alpha_1, \ldots, \alpha_n) \subset K$. It follows that $F(\alpha_1, \ldots, \alpha_n)$ contains all of the $F(\alpha_i)$ and is contained in every field containing all of the $F(\alpha_i)$, so $F(\alpha_1, \ldots, \alpha_n)$ is the composite of the fields $F(\alpha_1), F(\alpha_2), \ldots, F(\alpha_n)$.

Exercise 13.2.7. Since $\sqrt{2} + \sqrt{3}$ is an element of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, clearly $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$. On the other hand, consider $\theta = \sqrt{2} + \sqrt{3}$. Then $\theta^2 = 5 + 2\sqrt{6}$, and $\theta^3 = 11\sqrt{2} + 9\sqrt{3}$, so

$$\sqrt{2} = \frac{1}{2}(\theta^3 - 9\theta) \quad \text{and} \quad \sqrt{3} = \frac{1}{2}(11\theta - \theta^3).$$

Therefore $\sqrt{2} \in \mathbb{Q}(\theta)$ and $\sqrt{3} \in \mathbb{Q}(\theta)$, so $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subset \mathbb{Q}(\sqrt{2} + \sqrt{3})$. It follows that $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, so that $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$.

We also have

$$\theta^4 - 10\theta^2 = (49 + 20\sqrt{6}) - 10(5 + 2\sqrt{6}) = -1, \quad \text{so} \quad \theta^4 - 10\theta^2 + 1 = 0.$$

Since $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 4$, the polynomial $x^4 - 10x^2 + 1$ is irreducible over $\mathbb{Q}$, and is satisfied by $\sqrt{2} + \sqrt{3}$.

Exercise 13.2.8. The elements of $F(\sqrt{D_1}, \sqrt{D_2})$ can be written as

$$a + b\sqrt{D_1} + c\sqrt{D_2} + d\sqrt{D_1 D_2}, \quad \text{where } a, b, c, d \in F.$$

We have
$$[F(\sqrt{D_1},\sqrt{D_2}) : F] = [F(\sqrt{D_1},\sqrt{D_2}) : F(\sqrt{D_1})][F(\sqrt{D_1}) : F].$$
Since $[F(\sqrt{D_1}) : F] = 2$, $[F(\sqrt{D_1},\sqrt{D_2}) : F]$ can be either 2 or 4. Now $[F(\sqrt{D_1},\sqrt{D_2}) : F] = 2$ if and only if $[F(\sqrt{D_1},\sqrt{D_2}) : F(\sqrt{D_1})] = 1$, and that occurs exactly if $x^2 - D_2$ is reducible in $F(\sqrt{D_1})$ (i.e., if $\sqrt{D_2} \in F(\sqrt{D_1})$), that is, if there exists $a, b \in F$ such that
$$(a + b\sqrt{D_1})^2 = D_2, \quad \text{so that} \quad a^2 + 2ab\sqrt{D_1} + b^2 D_1^2 = D_2.$$
Note that $ab = 0$, as $ab \neq 0$ implies $\sqrt{D_1} \in F$, contrary to the assumption. Then $a = 0$ or $b = 0$. If $b = 0$, then D_2 is a square in F, contrary to the assumption. If $a = 0$, then $b^2 D_1 = D_2$, and thus $D_1 D_2 = (\frac{D_2}{b})^2$, so $D_1 D_2$ is a square in F. Thus $x^2 - D_2$ is reducible in $F(\sqrt{D_1})$ if and only if $D_1 D_2$ is a square in F. The result follows.

Exercise 13.2.9. Suppose $\sqrt{a+\sqrt{b}} = \sqrt{m} + \sqrt{n}$ for some $m, n \in F$, so that $a + \sqrt{b} = m + n + 2\sqrt{mn}$. Since b is not a square in F, this means $\sqrt{b} = 2\sqrt{mn}$. We also have $\sqrt{a+\sqrt{b}} - \sqrt{n} = \sqrt{m}$, so
$$\sqrt{b} = 2\sqrt{n}(\sqrt{a+\sqrt{b}} - \sqrt{n}).$$
Hence,
$$\begin{aligned} & \sqrt{b} = 2\sqrt{n(a+\sqrt{b})} - 2n \\ \Rightarrow \quad & (\sqrt{b} + 2n)^2 = 4n(a+\sqrt{b}) \\ \Rightarrow \quad & b + 4n\sqrt{b} + 4n^2 = 4n(a+\sqrt{b}) \\ \Rightarrow \quad & b + 4n^2 - 4na = 0 \\ \Rightarrow \quad & n = \frac{4a \pm \sqrt{16a^2 - 16b}}{8} \\ \Rightarrow \quad & \sqrt{a^2 - b} = \pm \frac{2n}{a}. \end{aligned}$$
Therefore, since a and n belong to F, so does $\sqrt{a^2 - b}$.

Conversely, assume that $a^2 - b$ is a square in F, so that $\sqrt{a^2 - b} \in F$. We prove that there exist $m, n \in F$ such that $\sqrt{a+\sqrt{b}} = \sqrt{m} + \sqrt{n}$. Consider
$$m = \frac{a + \sqrt{a^2 - b}}{2} \quad \text{and} \quad n = \frac{a - \sqrt{a^2 - b}}{2}.$$
Note that m and n belong to F as $\operatorname{char}(F) \neq 2$. We claim $\sqrt{a+\sqrt{b}} = \sqrt{m} + \sqrt{n}$. Indeed, we have
$$m = \frac{(a+\sqrt{b}) + 2\sqrt{a^2 - b} + (a - \sqrt{b})}{4} = \left(\frac{\sqrt{a+\sqrt{b}} + \sqrt{a - \sqrt{b}}}{2}\right)^2,$$

and

$$n = \frac{(a+\sqrt{b}) - 2\sqrt{a^2-b} + (a-\sqrt{b})}{4} = \left(\frac{\sqrt{a+\sqrt{b}} - \sqrt{a-\sqrt{b}}}{2}\right)^2.$$

Thus

$$\sqrt{m} = \frac{\sqrt{a+\sqrt{b}} + \sqrt{a-\sqrt{b}}}{2} \quad \text{and} \quad \sqrt{n} = \frac{\sqrt{a+\sqrt{b}} - \sqrt{a-\sqrt{b}}}{2},$$

so

$$\sqrt{m} + \sqrt{n} = \frac{\sqrt{a+\sqrt{b}} + \sqrt{a-\sqrt{b}}}{2} + \frac{\sqrt{a+\sqrt{b}} - \sqrt{a-\sqrt{b}}}{2} = \sqrt{a+\sqrt{b}},$$

as claimed.

Finally, we use this to determine when is the field $\mathbb{Q}(\sqrt{a+\sqrt{b}})$, $a, b \in \mathbb{Q}$, biquadratic over $\mathbb{Q}$. If $a^2 - b$ is a square in $\mathbb{Q}$ and b is not, we have $\mathbb{Q}(\sqrt{a+\sqrt{b}}) = \mathbb{Q}(\sqrt{m}+\sqrt{n}) = \mathbb{Q}(\sqrt{m}, \sqrt{n})$, so by Exercise 13.2.8, $\mathbb{Q}(\sqrt{a+\sqrt{b}})$ is biquadratic over $\mathbb{Q}$ when $a^2 - b$ is a square in $\mathbb{Q}$ and none of b, m, n or mn is a square in $\mathbb{Q}$. Since

$$mn = \frac{a+\sqrt{a^2-b}}{2}\frac{a-\sqrt{a^2-b}}{2} = \frac{b}{4},$$

mn is never a square when b is not. Thus, $\mathbb{Q}(\sqrt{a+\sqrt{b}})$ is biquadratic over $\mathbb{Q}$ exactly when $a^2 - b$ is a square in $\mathbb{Q}$ and none of b, m or n is a square in $\mathbb{Q}$.

Exercise 13.2.10. Note that $\sqrt{3+2\sqrt{2}} = \sqrt{3+\sqrt{8}}$. Recalling Exercise 13.2.9 with $a = 3$ and $b =$ 8,we have that $a^2 - b = 9 - 8 = 1$ is a square in $\mathbb{Q}$ and $b = 8$ is not. Hence, we find ($m = 2$ and $n = 1$ from Exercise 13.2.9) $\sqrt{3+\sqrt{8}} = \sqrt{2}+1$. Therefore, $\mathbb{Q}(\sqrt{3+2\sqrt{2}}) = \mathbb{Q}(\sqrt{2})$ and the degree of the extension $\mathbb{Q}(\sqrt{3+2\sqrt{2}})$ over $\mathbb{Q}$ is 2.

Exercise 13.2.11. (a) First, note that the conjugation map $a+bi \to a-bi$ is an automorphism of $\mathbb{C}$, so it takes squares roots to square roots. Furthermore, it maps the first quadrant onto the fourth (and reciprocally). Since $\sqrt{3+4i}$ is the square root of $3+4i$ in the first quadrant, its conjugate is the square of root of $3-4i$ in the fourth quadrant, so is $\sqrt{3-4i}$. Hence $\sqrt{3+4i}$ and $\sqrt{3-4i}$ are conjugates to each other. Now we use Exercise 13.2.9. Note that $\sqrt{3+4i} = \sqrt{3+\sqrt{-16}}$. With $a = 3$ and $b = -16$, we have $a^2 - b = 25$ is a square in $\mathbb{Q}$ and $b = -16$ is not. Hence, we find $m = 1$ and $n = -4$ and thus $\sqrt{3+4i} = 1 + \sqrt{-4} = 1 + 2i$. Furthermore, we find $\sqrt{3-4i} = 1 - 2i$. Therefore, $\sqrt{3+4i} + \sqrt{3-4i} = 4$, i.e., $\sqrt{3+4i} + \sqrt{3-4i} \in \mathbb{Q}$.

