Finite Extension Fields

Let F be a field, and $F[t]$ the ring of polynomials in an indeterminate t with coefficients in F. Let $f(t) \in F[t]$ be a polynomial of degree $n \geqslant 1$. Recall that $f(t)$ is *reducible in* $F[t]$ if it factors as $f(t) = g(t)h(t)$ where $g(t), h(t) \in F[t]$ have degree $\in \{1, 2, \ldots, n-1\}$; otherwise, $f(t)$ is *irreducible in* $F[t]$ (and we say simply that $f(t)$ is *irreducible over* F).

From our prior study of ring theory, we know that the ideal $\big(f(t)\big) \subset F[t]$ is maximal; therefore the quotient ring $E = F[t]/\big(f(t)\big)$ is a field. This new field is an extension of F of degree n; in other words, it is an n-dimensional vector space over F. This extension field has the form $E = F[\theta]$ where $\theta = t + \big(f(t)\big)$ is a root of $f(t)$ in E (not in F, unless $n = 1$). Formally, we have extended F to a new field E containing a root of $f(t)$. We have

$$F[\theta] = \{g(\theta) \,:\, g(t) \in F[t]\}.$$

The notation $E = F[\theta]$ reminds us that elements of E are obtained by evaluating polynomials $g(t) \in F[t]$ at θ; the evaluation map

$$F[t] \to F[\theta], \quad g(t) \mapsto g(\theta)$$

is a ring homomorphism. By the Division Algorithm, every $g(t) \in F[t]$ may be uniquely expressed in the form

$$g(t) = q(t)f(t) + r(t) \qquad \text{where } q(t), r(t) \in F[t],\ \deg r(t) < n.$$

Since $g(\theta) = q(\theta)f(\theta) + r(\theta) = r(\theta)$, we see that only polynomials of degree less than n are required to construct E:

$$F[\theta] = \big\{a_0 + a_1\theta + a_2\theta^2 + \cdots + a_{n-1}\theta^{n-1} \,:\, a_0, a_1, \ldots, a_{n-1} \in F\big\}.$$

One sometimes writes

$$E = F(\theta) = \left\{\frac{g(\theta)}{h(\theta)} \,:\, g(t), h(t) \in F[t],\ h(\theta) \neq 0\right\}$$

to indicate that E is a quotient field; but since $F[\theta]$ is already closed under division, we have $F(\theta) = F[\theta]$ and this extra notation serves only for emphasis[1].

Example 1

Suppose that $d \in F$ is not a square in F, i.e. the polynomial $t^2 - d \in F[t]$ is irreducible over F. Then we obtain an extension field

$$E = F[\sqrt{d}] = \{a+b\sqrt{d} \,:\, a, b \in F\}.$$

This is a *quadratic extension of* F, i.e. an extension of degree 2. In odd characteristic, every quadratic extension has this form.

Example 2

We wish to construct $\mathbb{F}_4$ as a quadratic extension of $\mathbb{F}_2$. Since every element of $\mathbb{F}_2$ is a square, we cannot use the method of Example 1. The unique irreducible polynomial of degree 2 over $\mathbb{F}_2$ is given by $f(t) = t^2 + t + 1$. Denote by θ a root of $f(t)$; then

$$F_4 = \mathbb{F}_2[\theta] = \{0,\, 1,\, \theta,\, \theta{+}1\}$$

where $\theta^2 = \theta + 1$.

Example 3

An *algebraic number field* is a finite extension of $\mathbb{Q}$, i.e. an extension of the form $\mathbb{Q}(\theta) \supseteq \mathbb{Q}$ where θ is algebraic over $\mathbb{Q}$. For example, consider the polynomial

$$f(t) = t^3 + t^2 - 3t - 1 \in \mathbb{Q}[t].$$

This polynomial is irreducible over $\mathbb{Q}$ by the Rational Root Theorem (check that ± 1 are not roots of $f(t)$). Now $f(t)$ has a root in the cubic extension field

$$\mathbb{Q}[\theta] = \{a+b\theta+c\theta^2 \,:\, a, b, c \in \mathbb{Q}\}$$

[1] By contrast, the element $\pi \in \mathbb{R}$ is not a root of any nonzero polynomial in $\mathbb{Q}[t]$; so $\mathbb{Q}[\pi] \neq \mathbb{Q}(\pi)$. In this case $\mathbb{Q}[\pi]$ is a subring of $\mathbb{R}$ and $\mathbb{Q}(\pi)$ is its field of quotients: $\mathbb{Q}[\pi] \subset \mathbb{Q}(\pi) \subset \mathbb{R}$.