(b) Let $\theta = \sqrt{1+\sqrt{-3}} + \sqrt{1-\sqrt{-3}}$. Then

$$\theta^2 = (\sqrt{1+\sqrt{-3}} + \sqrt{1-\sqrt{-3}})^2 = (1+\sqrt{-3}) + (2\sqrt{1+3}) + (1-\sqrt{-3}) = 6.$$

Since $x^2 - 6$ is irreducible over $\mathbb{Q}$ (Eisenstein with $p = 2$), it follows that θ has degree 2 over $\mathbb{Q}$.

Exercise 13.2.12. Let E be a subfield of K containing F. Then

$$[K:F] = [K:E][E:F] = p.$$

Since p is prime, either $[K:E] = 1$ or $[E:F] = 1$. The result follows.

Exercise 13.2.13. Note that, for all $1 \leq k \leq n$, $[\mathbb{Q}(\alpha_1, \dots, \alpha_k) : \mathbb{Q}(\alpha_1, \dots, \alpha_{k-1})]$ is either 1 or 2. Then $[F : \mathbb{Q}] = 2^m$ for some $m \in \mathbb{N}$. Suppose $\sqrt[3]{2} \in F$. Then $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subset F$, so $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$ divides $[F : \mathbb{Q}]$, that is, 3 divides 2^m, a contradiction. Thus $\sqrt[3]{2} \notin F$.

Exercise 13.2.14. Since $\alpha^2 \in F(\alpha)$, clearly $F(\alpha^2) \subset F(\alpha)$. Thus we have to prove $\alpha \in F(\alpha^2)$. For this purpose, consider the polynomial $p(x) = x^2 - \alpha^2$, so that $p(\alpha) = 0$. Note that $\alpha \in F(\alpha^2)$ if and only if $p(x)$ is reducible in $F(\alpha^2)$. For the sake of a contradiction, suppose $p(x)$ is irreducible in $F(\alpha^2)$, so that $[F(\alpha) : F(\alpha^2)] = 2$. Then

$$[F(\alpha) : F] = [F(\alpha) : F(\alpha^2)][F(\alpha^2) : F] = 2[F(\alpha^2) : F],$$

so $[F(\alpha) : F]$ is even, a contradiction. Therefore, $p(x)$ is reducible in $F(\alpha^2)$ and $\alpha \in F(\alpha^2)$.

Exercise 13.2.15. We follow the hint. Suppose there exists a counterexample. Let α be of minimal degree such that $F(\alpha)$ is not formally real and α having minimal polynomial f of odd degree, say $\deg f = 2k + 1$ for some $k \in \mathbb{N}$. Since $F(\alpha)$ is not formally real, -1 can be expressed as a sum of squares in $F(\alpha) \cong F[x]/(f(x))$. Then, there exist polynomials $p_1(x), \dots, p_m(x), g(x)$ such that

$$-1 + f(x)g(x) = (p_1(x))^2 + \cdots + (p_m(x))^2.$$

As every element in $F[x]/((f(x))$ can be written as a polynomial in α with degree less than $\deg f$, we have $\deg p_i < 2k + 1$ for all i. Thus, the degree in the right-hand side of the equation is less than $4k+1$, so $\deg g < 2k+1$ as well. From the equation $-1+f(x)g(x) = (p_1(x))^2+\cdots+(p_m(x))^2$, for proving that the degree of g is odd it suffices to prove that degree of $(p_1(x))^2 + \cdots + (p_m(x))^2$ is even. Let d be the maximal degree over all p_i, we prove that x^{2d} is the leading term of $(p_1(x))^2 + \cdots + (p_m(x))^2$. Note that x^{2d} is a sum of squares (of the leading coefficients of the p_i's of maximal degree). Now, since F is formally real, 0 cannot be expressed as a sum of squares in F. (Indeed, if $\sum_{i=1}^{l} a_i^2 = 0$, then $\sum_{i=1}^{l-1} (a_i/a_l)^2 = -1$.) Thus $x^{2d} \neq 0$, so the degree of $(p_1(x))^2 + \cdots + (p_m(x))^2$ is $2d$, and therefore the degree of g is odd. Then g must contain an irreducible factor of odd degree, say $h(x)$. Since $\deg g < \deg f$, we have $\deg h < \deg f$ as well. Let β be a root of $h(x)$, hence a root of $g(x)$. Then

$$-1 + h(x)\frac{f(x)g(x)}{h(x)} = (p_1(x))^2 + \cdots + (p_m(x))^2,$$

so -1 is a square in $F[x]/((h(x)) \cong F(\beta)$, which means that $F(\beta)$ is not formally real. It follows that β is a root of the odd degree polynomial h such that $F(\beta)$ is not formally real. Since $\deg h < \deg f$, this contradicts the minimality of α. The result follows.

Exercise 13.2.16. Let $r \in R$ be non-zero. Since r is algebraic over F, there exists an irreducible polynomial $p(x) = a_0 + a_1 x + \cdots + x^n \in F[x]$ such that $p(r) = 0$. Note that $a_0 \neq 0$ since p is irreducible. Then $r^{-1} = -a_0^{-1}(r^{n-1} + \cdots + a_1)$. Since $a_i \in F \subset R$ and $r \in R$, we have $r^{-1} \in R$.

Exercise 13.2.17. Let $p(x)$ be an irreducible factor of $f(g(x))$ of degree m. Let α be a root of $p(x)$. Since p is irreducible, it follows that $[F(\alpha) : F] = \deg p(x) = m$. Now, since $p(x)$ divides $f(g(x))$, we have $f(g(\alpha)) = 0$ and thus $g(\alpha)$ is a root of $f(x)$. Since f is irreducible, this means $n = [F(g(\alpha)) : F]$. Note that $F(g(\alpha)) \subset F(\alpha)$. Then

$$m = [F(\alpha) : F] = [F(\alpha) : F(g(\alpha))][F(g(\alpha)) : F] = [F(\alpha) : F(g(\alpha))] \cdot n,$$

so n divides m, that is, $\deg f$ divides $\deg p$.

Exercise 13.2.18. (a) We follow the hint. Since $k[t]$ is an unique factorisation domain and $k(t)$ is its field of fractions, it follows from the Gauss Lemma that $P(X) - tQ(X)$ is irreducible in $k((t))[X]$ if and only if it is irreducible in $(k[t])[X]$. Note that $(k[t])[X] = (k[X])[t]$. Since $P(X) - tQ(X)$ is linear in $(k[X])[t]$, it is clearly irreducible in $(k[X])[t]$ (i.e., in $(k[t])[X]$), hence in $(k(t))[X]$. Thus $P(X) - tQ(X)$ is irreducible in $k(t)$. Finally, x is clearly a root of $P(X) - tQ(X)$ since $P(x) - tQ(x) = P(x) - \dfrac{P(x)}{Q(x)}Q(x) = P(x) - P(x) = 0$.

(b) Let $n = \max\{\deg P(x), \deg Q(x)\}$. Write

$$P(x) = a_n x^n + \cdots + a_1 x + a_0 \quad \text{and} \quad Q(x) = b_n x^n + \cdots + b_1 x + b_0,$$

where $a_i, b_i \in k$ for all i, so at least one of a_n or b_n is non-zero. The degree of $P(X) - tQ(X)$ is clearly $\leq n$, we shall prove it is precisely n. If either a_n or b_n is zero then clearly $\deg\,(P(X) - tQ(X)) = n$, so assume $a_n, b_n \neq 0$. Then $a_n, b_n \in k$, but $t \notin k$, so it cannot be that $a_n = tb_n$. Thus $(a_n - tb_n)X^n \neq 0$ and the degree of $P(X) - tQ(X)$ is precisely n.

(c) Since $P(X) - tQ(X)$ is irreducible over $k(t)$ and x is a root by part (a), it follows that $[k(x) : k(t)] = \deg P(X) - tQ(X)$, and this degree equals $\max\{\deg P(x), \deg Q(x)\}$ by part (b).

Exercise 13.2.19. (a) Fix α in K. Since K is (in particular) a commutative ring, we have $\alpha(a+b) = \alpha a + \alpha b$ and $\alpha(\lambda a) = \lambda(\alpha a)$ for all $a, b, \lambda \in K$. If, in particular, $\lambda \in F$, we have the result.

(b) Fix a basis for K as a vector space over F. By part (a), for every $\alpha \in K$ we can associate an F-linear transformation T_α of K. Denote by $\left(T_\alpha\right)$ the matrix of T_α with respect to the basis previously fixed. Then define $\varphi \colon K \to M_n(F)$ by $\varphi(\alpha) = \left(T_\alpha\right)$. We claim that φ is an isomorphism onto its image. Indeed, if $\alpha, \beta \in K$, then $T_{(\alpha+\beta)}(k) = (\alpha + \beta)(k) = \alpha k + \beta k = T_\alpha(k) + T_\beta(k)$ for every $k \in K$, so $T_{(\alpha+\beta)} = T_\alpha + T_\beta$. We also have $T_{(\alpha\beta)}(k) = (\alpha\beta)(k) = \alpha(\beta k) = T_\alpha T_\beta(k)$ for every $k \in K$, so $T_{(\alpha\beta)} = T_\alpha T_\beta$. Thus $\varphi(\alpha + \beta) = \varphi(\alpha) + \varphi(\beta)$ and $\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$ (since the basis is fixed), so φ is an homomorphism. Now, if $\varphi(\alpha) = \varphi(\beta)$, then $\alpha k = \beta k$ for every $k \in K$, so letting $k = 1$ we find that φ is injective. Therefore, $\varphi(K)$ is isomorphic to a subfield of $M_n(F)$, so the ring $M_n(F)$ contains an isomorphic copy of every extension of F of degree $\leq n$.

Exercise 13.2.20. The characteristic polynomial of A is $p(x) = \det(Ix - A)$. For every $k \in K$, we have $(I\alpha - A)k = \alpha k - Ak = \alpha k - \alpha k = 0$, so $\det(I\alpha - A) = 0$ in K. Therefore $p(\alpha) = 0$.

Now, consider the field $\mathbb{Q}(\sqrt[3]{2})$ with basis $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ over $\mathbb{Q}$. Denote the elements of this basis by $e_1 = 1$, $e_2 = \sqrt[3]{2}$ and $e_3 = \sqrt[3]{4}$. Let $\alpha = \sqrt[3]{2}$ and $\beta = 1 + \sqrt[3]{2} + \sqrt[3]{4}$. Then $\alpha(e_1) = e_2$, $\alpha(e_2) = e_3$ and $\alpha(e_3) = 2e_1$. We also have $\beta(e_1) = e_1 + e_2 + e_3$, $\beta(e_2) = 2e_1 + e_2 + e_3$ and $\beta(e_3) = 2e_1 + 2e_2 + e_3$. Thus, the associated matrices of the their linear transformations are, respectively,

$$A_\alpha = \begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \quad \text{and} \quad A_\beta = \begin{pmatrix} 1 & 2 & 2 \\ 1 & 1 & 2 \\ 1 & 1 & 1 \end{pmatrix}.$$

The characteristic polynomial of A_α is $x^3 - 2$, hence is the monic polynomial of degree 3 satisfied by $\alpha = \sqrt[3]{2}$. Furthermore, the characteristic polynomial of A_β is $x^3 - 3x^2 - 3x - 1$, hence is the monic polynomial of degree 3 satisfied by $\beta = 1 + \sqrt[3]{2} + \sqrt[3]{4}$.

Exercise 13.2.21. The matrix of the linear transformation "multiplication by α" on K is found by acting of α in the basis $1, \sqrt{D}$. We have $\alpha(1) = \alpha = a + b\sqrt{D}$ and $\alpha(\sqrt{D}) = a\sqrt{D} + bD$. Hence the matrix is $\begin{pmatrix} a & bD \\ b & a \end{pmatrix}$. Now let $\varphi \colon K \longrightarrow M_2(\mathbb{Q})$ be defined by $\varphi(a + b\sqrt{D}) = \begin{pmatrix} a & bD \\ b & a \end{pmatrix}$.

We have

$$\varphi(a + b\sqrt{D} + c + d\sqrt{D}) = \begin{pmatrix} a+c & (b+d)D \\ b+d & a+c \end{pmatrix} = \begin{pmatrix} a & bD \\ b & a \end{pmatrix} + \begin{pmatrix} c & dD \\ d & c \end{pmatrix} = \varphi(a + b\sqrt{D}) + \varphi(c + d\sqrt{D}),$$

and

$$\begin{aligned} \varphi((a + b\sqrt{D}) \cdot (c + d\sqrt{D})) = \begin{pmatrix} ac + bdD & (ad+bc)D \\ ad + bc & ac + bdD \end{pmatrix} &= \begin{pmatrix} a & bD \\ b & a \end{pmatrix} \cdot \begin{pmatrix} c & dD \\ d & c \end{pmatrix} \\ &= \varphi(a + b\sqrt{D})\varphi(c + d\sqrt{D}), \end{aligned}$$

so φ is an homomorphism. Since K is a field, its only ideals are $\{0\}$ and K, so $\ker(\varphi)$ is either trivial or all of K. But $\varphi(K)$ is clearly non-zero, so $\ker(\varphi) \neq K$ and thus $\ker(\varphi) = \{0\}$. Hence φ is injective. It follows that φ is an isomorphism of K with a subfield of $M_2(\mathbb{Q})$.

Exercise 13.2.22. Define $\varphi \colon K_1 \times K_2 \longrightarrow K_1K_2$ by $\varphi(a, b) = ab$. We prove that φ is F-bilinear. Let $a, a_1, a_2 \in K$ and $b, b_1, b_2 \in K_2$. Then

$$\varphi((a_1, b) + (a_2, b)) = \varphi(a_1 + a_2, b) = (a_1 + a_2)b = a_1b + a_2b = \varphi(a_1, b) + \varphi(a_2, b),$$

and

$$\varphi((a,_1 b) + (a, b_2)) = \varphi(a, b_1 + b_2) = a(b_1 + b_2) = ab_1 + ab_1 = \varphi(a, b_1) + \varphi(a, b_2).$$

We also have, for $r \in F$, $\varphi(ar, b) = (ar)b = a(rb) = \varphi(rb)$. Thus φ is a F-bilinear map, so it induces an F-algebra homomorphism $\Phi : K_1 \otimes_F K_2 \longrightarrow K_1K_2$. We shall use Φ to prove both directions. Note that $K_1 \otimes_F K_2$ have dimension $[K_1 : F][K_2 : F]$ as a vector space over F.

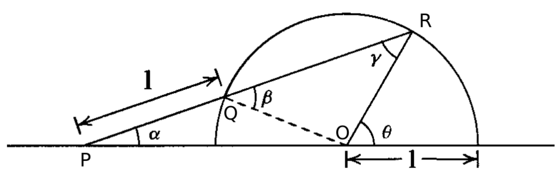
First, we assume $[K_1K_2 : F] = [K_1 : F][K_2 : F]$ and shall prove that $K_1 \otimes_F K_2$ is a field. In this case $K_1 \otimes_F K_2$ and K_1K_2 have the same dimension over F. Let $L = \Phi(K_1 \otimes_F K_2)$. We claim $L = K_1K_2$, i.e. Φ is surjective. Note that L contains K_1 and K_2. Since L is a subring of K_1K_2 containing K_1 (or K_2), it follows that L is a field (Exercise 13.2.16). Hence L is a field containing both K_1 and K_2, and since K_1K_2 is the smallest such field (by definition), we have $L = K_1K_2$. So Φ is surjective, as claimed. It follows that Φ is an F-algebra surjective homomorphism between F-algebras of the same dimension, hence is an isomorphism. Thus, $K_1 \otimes_F K_2$ is a field.

Now assume that $K_1 \otimes_F K_2$ is a field. In this case Φ is a field homomorphism, so it either injective or trivial. It is clearly non-trivial since $\Phi(1 \otimes 1) = 1$, so it must be injective. Hence, $[K_1 : F][K_2 : F] \leq [K_1K_2 : F]$. As we already have $[K_1K_2 : F] \leq [K_1 : F][K_2 : F]$ (by Proposition 21 in the book), the equality follows.

13.3 Classical Straightedge and Compass Constructions

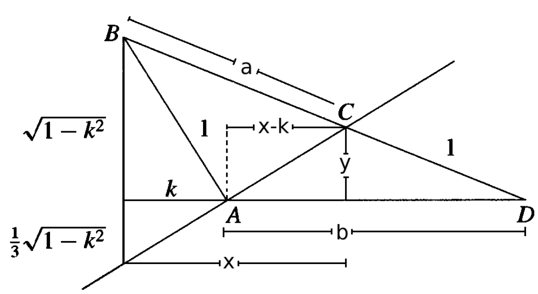
Exercise 13.3.1. Suppose that the 9-gon is constructible. It has angles of 40°. Since we can bisect an angle by straightedge and compass, the angle of 20° would be constructible. But then $\cos 20°$ and $\sin 20°$ would be constructible too, a contradiction (see proof of Theorem 24).

Exercise 13.3.2. Let O, P, Q and R be the points marked in the figure below.



Then $\alpha = \angle QPO$, $\beta = \angle RQO$, $\gamma = \angle QRO$, and θ is an exterior angle of $\triangle PRO$. Since $\triangle PQO$ is isosceles, $\alpha = \angle QPO = \angle QOP$. Since β is an exterior angle of $\triangle PQO$, it equals the sum of the two remote interior angles, i.e., equals $\angle QPO + \angle QOP$. These two angles equal α, so $\beta = 2\alpha$. Now, $\triangle QRO$ is isosceles, so $\beta = \gamma$. Finally, since θ is an exterior angle of $\triangle PRO$, it equals the sum of the two remote interior angles, which are α and γ. It follows that $\theta = \alpha + \gamma = \alpha + \beta = 3\alpha$.

Exercise 13.3.3. We follow the hint. The distances a, b, x, y and $x - k$ are marked in the figure below.



From the figure, using similar triangles for (a), (b) and (c), and Pythagoras Theorem for (d), the 4 relations are clear, that is,

$$y = \frac{\sqrt{1-k^2}}{1+a}, \quad x = a\frac{b+k}{1+a}, \quad \frac{y}{x-k} = \frac{\sqrt{1-k^2}}{3k} \quad \text{and} \quad (1-k^2)+(b+k)^2 = (1+a)^2.$$

Thus $y(1+a) = \sqrt{1-k^2} = \frac{3ky}{x-k}$, which implies $3k = (x-k)(1+a)$. From the equation for x above, we find $3k = (\frac{a(b+a)}{1+a} - k)(1+a) = a(b+k) - k(1+a)$, so $b + k = \frac{4k+ka}{a}$. Using this in the last equation and reducing, we obtain

$$\begin{aligned} & & (1-k^2)+(b+k)^2 &= (1+a)^2 \\ &\Rightarrow & (1-k^2)+\left(\frac{4k+ka}{a}\right)^2 &= (1+a)^2 \\ &\Rightarrow & a^2(1-k^2)+(4k+ka)^2 &= a^2(1+a)^2 \\ &\Rightarrow & a^2-(ka)^2+(4k)^2+8k^2a+(ka)^2 &= a^2+2a^3+a^4 \\ &\Rightarrow & a^4+2a^3-8k^2a-16k^2 &= 0. \end{aligned}$$

We let $a = 2h$ to obtain

$$h^4 + h^3 - k^2h - k^2 = 0.$$

We find $h = k^{2/3}$, so that $a = 2k^{2/3}$. Finally, from $b = \frac{4k+ka}{a} - k$ we find $b = 2k^{1/3}$. It follows that we can construct $2k^{1/3}$ and $2k^{2/3}$ using Conway's construction.