where

$$\begin{aligned}\theta^3 &= -\theta^2 + 3\theta + 1;\\ \theta^4 &= -\theta^3 + 3\theta^2 + \theta\\ &= (\theta^2 - 3\theta - 1) + 3\theta^2 + \theta\\ &= 4\theta^2 - 2\theta - 1;\end{aligned}$$

etc. For example, consider the elements $\alpha, \beta \in \mathbb{Q}[\theta]$ given by

$$\alpha = 2\theta^2 + \theta - 3; \qquad \beta = \theta^2 - 5\theta - 2.$$

We have

$$\begin{aligned}\alpha + \beta &= 3\theta^2 - 4\theta - 5;\\ \alpha\beta &= (2\theta^2 + \theta - 3)(\theta^2 - 5\theta - 2)\\ &= 2\theta^4 - 9\theta^3 - 12\theta^2 + 13\theta + 6\\ &= 2(4\theta^2 - 2\theta - 1) - 9(-\theta^2 + 3\theta + 1) - 12\theta^2 + 13\theta + 6\\ &= 5\theta^2 - 18\theta - 5.\end{aligned}$$

Inverses of elements in $\mathbb{Q}[\theta]$ may sometimes be found by inspection, e.g. dividing both sides of

$$1 = \theta^3 + \theta^2 - 3\theta$$

by θ gives

$$\frac{1}{\theta} = \theta^2 + \theta - 3.$$

But for more general cases, we may use the extended Euclidean algorithm, in just the same way as in the finite field $\mathbb{F}_p$. For example let us compute α/β for the values of $\alpha, \beta \in \mathbb{Q}[\theta]$ chosen above. We first find $1/\beta$ using the extended Euclidean Algorithm. Since $\beta = g(\theta) \neq 0$ where $g(t) = t^2 - 5t - 2$ and $f(t)$ is irreducible, $g(t)$ is not divisible by $f(t)$ and $\gcd(f(t), g(t)) = 1$. We therefore find polynomials $u(t), v(t) \in \mathbb{Q}[t]$ such that $u(t)f(t) + v(t)g(t) = 1$, using elementary row operations:

$f(t)$	$g(t)$	
1	0	$t^3 + t^2 - 3t - 1$
0	1	$t^2 - 5t - 2$
1	$-t - 6$	$29t + 11$
$\frac{156}{841} - \frac{1}{29}t$	$\frac{1}{29}t^2 + \frac{18}{841}t - \frac{95}{841}$	$\frac{34}{841}$
$-\frac{29}{34}t + \frac{78}{17}$	$\frac{29}{34}t^2 + \frac{9}{17}t - \frac{95}{34}$	1

The last row expresses the desired relation

$$\left(-\tfrac{29}{34}t + \tfrac{78}{17}\right)f(t) + \left(\tfrac{29}{34}t^2 + \tfrac{9}{17}t - \tfrac{95}{34}\right)g(t) = 1.$$