Exercise 13.3.4. Let $p(x) = x^3+x^2-2x-1$ and $\alpha = 2\cos(2\pi/7)$. By the Rational Root Theorem, if p has a root in $\mathbb{Q}$, it must be ± 1 since it must divide its constant term. But $p(1) = -1$ and $p(-1) = 1$, so p is irreducible over $\mathbb{Q}$. Therefore, α is of degree 3 over $\mathbb{Q}$, so $[\mathbb{Q}(\alpha) : Q]$ cannot be a power of 2. Since we cannot construct α, it follows that the regular 7-gon is not constructible by straightedge and compass.

Exercise 13.3.5. Let $p(x) = x^2 + x - 1 = 0$ and $\alpha = 2\cos(2\pi/5)$. By the Rational Root Theorem, if p has a root in $\mathbb{Q}$, it must be ± 1. Since $p(1) = 1$ and $p(-1) = -1$, we deduce that p is irreducible over $\mathbb{Q}$. Hence α is of degree 2 over $\mathbb{Q}$, so it is constructible. We can bisect an angle by straightedge and compass, so $\beta = \cos(2\pi/5)$ is also constructible. Finally, as $\sin(2\pi/5) = \sqrt{1-\cos^2(2\pi/5)}$, $\sin(2\pi/5)$ is also constructible. We conclude that the regular 5-gon is constructible by straightedge and compass.

13.4 Splitting Fields and Algebraic Closures

Exercise 13.4.1. Let $f(x) = x^4-2$. The roots of f are $\sqrt[4]{2}$, $-\sqrt[4]{2}$, $i\sqrt[4]{2}$ and $-i\sqrt[4]{2}$. Hence, the splitting field of f is $\mathbb{Q}(i, \sqrt[4]{2})$. This field has degree $[\mathbb{Q}(i, \sqrt[4]{2}) : \mathbb{Q}] = [\mathbb{Q}(i, \sqrt[4]{2}) : \mathbb{Q}(\sqrt[4]{2})][\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}]$ over $\mathbb{Q}$. Since $\sqrt[4]{2}$ is a root of the irreducible polynomial $x^4 - 2$ over $\mathbb{Q}$, we have $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$. Furthermore, $i \notin \mathbb{Q}(\sqrt[4]{2})$, so $x^2 + 1$ is irreducible over $\mathbb{Q}(\sqrt[4]{2})$ having i as a root. So $[\mathbb{Q}(i, \sqrt[4]{2}) : \mathbb{Q}(\sqrt[4]{2})] = 2$ and therefore $[\mathbb{Q}(i, \sqrt[4]{2}) : \mathbb{Q}] = 8$.

Exercise 13.4.2. Let $f(x) = x^4 + 2$. Let K be the splitting field of f and let L be the splitting field of $x^4 - 2$, that is, $L = \mathbb{Q}(i, \sqrt[4]{2})$ (Exercise 13.4.1). We claim $K = L$, so that $[K : \mathbb{Q}] = 8$ by Exercise 13.4.1.

Let $\zeta = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$. First we prove $\zeta \in L$ and $\zeta \in K$. That $\zeta \in L$ is easy: let $\theta = \sqrt[4]{2}$. Since $\theta \in L$, we have $\theta^2 = \sqrt{2} \in L$. We also have $i \in L$, so $\sqrt{2}, i \in L$ implies $\zeta \in L$. We now prove $\zeta \in K$. We shall prove $i \in K$ and $\sqrt{2} \in K$. Let α be a root of $x^4 + 2$ and β be a root of $x^4 - 1$. Then $(\alpha\beta)^4 = \alpha^4\beta^4 = -2$, so $\alpha\beta$ is also a root of $x^4 + 2$. Since the roots of $x^4 - 1$ are $\pm 1, \pm i$, the roots of $x^4 + 2$ are $\pm\alpha$ and $\pm i\alpha$. Since K is generated over $\mathbb{Q}$ by these roots, it follows that $i\alpha/\alpha = i \in K$. Now let $\gamma = \alpha^2 \in K$. As $\gamma^2 = \alpha^4 = -2$, we have that γ is a root of $x^2 + 2$. Since the roots of $x^2 + 2$ are $i\sqrt{2}$ and $-i\sqrt{2}$, γ must be one of this roots. In either case $\gamma/i \in K$, which implies $\sqrt{2} \in K$, and therefore $\zeta \in K$.

Now we prove $L = K$. On the one hand, let α be a root of $x^4 + 2$ and θ be a root of $x^4 - 2$. Then $\alpha^4 = -2$ and $\theta^4 = 2$. Note that $\zeta^2 = i$, so $\zeta^4 = -1$. Hence $(\zeta\theta)^4 = \zeta^4\theta^4 = -2$, so $\zeta\theta$ is a root of $x^4 + 2$. Then, as we proved earlier, the roots of $x^4 + 2$ are $\pm\zeta\theta$ and $\pm i\zeta\theta$. We also have $(\zeta\alpha)^4 = \zeta^4\alpha^4 = 2$, so $\zeta\alpha$ is a root of $x^4 - 2$. Then, by Exercise 13.4.1, the roots of $x^4 - 2$ are $\pm\zeta\alpha$ and $\pm i\zeta\alpha$. Now, since ζ and α are in K, we have $\zeta\alpha \in K$. We also have $i \in K$, so all the roots of $x^4 - 2$ are in K. Since L is generated by these roots, it follows that $L \subset K$. Similarly, ζ and θ belong to L, so $\zeta\theta \in L$; since $i \in L$, all the roots of $x^4 + 2$ are in L. Since K is generated by these roots, it follows that $K \subset L$. We conclude that $K = L$; in particular, $[K : \mathbb{Q}] = 8$.

Exercise 13.4.3. Let $f(x) = x^4 + x^2 + 1$. Note that $f(x) = (x^2 + x + 1)(x^2 - x + 1)$, so the roots of f are $\pm\frac{1}{2} \pm i\frac{\sqrt{3}}{2}$. Write $w = \frac{1}{2} - i\frac{\sqrt{3}}{2}$, so that these roots are precisely $w, -w, \overline{w}, -\overline{w}$, where $\overline{w}$ denotes the complex conjugate of w. Hence, the splitting field of f is $\mathbb{Q}(w, \overline{w})$. Since $w + \overline{w} = 1$, we have $\mathbb{Q}(w, \overline{w}) = \mathbb{Q}(w)$. Furthermore, w is a root of $x^2 - x + 1$, which is irreducible over $\mathbb{Q}$ since $w \notin \mathbb{Q}$. Therefore, the degree of the splitting field of f is $[\mathbb{Q}(w) : \mathbb{Q}] = 2$.

Exercise 13.4.4. Let $f(x) = x^6 - 4$. Note that $f(x) = (x^3 - 2)(x^3 + 2)$. The roots of $x^3 - 2$ are $\sqrt[3]{2}$, $\zeta\sqrt[3]{2}$ and $\zeta^2\sqrt[3]{2}$, where ζ denotes the primitive 3rd root of unity, i.e., $\zeta = \exp(2\pi i/3) = \cos(2\pi/3) + i\sin(2\pi/3) = -\frac{1}{2} + \frac{\sqrt{3}}{2}$. Furthermore, the roots of $x^3 + 2$ are $-\sqrt[3]{2}$, $-\zeta\sqrt[3]{2}$ and $-\zeta^2\sqrt[3]{2}$. Therefore, the splitting field of f is $\mathbb{Q}(\zeta, \sqrt[3]{2})$. We have $[\mathbb{Q}(\zeta, \sqrt[3]{2}) : \mathbb{Q}] = [\mathbb{Q}(\zeta, \sqrt[3]{2}) : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$. As $\sqrt[3]{2}$ is a root of the irreducible polynomial $x^3 - 2$ over $\mathbb{Q}$, $\sqrt[3]{2}$ has degree 3 over $\mathbb{Q}$. Furthermore, ζ is a root of $x^2 + x + 1$, which is irreducible over $\mathbb{Q}(\sqrt[3]{2})$, so ζ has degree 2 over $\mathbb{Q}(\sqrt[3]{2})$. It follows that the degree of the splitting field of f is $[\mathbb{Q}(\zeta, \sqrt[3]{2}) : \mathbb{Q}] = 6$.

Exercise 13.4.5. We follow the hint. First assume that K is a splitting field over F. Then there exists $f(x) \in F[x]$ such that K is the splitting field of f. Let $g(x)$ be an irreducible polynomial in $F[x]$ with a root $\alpha \in K$. Let β be any root of g. We prove $\beta \in K$, so that g splits completely in $K[x]$. By Theorem 8, there is an isomorphism $\varphi : F(\alpha) \xrightarrow{\sim} F(\beta)$ such that $\varphi(\alpha) = \beta$. Furthermore, $K(\alpha)$ is the splitting field of f over $F(a)$, and $K(\beta)$ is the splitting field of f over $F(\beta)$. Therefore, by Theorem 28, φ extends to an isomorphism $\sigma : K(\alpha) \xrightarrow{\sim} K(\beta)$. Since $K = K(\alpha)$, we have $[K : F] = [K(\alpha) : F] = [K(\beta) : F]$, and therefore $K = K(\beta)$. Thus $\beta \in K$.

Conversely, assume that every irreducible polynomial in $F[x]$ that has a root in K splits completely in $K[x]$. Since $[K : F]$ is finite, we have $K = F(\alpha_1, \dots, \alpha_n)$ for some $\alpha_1, \dots, \alpha_n$. For every $1 \leq i \leq n$, let p_i be the minimal polynomial of α_i over F, and let $f = p_1 p_2 \cdots p_n$. Since every α_i is in K, every p_i has a root in K, hence splits completely in K. Therefore, f splits completely in K and K is generated over F by its roots, so K is the splitting field of $f(x) \in F[x]$.

Exercise 13.4.6. (a) Let K_1 be the splitting field of $f_1(x) \in F[x]$ over F and K_2 be the splitting field of $f_2(x) \in F[x]$ over F. Thus K_1 is generated over F by the roots of f_1, and K_2 is generated over F by the roots of f_2. Then $f_1 f_2$ splits completely in K_1K_2 and K_1K_2 is generated over F by its roots, hence is the splitting field of $f_1 f_2(x) \in F[x]$.

(b) We follow the hint. By Exercise 13.4.5, we shall prove that every irreducible polynomial in $F[x]$ that has a root in $K_1 \cap K_2$ splits completely in $(K_1 \cap K_2)[x]$. Thus, let $f(x)$ be an irreducible polynomial in $F[x]$ that has a root, say α, in $K_1 \cap K_2$. By Exercise 13.4.5, f splits completely in K_1 and splits completely in K_2. Since K_1 and K_2 are contained in K, by the uniqueness of the factorisation of f in K, the roots of f in K_1 must coincide with its roots in K_2. It follows that f splits completely in $(K_1 \cap K_2)[x]$.

13.5 Separable and Inseparable Extension

Exercise 13.5.1. Let $f(x) = a_n x^n + \cdots + a_1 x + a_0$ and $g(x) = b_m x^m + \cdots + b_1 x + b_0$ be two polynomials. We may assume, without any loss of generality, that $n \geq m$. Thus, we can write $g(x) = b_n x^n + \cdots + b_1 x + b_0$, where some of the last coefficients b_i could be zero. We have $f(x) + g(x) = (a_n + b_n)x^n + \cdots + (a_1 + b_1)x + (a_0 + b_0)$, so

$$D_x(f(x) + g(x)) = n(a_n + b_n)x^{n-1} + \cdots + 2(a_2 + b_2)x + (a_1 + b_1) = D_x(f(x)) + D_x(g(x)).$$

Now, for $\ell = 1, \dots, 2n$, set $c_n = \sum_{k=0}^{n} a_k b_{n-k}$, where we also set $a_i = 0$ and $b_i = 0$ if $i > n$. Then

$$f(x)g(x) = \left(\sum_{i=0}^{n} a_i x^i\right)\left(\sum_{j=0}^{n} b_j x^j\right) = \sum_{\ell=0}^{2n}(\sum_{k=0}^{\ell} a_k b_{\ell-k})x^\ell = \sum_{\ell=0}^{2n} c_\ell x^\ell,$$

so that

$$D_x(f(x)g(x)) = D_x\left(\sum_{\ell=0}^{2n} c_\ell x^\ell\right) = \sum_{\ell=0}^{2n-1}(\ell+1)c_{\ell+1}x^\ell.$$

Thus, the coefficient of x^ℓ in $D_x(f(x)g(x))$ is $(\ell+1)c_{\ell+1}$. On the other hand, we have

$$D_x(f(x))\, g(x) = \left(\sum_{k=0}^{n-1}(k+1)a_{k+1}x^k\right)\left(\sum_{k=0}^{n} b_k x^k\right) = \sum_{\ell=0}^{2n-1}\left(\sum_{k=0}^{\ell}(k+1)a_{k+1}b_{\ell-k}\right)x^\ell$$

and

$$f(x)D_x(g(x)) = \left(\sum_{k=0}^{n} a_k x^k\right)\left(\sum_{k=0}^{n-1}(k+1)b_{k+1}x^k\right) = \sum_{\ell=0}^{2n-1}(\sum_{k=0}^{\ell} a_k(\ell-k+1)b_{\ell-k+1})x^\ell,$$

so the coefficient of x^ℓ in $D_x(f(x))g(x) + D_x(g(x))f(x)$ is

$$
\begin{aligned}
&\left(\sum_{k=0}^{\ell}(k+1)a_{k+1}b_{\ell-k}\right) + \left(\sum_{k=0}^{\ell}(\ell-k+1)a_k b_{\ell-k+1}\right)\\
&= (\ell+1)a_{\ell+1}b_0 + \left(\sum_{k=0}^{\ell-1}(k+1)a_{k+1}b_{\ell-k}\right) + \left(\sum_{k=1}^{\ell}(\ell-k+1)a_k b_{\ell-k+1}\right) + (\ell+1)a_0 b_{\ell+1}\\
&= (\ell+1)a_{\ell+1}b_0 + \left(\sum_{k=1}^{\ell}k a_k b_{\ell-k+1}\right) + \left(\sum_{k=1}^{\ell}(\ell-k+1)a_k b_{\ell-k+1}\right) + (\ell+1)a_0 b_{\ell+1}\\
&= (\ell+1)a_{\ell+1}b_0 + \left(\sum_{k=1}^{\ell}(\ell+1)a_k b_{\ell-k+1}\right) + (\ell+1)a_0 b_{\ell+1}\\
&= (\ell+1)\left(\sum_{k=0}^{\ell+1}a_k b_{\ell-k+1}\right) = (\ell+1)c_{\ell+1}.
\end{aligned}
$$

We deduce that $D_x(f(x)g(x)) = D_x(f(x))g(x) + D_x(g(x))f(x)$.

Exercise 13.5.2. The polynomials x and $x+1$ are the only (non-constant, i.e. $\neq 0, 1$) polynomials of degree 1 over $\mathbb{F}_2$; they are clearly irreducible. A polynomial $f(x) \in \mathbb{F}_2[x]$ of degree 2 is irreducible over $\mathbb{F}_2$ if and only if it does not have a root in $\mathbb{F}_2$, that is, exactly if $f(0) = f(1) = 1$. Hence, the only irreducible polynomial of degree 2 over $\mathbb{F}_2$ is $x^2 + x + 1$. Now, for a polynomial $f(x) \in \mathbb{F}_2[x]$ of degree 4 to be irreducible, it must have no linear or quadratic factors. We can also apply the condition $f(1) = f(0) = 1$ to discard the ones with linear factors. Furthermore, f must have an odd number of terms (otherwise it would be 0), and must have constant term 1 (otherwise x would be a factor). We are left with

$$
\begin{aligned}
&x^4 + x^3 + x^2 + x + 1, \qquad && x^4 + x^3 + 1,\\
&x^4 + x^2 + 1, && x^4 + x + 1.
\end{aligned}
$$

For any of these polynomials to be irreducible, it cannot be factorised as a product of two quadratic irreducible factors. Since $x^2 + x + 1$ is the only irreducible polynomial of degree 2 over $\mathbb{F}_2$, only $(x^2 + x + 1)^2 = x^4 + x^2 + 1$ of these four is not irreducible. Hence, the irreducible polynomials of degree 4 over $\mathbb{F}_2$ are precisely $x^4 + x^3 + x^2 + x + 1$, $x^4 + x^3 + 1$ and $x^4 + x + 1$.

Now, since $x + 1 = x - 1$ in $\mathbb{F}_2$, we have $(x+1)(x^4 + x^3 + x^2 + x + 1) = x^5 - 1$. We also have $(x^2+x+1)(x^4+x+1)(x^4+x^3+1) = x^{10}+x^5+1$. It follows that the product of all these irreducible polynomials is

$$
\begin{aligned}
&x(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)\\
&= x(x^5-1)(x^{10}+x^5+1) = x^{16} - x.
\end{aligned}
$$

Exercise 13.5.3. We follow the hint. First assume that d divides n, so that $n = qd$ for some $q \in \mathbb{Z}_+$. Then $x^n - 1 = x^{qd} - 1 = (x^d - 1)(x^{qd-d} + x^{qd-2d} + \ldots + x^d + 1)$, so $x^d - 1$ divides $x^n - 1$.

Conversely, assume that d does not divide n. Then $n = qd + r$ for some $q \in \mathbb{Z}_{\geq 0}$ and $0 < r < d$, so that

$$x^n - 1 = (x^{qd+r} - x^r) + (x^r - 1) = x^r(x^{qd} - 1) + (x^r - 1) = x^r(x^d - 1)(x^{qd-d} + x^{qd-2d} + \cdots + x^d + 1) + (x^r - 1).$$

Since $x^d - 1$ divides the first term, but does nt divide $x^r - 1$ (as $r < d$), it follows that $x^d - 1$ does not divide $x^n - 1$.

Exercise 13.5.4. The first assertion follows analogously as in Exercise 13.5.3. Now, $\mathbb{F}_{p^d}$ is defined as the field whose p^d elements are the roots of $x^{p^d} - x$ over $\mathbb{F}_p$, and similarly $\mathbb{F}_{p^n}$. Take $a = p$. Thus, d divides n if and only if $p^d - 1$ divides $p^n - 1$, and that occurs exactly when $x^{p^d - 1} - 1$ divides $x^{p^n - 1} - 1$ (by Exercise 13.5.3). Thus, if d divides n, any root of $x^{p^d} - x = x(x^{p^d - 1} - 1)$ must be a root of $x^{p^n} - x = x(x^{p^n - 1} - 1)$. Hence $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$. Conversely, if $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$, then $x^{p^d - 1} - 1$ divides $x^{p^n - 1} - 1$, so d divides n.