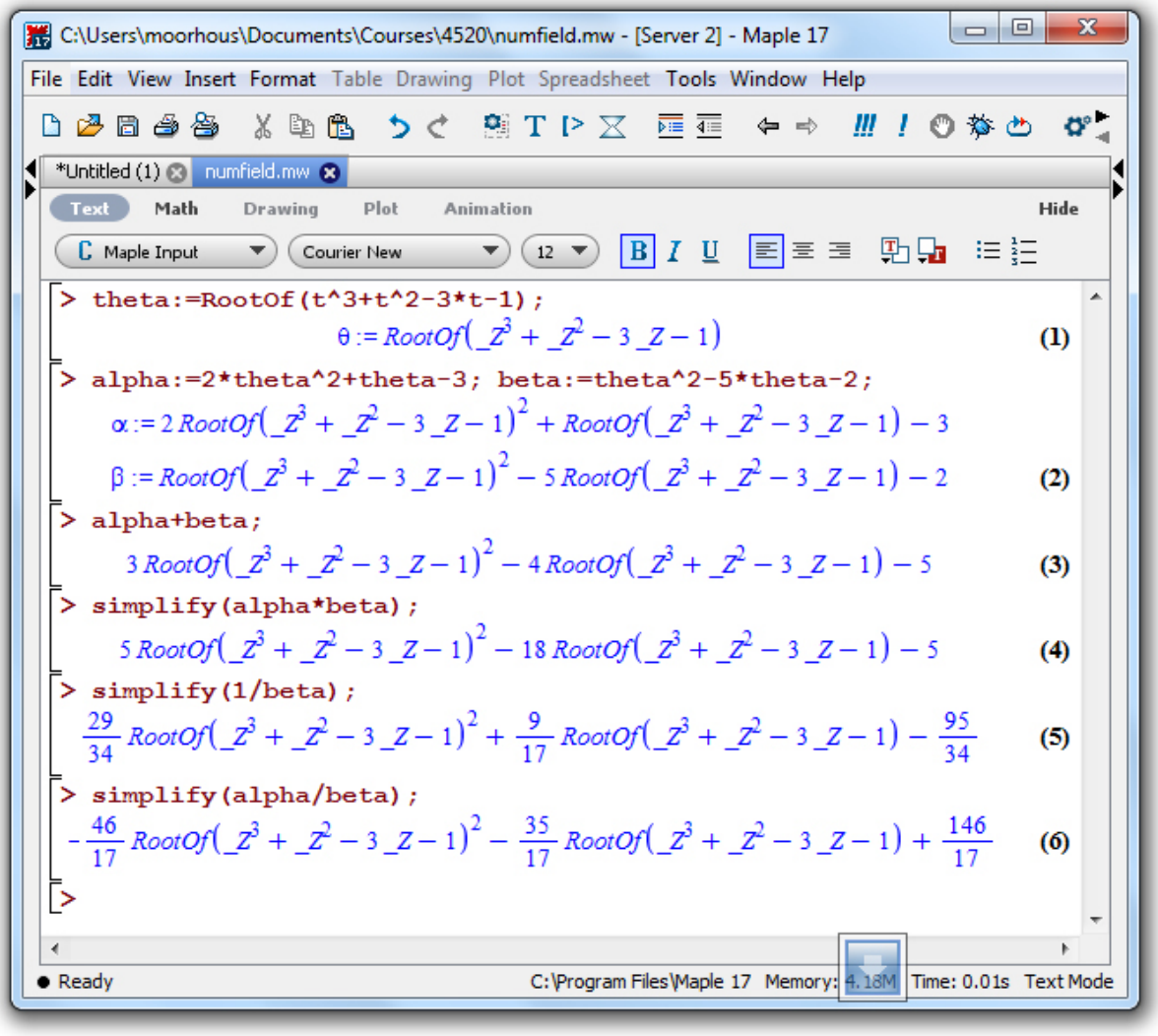
Evaluating at θ and using the defining relation $f(\theta) = 0$ gives

$$1/\beta \;=\; \tfrac{29}{34}\theta^2 + \tfrac{9}{17}\theta - \tfrac{95}{34}.$$

Finally,

$$\begin{aligned}
\alpha/\beta &= \left(2\theta^2+\theta-3\right)\left(\tfrac{29}{34}\theta^2 + \tfrac{9}{17}\theta - \tfrac{95}{34}\right) \\
&= \tfrac{29}{17}\theta^4 + \tfrac{65}{34}\theta^3 - \tfrac{259}{34}\theta^2 - \tfrac{149}{34}\theta + \tfrac{285}{34} \\
&= \tfrac{29}{17}\left(4\theta^2-2\theta-1\right) + \tfrac{65}{34}\left(-\theta^2+3\theta+1\right) - \tfrac{259}{34}\theta^2 - \tfrac{149}{34}\theta + \tfrac{285}{34} \\
&= -\tfrac{46}{17}\theta^2 - \tfrac{35}{17}\theta + \tfrac{146}{17}.
\end{aligned}$$

Let us check these results using Maple:



Algebraic and Transcendental Elements

Now let $E \supseteq F$ be an extension of fields, and let $\theta \in E$. Consider the 'evaluation map'

$$F[t] \to E, \quad g(t) \mapsto g(\theta).$$

This is clearly a ring homomorphism; and by definition, its image is the subring

$$F[\theta] = \{g(\theta) : g(t) \in F[t]\} \subseteq E.$$

The kernel of the evaluation map is an ideal in the polynomial ring $F[t]$. However, $F[t]$ is a principal ideal ring (i.e. every ideal is principal) so by the First Isomorphism Theorem for Rings,

$$F[t]/\big(f(t)\big) \cong F[\theta] \subseteq E$$

where every $g(t) \in F[t]$ satisfies

$$g(\theta) = 0 \iff f(t) \,\big|\, g(t) \iff g(t) = m(t)f(t) \text{ for some } m(t) \in F(t).$$

The principal ideal $\big(f(t)\big)$ generated by $f(t)$ is the set of all multiples of $f(t)$; this is the set of all polynomials having θ as a root. We have two cases:

Case (i): $f(t) = 0$. This says that θ is not a root of any nonzero polynomial $g(t) \in F[t]$; we say that θ is *transcendental over* F. (It may be shown, for example, that the well-known constants $\pi, e \in \mathbb{R}$ are transcendental over $\mathbb{Q}$. I will distribute a handout containing proofs of these facts, although we won't cover all details in class.) In this case our isomorphism reduces to

$$F \subset F[\theta] \subset E \quad \text{and} \quad F[\theta] \cong F[t].$$

Note that $F[\theta] \cong F[t]$ is a ring but not a field; this is why each of the containments in $F \subset F[\theta] \subset E$ is proper. In fact, $F[\theta] \cong F[t]$ is an integral domain and its field of quotients is the subfield $F(\theta)$. So we have

$$F \subset F[\theta] \subset F(\theta) \subset E.$$

Case (ii): $f(t)$ has degree $n \geqslant 1$. We may assume $f(t)$ is monic; otherwise divide $f(t)$ by its leading coefficient. In this case we say θ is *algebraic of degree* n *over* F, and $f(t)$ is the *minimal polynomial of* θ *over* F. By the Division Algorithm,

$$F[t]/\big(f(t)\big) \cong F[\theta] = \{a_0 + a_1\theta + a_2\theta^2 + \cdots + a_{n-1}\theta^{n-1} : a_i \in F\} \subseteq E.$$

In this case $F[\theta]$ is actually a subfield of E, and we have a tower of extension fields

$$F \subseteq F[\theta] = F(\theta) \subseteq E.$$

Here $[F[\theta] : F] = n$ since $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ is a basis for $F[\theta]$ over F.

The arguments above require that we recognize when a polynomial is irreducible. For a polynomial $f(t)$ of degree n over a *finite* field F, this can be done by simply enumerating *reducible* polynomials of degree n, of which there is certainly only a finite number. Moreover for an arbitrary ground field F, if $n \in \{2, 3\}$ then it suffices to check that $f(t) \in F[t]$ has no roots in F. It is helpful to have more general techniques for verifying irreducibility of $f(t)$. The following is very helpful when working over the ground field $\mathbb{Q}$:

Theorem. Let $f(t) \in \mathbb{Z}[t]$. If $f(t)$ is irreducible over $\mathbb{Z}$, then $f(t)$ is irreducible over $\mathbb{Q}$.

This is a standard result from ring theory[1].

Example 4

Consider $\alpha = \sqrt{2}+\sqrt{3} \in \mathbb{R}$. It is easy to check that α is a root of $f(t) = t^4-10t^2+1 \in \mathbb{Q}[t]$. To show that this is the minimal polynomial of α over $\mathbb{Q}$, we must show that it is irreducible over $\mathbb{Q}$. If not, then it is reducible over $\mathbb{Z}$, and we have either

(i) $f(t) = (t \pm 1)(t^3 + at^2 + bt \pm 1)$ where $a, b \in \mathbb{Z}$, or
(ii) $f(t) = (t^2 + at \pm 1)(t^2 + bt \pm 1)$ where $a, b \in \mathbb{Z}$.

Case (i) cannot occur since neither 1 nor -1 is a root of $f(t)$. In case (ii) we must have $b = -a$ and $-a^2 \pm 2 = 10$, which has no integer solutions. We deduce that $f(t)$ is irreducible over $\mathbb{Q}$, and hence $f(t)$ is the minimal polynomial of α.

Observe the factorization

$$f(t) = \big(t - \sqrt{2} - \sqrt{3}\big)\big(t - \sqrt{2} + \sqrt{3}\big)\big(t + \sqrt{2} - \sqrt{3}\big)\big(t + \sqrt{2} + \sqrt{3}\big)$$

in $\mathbb{R}[t]$. We have a tower of fields

$$\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{2}] \subseteq \mathbb{Q}[\alpha]$$

[1] See e.g. Theorem 4.18 of Hungerford, *Abstract Algebra: An Introduction*; or `http://www/uwyo.edu/moorhouse/handouts/algebra.pdf` p.67.

of degree $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 4$. However, $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$ since $t^2 - 2$ is the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$. (This follows from the fact that $t^2 - 2$ is irreducible over $\mathbb{Q}$, and has $\sqrt{2}$ as a root; it can also be deduced from the classical fact that $\sqrt{2}$ is irrational.) By the transitivity of degrees, we deduce that $[\mathbb{Q}[\alpha] : \mathbb{Q}[\sqrt{2}]] = 2$. In particular, $\alpha \notin \mathbb{Q}[\sqrt{2}]$, which implies that $\sqrt{3} \notin \mathbb{Q}[\sqrt{2}]$; this is stronger than the fact that $\sqrt{3}$ is irrational. Similarly, $\sqrt{2} \notin \mathbb{Q}[\sqrt{3}]$.