Exercise 13.5.5. Let $f(x) = x^p - x + a$. Let α be a root of $f(x)$. First we prove f is separable. Since $(\alpha + 1)^p - (\alpha + 1) + a = \alpha^p + 1 - \alpha - 1 + a = 0$, it follows that $\alpha + 1$ is also a root of $f(x)$. This gives p distinct roots of $f(x)$ given by $\alpha + k$ with $k \in \mathbb{F}_p$, so f is separable.

Now we prove f is irreducible. Let $f = f_1 f_2 \cdots f_n$ where $f_i(x) \in \mathbb{F}_p[x]$ is irreducible for all $1 \leq i \leq n$. Let $1 \leq i < j \leq n$, let α_i be a root of f_i and α_j be a root of f_j, so that f_i is the minimal polynomial of α_i and f_j the minimal polynomial of α_j. We prove $\deg f_i = \deg f_j$. Since α_i is a root of f_i, it is a root of f, hence there exists $k_1 \in \mathbb{F}_p$ such that $\alpha_i = \alpha + k_1$. Similarly, there exists $k_2 \in \mathbb{F}_p$ such that $\alpha_j = \alpha + k_2$. Thus $\alpha_i = \alpha_j + k_1 - k_2$, so $f_i(x + k_1 - k_2)$ is irreducible having α_j as a root, so it must be its minimal polynomial. It follows that $f_i(x + k_1 - k_2) = f_j(x)$, so $\deg f_i = \deg f_j$, as claimed. Since i and j were arbitrary, all the f_i are of the same degree, say q. Then $p = \deg f = nq$, so we must have either $n = 1$ or $n = p$ (as p is prime). If $n = p$, then all roots of f are in $\mathbb{F}_p$, so $\alpha \in \mathbb{F}_p$ and thus $0 = \alpha^p - \alpha + a = a$, contrary to the assumption. Therefore $n = 1$, so f is irreducible.

Exercise 13.5.6. By definition, $\mathbb{F}_{p^n}$ is the field whose p^n elements are the roots of $x^{p^n} - x$ over $\mathbb{F}_p$. Since $x^{p^n} - 1 = x(x^{p^n - 1} - 1)$, clearly

$$x^{p^n - 1} - 1 = \prod_{\alpha \in \mathbb{F}_{p^n}^\times} (x - \alpha).$$

Setting $x = 0$, we have

$$\begin{aligned}
-1 &= \prod_{\alpha \in \mathbb{F}_{p^n}^\times} (-\alpha) = (-1)^{p^n - 1} \prod_{\alpha \in \mathbb{F}_{p^n}^\times} \alpha \\
\Rightarrow \quad (-1)^{p^n - 1}(-1) &= (-1)^{p^n - 1}(-1)^{p^n - 1} \prod_{\alpha \in \mathbb{F}_{p^n}^\times} \alpha \\
\Rightarrow \quad (-1)^{p^n} &= \prod_{\alpha \in \mathbb{F}_{p^n}^\times} \alpha.
\end{aligned}$$

It follows that the product of the non-zero elements of $\mathbb{F}_{p^n}$ is $+1$ if $p = 2$ and -1 is p is odd.

For p odd and $n = 1$ we have

$$-1 = \prod_{\alpha \in \mathbb{F}_p^\times} \alpha,$$

so taking module p we find $[1][2] \cdots [p-1] = [-1]$, i.e., $(p-1)! \equiv -1 \pmod{p}$.

Exercise 13.5.7. Let $a \in K$ such that $a \neq b^p$ for every $b \in K$. Let $f(x) = x^p - a$. We prove that f is irreducible and inseparable. If α is a root of $x^p - a$, then $x^p - a = (x-\alpha)^p$, so α is a multiple root of f (with multiplicity p) and hence f is inseparable. Now let $g(x)$ be an irreducible factor of $f(x)$. Note that $\alpha \notin K$, otherwise $a = \alpha^p$, contrary to the assumption. Then $g(x) = (x-\alpha)^k$ for some $k \leq p$. Using the binomial theorem, we have

$$g(x) = (x-\alpha)^k = x^k - k\alpha x^{k-1} + \cdots + (-\alpha)^k,$$

so that $k\alpha \in K$. Since $\alpha \notin K$, it follows that $k = p$, so $g = f$. Hence f is irreducible. We conclude that $K(\alpha)$ is an inseparable finite extension of K.

Exercise 13.5.8. Let $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{F}_p[x]$. Since $\mathbb{F}_p$ has characteristic p, we have $(a+b)^p = a^p + b^p$ for any $a, b \in \mathbb{F}_p$. We can easily generalise this to a finite number of terms, so that $(c_1 + \cdots + c_n)^p = c_1^p + \cdots + c_n^p$ for any $c_1, \ldots, c_n \in \mathbb{F}_p$. Furthermore, by Fermat's Little Theorem, $a^p = a$ for every $a \in \mathbb{F}_p$. Thus, over $\mathbb{F}_p$, we have

$$f(x)^p = (a_n x^n + \cdots + a_1 x + a_0)^p = a_n^p x^{np} + \cdots + a_1^p x^p + a_0^p = a_n x^{np} + \cdots + a_1 x^p + a_0 = f(x^p).$$

Exercise 13.5.9. From the binomial theorem we have

$$(1+x)^{pn} = \sum_{i=0}^{pn} \binom{pn}{i} x^i,$$

so the coefficient of x^{pi} in the expansion of $(1+x)^{pn}$ is $\binom{pn}{pi}$. Since $\mathbb{F}_p$ has characteristic p, we have $(1+x)^{pn} = 1 + x^{pn} = (1+x^p)^n$, so over $\mathbb{F}_p$ we have that $\binom{pn}{pi}$ is the coefficient of $(x^p)^i$ in $(1+x^p)^n$. Furthermore, $(1+x)^{pn} = (1+x^p)^n$ implies

$$(1+x^p)^n = \sum_{i=0}^{n} \binom{n}{i} (x^p)^i = \sum_{i=0}^{pn} \binom{pn}{k} x^i = (1+x)^{pn}$$

over $\mathbb{F}_p$, so that $\binom{pn}{pi} \equiv \binom{n}{i} \pmod{p}$.

Exercise 13.5.10. This is equivalent to proving that for any prime number p, we have $f(x_1, x_2, \ldots, x_n)^p = f(x_1^p, x_2^p, \ldots, x_n^p)$ in $\mathbb{F}_p[x_1, x_2, \ldots, x_n]$. Let

$$f(x_1, x_2, \ldots, x_n) = \sum_{\gamma_1, \ldots, \gamma_n = 0} a_{\gamma_1, \ldots, \gamma_n} x_1^{\gamma_1} \ldots x_n^{\gamma_n}$$

be an arbitrary element of $\mathbb{F}_p[x_1, x_2, \ldots, x_n]$. Since $\mathbb{F}_p$ has characteristic p, we have $(c_1+\cdots+c_n)^p = c_1^p + \cdots + c_n^p$ for any $c_1, \cdots, c_n \in \mathbb{F}_p$. Furthermore, by Fermat's Little Theorem, $a^p = a$ for every $a \in \mathbb{F}_p$. Hence, over $\mathbb{F}_p$,

$$\begin{aligned} f(x_1, x_2, \ldots, x_n)^p = \left(\sum a_{\gamma_1,\ldots,\gamma_n} x_1^{\gamma_1} \ldots x_n^{\gamma_n}\right)^p = \sum (a_{\gamma_1,\ldots,\gamma_n} x_1^{\gamma_1} \ldots x_n^{\gamma_n})^p &= \sum a_{\gamma_1,\ldots,\gamma_n} (x_1^{p\gamma_1} \ldots x_n^{p\gamma_n}) \\ &= f(x_1^p, x_2^p, \ldots, x_n^p). \end{aligned}$$

Exercise 13.5.11. Let $f(x) \in F[x]$ have no repeated irreducible factors in $F[x]$. We may assume that f is monic. Then $f = f_1 f_2 \cdots f_n$ for some monic irreducible polynomials $f_i(x) \in F[x]$. Since F is perfect, f is separable, hence all the f_i have distinct roots. Thus, f splits in linear factors in the closure of F, hence splits in linear factors in the closure of K. It follows that $f(x)$ has no repeated irreducible factors in $K[x]$.

13.6 Cyclotomic Polynomials and Extensions

Exercise 13.6.1. Since $(\zeta_m \zeta_n)^{mn} = 1$, it follows that $\zeta_m \zeta_n$ is an mn^{th} root of unity. Now assume that for some positive integer k we have $(\zeta_m \zeta_n)^k = 1$. Then $(\zeta_m)^{kn} = (\zeta_m)^{kn} (\zeta_n)^{kn} = \zeta^{kn} = 1$, so that m divides kn. Since m and n are relatively prime, it follows that m divides k. Similarly, n divides k. Thus k is a common multiple of m and n; since they are coprime, it follows that k is a multiple of mn. We conclude that $\zeta_m \zeta_n$ is a primitive mn^{th} root of unity.

Exercise 13.6.2. Since $(\zeta_n^d)^{(n/d)} = \zeta_n^n = 1$, it follows that ζ_n^d is an $(n/d)^{\text{th}}$ root of unity. Now let $1 \le k < (n/d)$. Then $(\zeta_n^d)^k = \zeta_n^{kd}$. Since $1 \le kd < n$, we have $\zeta_n^{kd} \ne 1$, so $(\zeta_n^d)^k \ne 1$. Hence, the order of ζ_n^d is precisely (n/d), so it generates the cyclic group of all $(n/d)^{\text{th}}$ roots of unity, that is, ζ_n^d is a primitive $(n/d)^{\text{th}}$ root of unity.

Exercise 13.6.3. Let F be a field containing the n^{th} roots of unity for n odd and let ζ be a $2n^{\text{th}}$ root of unity. If $\zeta^n = 1$, then $\zeta \in F$, so assume $\zeta^n \ne 1$. Since $\zeta^{2n} = 1$, we have that ζ^n is a root of $x^2 - 1$. The roots of this polynomial are 1 and -1, and $\zeta^n \ne 1$, so $\zeta^n = -1$. Hence, $(-\zeta)^n = (-1)^n (\zeta)^n = (-1)^{n+1} = 1$ (since n is odd), so $-\zeta \in F$. Since F is a field, we deduce that $\zeta \in F$.

Exercise 13.6.4. Let F be a field with char $F = p$. The roots of unity over F are the roots of $x^n - 1 = x^{p^k m} - 1 = (x^m - 1)^{p^k}$, so are the roots of $x^m - 1$. Now, since m is relatively prime to p, so is $x^m - 1$ and its derivative mx^{m-1}, so $x^m - 1$ has no multiple roots. Hence, the m different roots of $x^m - 1$ are precisely the m distinct n^{th} roots of unity over F.

Exercise 13.6.5. We use the inequality $\varphi(n) \ge \sqrt{n}/2$ for all $n \ge 1$, where φ denotes the Euler's phi-function. Let K be an extension of $\mathbb{Q}$ with infinitely many roots of unity. Let $N \in \mathbb{N}$. Then there exists $n \in \mathbb{N}$ such that $n > 4N^2$ and there exists some n^{th} root of unity $\zeta \in K$. Thus $[K : \mathbb{Q}] \ge [\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n) \ge \sqrt{n}/2 > N$. Since N was arbitrary, we deduce that $[K : \mathbb{Q}] > N$ for all $N \in \mathbb{N}$, so $[K : \mathbb{Q}]$ is infinite. It follows that in any finite extension of $\mathbb{Q}$ there are only a finite number of roots of unity.

Exercise 13.6.6. Since $\Phi_{2n}(x)$ and $\Phi_n(-x)$ are irreducible, they are the minimal polynomial of any of its roots. Thus, it suffices to find a common root of both. Let $\zeta_2 = -1$ be the primitive 2^{th} root of unity and let ζ_n be a primitive n^{th} root of unity, so that $\zeta_2\zeta_n = -\zeta_n$. Since n is odd, 2 and n are relatively prime. Thus, by Exercise 13.6.1, $\zeta_2\zeta_n$ is a primitive $2n^{\text{th}}$ root of unity, i.e, a root of $\Phi_{2n}(x)$. Furthermore, $-\zeta_n$ is clearly a root of $\Phi_n(-x)$. Thus $-\zeta_n$ is a common root of both $\Phi_{2n}(x)$ and $\Phi_n(-x)$, so $\Phi_{2n}(x) = \Phi_n(-x)$.

Exercise 13.6.7. The Möbius Inversion Formula states that if $f(n)$ is defined for all non-negative integers and $F(n) = \sum_{d|n} f(d)$, then $f(n) = \sum_{d|n} \mu(d)F(\frac{n}{d})$. So let us start with the formula

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

We take natural logarithm in both sides and obtain

$$\ln(x^n - 1) = \ln\left(\prod_{d|n} \Phi_d(x)\right) = \sum_{d|n} \ln \Phi_d(x).$$

Thus, we use the Möbius Inversion Formula for $f(n) = \ln \Phi_n(x)$ and $F(n) = \ln(x^n - 1)$ to obtain

$$\ln \Phi_n(x) = \sum_{d|n} \mu(d) \ln(x^{n/d} - 1) = \sum_{d|n} \ln(x^{n/d} - 1)^{\mu(d)}.$$

Taking exponentials we deduce

$$\Phi_n(x) = \exp\left(\sum_{d|n} \ln(x^{n/d} - 1)^{\mu(d)}\right) = \prod_{d|n}(x^{n/d} - 1)^{\mu(d)} = \prod_{d|n}(x^d - 1)^{\mu(n/d)}.$$

Exercise 13.6.8. (a) Since p is prime, in $\mathbb{F}_p[x]$ we have $(x-1)^p = x^p - 1$, so

$$\Phi_\ell(x) = \frac{x^{\ell-1}}{x-1} = \frac{(x-1)^\ell}{x-1} = (x-1)^{\ell-1}.$$

(b) Note that ζ has order ℓ, being a primitive ℓ^{th} root of unity. Since $p^f \equiv 1 \bmod \ell$, we have $p^f - 1 = q\ell$ for some integer q, so that $\zeta^{p^f-1} = \zeta^{q\ell} = 1$ and hence $\zeta \in \mathbb{F}_{p^f}$. Now we prove that f is the smallest integer with this property. Suppose $\zeta \in \mathbb{F}_{p^n}$ for some n. Then ζ is a root of $x^{p^n-1} - 1$, so ℓ divides $p^n - 1$ (see Exercise 13.5.3). Since f is the smallest power of p such that $p^f \equiv 1$ mod ℓ, it is the smallest integer such that ℓ divides $p^f - 1$, so $n \geq l$, as desired. This in fact proves that $\mathbb{F}_p(\zeta) = \mathbb{F}_{p^f}$, so the minimal polynomial of ζ over $\mathbb{F}_p$ has degree f.

(c) Since $\zeta^a \in \mathbb{F}_p(\zeta)$, clearly $\mathbb{F}_p(\zeta^a) \subset \mathbb{F}_p(\zeta)$. For the other direction we follow the hint. Let b be the multiplicative inverse of a mod ℓ, i.e $ab \equiv 1 \bmod \ell$. Then $(\zeta^a)^b = \zeta$, so $\zeta \in \mathbb{F}_p(\zeta^a)$ and thus $\mathbb{F}_p(\zeta) \subset \mathbb{F}_p(\zeta^a)$. It follows that $\mathbb{F}_p(\zeta^a) = \mathbb{F}_p(\zeta)$.

Now, consider $\Phi_\ell(x)$ as a polynomial over $\mathbb{F}_p[x]$. Let ζ_i, for $1 \leq i \leq \ell$, be ℓ distinct primitive ℓ^{th} roots of unity. The minimal polynomial of each ζ_i has degree f by part (b). Hence, the irreducible factors of $\Phi_\ell(x)$ have degree f. Since Φ_ℓ have degree $\ell - 1$, there must be $\frac{\ell-1}{f}$ factors, and all of them are different since $\Phi_\ell(x)$ is separable.

(d) If $p = 7$, then $\Phi_7(x) = (x-1)^6$ by part (a). If $p \equiv 1 \bmod 7$, then $f = 1$ in (b) and all roots have degree 1, so $\Phi_7(x)$ splits in distinct linear factors. If $p \equiv 6 \bmod 7$, then $f = 2$ is the smallest integer such that $p^f = p^2 \equiv 36 \equiv 1 \bmod 7$, so we have 3 irreducible quadratics. If $p \equiv 2, 4 \bmod 7$, then $f = 3$ is the smallest integer such that $p^3 \equiv 2^3, 4^3 \equiv 8, 64 \equiv 1 \bmod 7$, so we have 2 irreducible cubics. Finally, if $p \equiv 3, 5 \bmod 7$, then $f = 6$ is the smallest integer such that $p^6 \equiv 3^6, 5^6 \equiv 729, 15626 \equiv 1 \bmod 7$, hence we have an irreducible factor of degree 6.

Exercise 13.6.9. Let A be an $n \times n$ matrix over $\mathbb{C}$ for which $A^k = I$ for some integer $k \geq 1$. Then the minimal polynomial of A divides $x^k - 1$. Since we are working over $\mathbb{C}$, there are k distinct roots of this polynomial, so the minimal polynomial of A splits into linear factors. Thus A is diagonalisable.

Now consider $A = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$, where α is an element of a field of characteristic p.

Computing powers of A, inductively it follows that $A^n = \begin{pmatrix} 1 & n\alpha \\ 0 & 1 \end{pmatrix}$ for every positive integer n. Since $p\alpha = 0$, we have $A^p = I$. Now, if A is diagonalizable, then there exists some non-singular matrix P such that $A = PDP^{-1}$, where D is a diagonal matrix whose diagonal entries are the eigenvalues of A. Since A has 1 as its only, D must be the identity and therefore also A. That is, if A is diagonalisable, we must have $\alpha = 0$.

Exercise 13.6.10. For $a, b \in \mathbb{F}_{p^n}$ we have $\varphi(a+b) = (a+b)^p = a^p + b^p = \varphi(a) + \varphi(b)$, and $\varphi(ab) = (ab)^p = a^p b^p = \varphi(a)\varphi(b)$, so φ is a homomorphism. Moreover, if $\varphi(a) = 0$, then $a^p = 0$ implies $a = 0$, so φ is injective. Since $\mathbb{F}_{p^n}$ is finite, φ is also surjective and hence an isomorphism. Furthermore, since every element of $\mathbb{F}_{p^n}$ is a root of $x^{p^n} - x$, we have $\varphi^n(a) = a^{p^n} = a$ for all $a \in \mathbb{F}_{p^n}$, so φ^n is the identity map. Now, let m be a positive integer such that φ^m is the identity map. Then $a^{p^m} = a$ for all $a \in \mathbb{F}_{p^n}$, so every element of $\mathbb{F}_{p^n}$ must be a root of $x^{p^m} - x$. Hence, $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$ and thus n divides m (Exercise 13.5.4), so $n \leq m$.

Exercise 13.6.11. Note that the minimal polynomial of φ is $x^n - 1$, for if φ satisfies some polynomial $x^{n-1} + \cdots + a_1 x + a_0$ of degree $n-1$ (or less) with coefficients in $\mathbb{F}_p$, then $x^{p^{n-1}} + \cdots + a_1 x^p + a_0$ for all $x \in \mathbb{F}_{p^n}$, which is impossible. Since $\mathbb{F}_{p^n}$ has degree n as a vector space over $\mathbb{F}_p$, it follows that $x^n - 1$ is also the characteristic polynomial of φ, hence is the only invariant factor. Therefore, the rational canonical form of φ over $\mathbb{F}_p$ is the companion matrix of $x^n - 1$, which is

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}.$$

Exercise 13.6.12. We will work over the algebraic closure of $\mathbb{F}_{p^n}$, to ensure the field contains all eigenvalues. In Exercise 13.6.11 we proved that the minimal and characteristic polynomial of φ is $x^n - 1$. Moreover, the eigenvalues of φ are the n^{th} roots of unity. We use Exercise 13.6.4 and write $n = p^k m$ for some prime p and some m relatively prime to p, so that $x^n - 1 = (x^m - 1)^{p^k}$ and we get exactly m distinct n^{th} roots of unity, each one of multiplicity p^k. Since all the eigenvalues are zeros of both the minimal and characteristic polynomial of multiplicity p^k, we get m Jordan blocks of size p^k. Now, fix a primitive m^{th} root of unity, say ζ. Then each Jordan block has the form

$$J_i = \begin{pmatrix} \zeta^i & 1 & 0 & \cdots & 0 & 0 \\ 0 & \zeta^i & 1 & \cdots & 0 & 0 \\ 0 & 0 & \zeta^i & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \zeta^i & 1 \\ 0 & 0 & 0 & \cdots & 0 & \zeta^i \end{pmatrix}$$

for some $0 \le i \le m - 1$. Finally, we already know the Jordan canonical form is given by

$$\begin{pmatrix} J_0 & 0 & \cdots & 0 \\ 0 & J_1 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & J_{m-1} \end{pmatrix}.$$

Exercise 13.6.13. (a) Z is a division subring of D, and it is commutative by definition of the centre, so Z is a field. Since it is finite, its prime subfield is $\mathbb{F}_p$ for some prime p, so Z is isomorphic to $\mathbb{F}_{p^n}$ for some integer n. Let $q = p^n$. Since D is a vector space over Z, we have $|D| = q^n$ for some integer n.

(b) Let $x \in D^\times$ and let $C_D(x)$ be the set of the elements in D that commutes with x. Clearly $Z \subset C_D(x)$. We prove that every element $a \in C_D(x)$ has an inverse in $C_D(x)$. Since $a \in C_D(x)$, we have $ax = xa$, and since D is a division ring, we also have $a^{-1} \in D$. Moreover, $a^{-1}ax = a^{-1}xa$ and thus $x = a^{-1}xa$, so $xa^{-1} = a^{-1}x$ and $a^{-1} \in C_D(x)$. Therefore $C_D(x)$ is a division ring. As $Z \subset C_D(x)$, it follows that $C_D(x)$ is a Z-vector space, so $|C_D(x)| = q^m$ for some integer m. If $x \notin Z$, then $C_D(x)$ is a proper subset of D and hence $m < n$.

(c) The class equation for the group $D^\times$ is

$$|D^\times| = |Z(D^\times)| + \sum_{i=1}^{r} |D^\times : C_{D^\times}(x_i)|,$$

where the x_i are representatives of the distinct conjugacy classes in $D^\times$ not contained in the centre of $D^\times$. By (a) we have $|D^\times| = q^n - 1$, $|Z(D^\times)| = q - 1$ and $|C_{D^\times}(x_i)| = q^{m_i} - 1$. Then

$|D^\times : C_{D^\times}(x_i)| = \dfrac{q^n-1}{|C_{D^\times}(x_i)|} = \dfrac{q^n-1}{q^{m_i}-1}$. Plugging these values in the class equation we obtain

$$q^n - 1 = (q-1) + \sum_{i=1}^{r} \frac{q^n-1}{|C_{D^\times}(x_i)|} = (q-1) + \sum_{i=1}^{r} \frac{q^n-1}{q^{m_i}-1}.$$

(d) Since $|D^\times : C_{D^\times}(x_i)|$ is an integer, $|D^\times : C_{D^\times}(x_i)| = \dfrac{q^n-1}{q^{m_i}-1}$ is also an integer. Hence $q^{m_i}-1$ divides q^n-1, so (Exercise 13.5.4) m_i divides n. Since $m_i < n$ (no x_i is in Z), no m_i^{th} root of unity is a n^{th} root of unity. Therefore, as $\Phi_n(x)$ divides x^n-1, it must divide $(x^n-1)/(x^{m_i}-1)$ for $i = 1, 2, \dots, r$.. Letting $x = q$ we deduce that $\Phi_n(q)$ divides $(q^n-1)/(q^{m_i}-1)$ for $i = 1, 2, \dots, r$.

(e) From (d), $\Phi_n(q)$ divides $(q^n-1)/(q^{m_i}-1)$ for $i = 1, 2, \dots, r$, so the class equation in (c) implies that $\Phi_n(q)$ divides $q-1$. Now, let $\zeta \neq 1$ be a n^{th} root of unity. In the complex plane q is closer to 1 than ζ is, so $|q-\zeta| > |q-1| = q-1$. Since $\Phi_n(q) = \prod_{\zeta \text{ primitive}}(q-\zeta)$ divides $q-1$, this is impossible unless $n = 1$. Hence, $D = Z$ and D is a field.

Exercise 13.6.14. We follow the hint. Let $P(x) = x^n + \cdots + a_1x + a_0$ be a monic polynomial over $\mathbb{Z}$ of degree $n \geq 1$. For the sake of a contradiction, suppose there are only finitely many primes dividing the values $P(n)$, $n = 1, 2, \dots$, say $p_1, p_2, \dots, p_k$. Let N be an integer such that $P(N) = a \neq 0$. Let $Q(x) = a^{-1}P(N + ap_1p_2\dots p_kx)$. Then, using the binomial theorem, we have

$$\begin{aligned}
Q(x) &= a^{-1}P(N + ap_1p_2\dots p_kx) \\
&= a^{-1}((N + ap_1p_2\dots p_kx)^n + \cdots + a_1(N + ap_1p_2\dots p_kx) + a_0) \\
&= a^{-1}(N^n + a_{n-1}N^{n-1} + \cdots + a_1N + a_0 + R(x)) \\
&= a^{-1}(P(N) + R(x)) \\
&= 1 + a^{-1}R(x)
\end{aligned}$$

for some polynomial $R(x) \in \mathbb{Z}[x]$ divisible by $ap_1p_2\dots p_k$. Thus $Q(x) \in \mathbb{Z}[x]$. Moreover, for all $n \in \mathbb{Z}_+$ we have $P(N + ap_1p_2\dots p_kn) \equiv a \pmod{p_1, p_2, \dots, p_k}$, so $Q(n) = a^{-1}P(N+ap_1p_2\dots p_kn) \equiv a^{-1}a = 1 \pmod{p_1, p_2, \dots, p_k}$. Now let m be a positive integer such that $|Q(m)| > 1$, so that $Q(m) \equiv 1 \pmod{p_i}$ for all i. Therefore, none of the p_i's divide $Q(m)$. Since $|Q(m)| > 1$, there exists a prime q such that $q \neq p_i$ for all i and such that q divides $Q(m)$. Then q divides $aQ(m) = P(N + ap_1p_2\dots p_km)$, contradicting the fact that only the primes $p_1, p_2, \dots, p_k$ divide the numbers $P(1), P(2), \dots$.

Exercise 13.6.15. We follow the hint. Since $\Phi_m(a) \equiv 0 \pmod p$, we have $a^m \equiv 1 \pmod p$. Then there exists b such that $ba \equiv 1 \bmod p$ (indeed, $b = a^{m-1}$ works), so a is relatively prime to p. We prove that the order of a is precisely m. For the sake of a contradiction, suppose $a^d \equiv 1 \pmod p$ for some d dividing m, so that $\Phi_d(a) \equiv 0 \pmod p$ for some $d < m$. Then a is a multiple root of $x^m - 1$, so it is also a root of its derivative ma^{m-1}. But then $ma^{m-1} \equiv 0 \bmod p$, impossible since p does not divide m nor a. Therefore, the order of a in $(\mathbb{Z}/p\mathbb{Z})^\times$ is precisely m.

Exercise 13.6.16. Let p be an odd prime dividing $\Phi_m(a)$. If p does not divide m, then, by (c), a is relatively prime to p and the order of a in $\mathbb{F}_p^\times$ is m. Since $|\mathbb{F}_p^\times| = p - 1$, this implies that m divides $p - 1$, that is, $p \equiv 1 \pmod{m}$.

Exercise 13.6.17. By Exercise 13.6.14, there are infinitely many primes dividing $\Phi_m(1), \Phi_m(2), \Phi_m(3), \ldots$. Since only finitely many of them can divide m, it follows from by Exercise 13.6.16 that there must exist infinitely many primes p with $p \equiv 1 \pmod{m}$.

Please send comments, suggestions and corrections by e-mail, or at website.
`https://positron0802.wordpress.com`
positron0802@mail.com