Example 5

This example yields a proof that an arbitrary angle cannot be trisected using a straightedge and compass. Define $\zeta \in \mathbb{C}$ by

$$\zeta = e^{2\pi i/9} = \cos\left(\tfrac{2\pi}{9}\right) + i \sin\left(\tfrac{2\pi}{9}\right);$$
$$\zeta^{-1} = \overline{\zeta} = e^{-2\pi i/9} = \cos\left(\tfrac{2\pi}{9}\right) - i \sin\left(\tfrac{2\pi}{9}\right).$$

We have

$$0 = \zeta^9 - 1 = (\zeta^3 - 1)(\zeta^6 + \zeta^3 + 1)$$

and since $\zeta^3 = e^{2\pi i/3} \neq 1$, it follows that

$$\zeta^6 + \zeta^3 + 1 = 0.$$

Now consider

$$\alpha = \zeta + \zeta^{-1} = \zeta + \overline{\zeta} = 2\cos\left(\tfrac{2\pi}{9}\right) \in \mathbb{R};$$

then

$$\begin{aligned}
\alpha^3 - 3\alpha + 1 &= \left(\zeta + \zeta^{-1}\right)^3 - 3\left(\zeta + \zeta^{-1}\right) + 1 \\
&= \left(\zeta^3 + 3\zeta + 3\zeta^{-1} + \zeta^{-3}\right) - 3\zeta - 3\zeta^{-1} + 1 \\
&= \zeta^3 + \zeta^{-3} + 1 \\
&= \zeta^6 + \zeta^3 + 1 \\
&= 0.
\end{aligned}$$

We claim that the polynomial $f(t) = t^3 - 3t + 1 \in \mathbb{Z}[t]$ is irreducible over $\mathbb{Q}$. If not, then it is reducible over $\mathbb{Z}$ and

$$f(t) = (t \pm 1)(t^2 + at \pm 1)$$

for some $a \in \mathbb{Z}$; but since neither 1 nor -1 is a root of $f(t) = t^3 - 3t + 1$, this is impossible. Therefore $f(t)$ is the minimal polynomial of $\alpha = 2\cos\frac{2\pi}{9}$ over $\mathbb{Q}$, and

$$[Q[\alpha] : \mathbb{Q}] = 3.$$

Suppose we are given an initial configuration of labeled points, line segments and circular arcs in $\mathbb{R}^2$. Each labeled points in this initial configuration have all been identified as a point of intersection of two lines, or of two arcs, or of a line and an arc. Starting from this initial configuration of points and lines, we proceed to use straightedge and compass to construct new points, lines and arcs using straightedge and compass by a sequence of steps. Legal steps are as follows:

(A) Join two previously labeled points to form a line (or a segment thereof).
(B) Using three previously labeled points P, Q, R, construct the circle (or arc thereof) with center P having QR as radius.
(C) Intersect two previously constructed lines to form a new labeled point.
(D) Intersect two previously constructed circular arcs to form a new labeled point.
(E) Intersect a line and a circular arc (previously constructed) to form a new labeled point.

Denote by $F \supseteq \mathbb{Q}$ the extension field generated by

- the coordinates of the points,
- the slopes and intercepts of the lines, and
- the radii of the circles

in the initial configuration. After n steps we obtain a tower of fields

$$F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_n$$

where $F_n \supseteq \mathbb{Q}$ is the extension field generated by the coordinates of the points, the slopes and intercepts of the lines, and the radii of the circles after n steps. It is not hard to see that $[F_k : F_{k-1}] = 1$ or 2 for each $k \in \{1, 2, \ldots, n\}$. Indeed, steps of type (A), (B) and (C) do not increase the coordinate field at all, so that $[F_k : F_{k-1}] = 1$. Steps of type (D) and (E) yield new points whose coordinates are roots of a quadratic equation with coefficients in F_{k-1}, so that $[F_k : F_{k-1}] \leqslant 2$. The claim follows. Now by the transitivity of degrees for field extensions, we conclude that $[F_n : F]$ is a power of 2.

It is well known that the angle $\frac{2\pi}{3} = 120^\circ$ is constructible. If an arbitrary angle can be trisected using a straightedge and compass, then an angle $\frac{2\pi}{9} = 40^\circ$ is constructible using a straightedge and compass. We will show that this is impossible:

We may assume that the circle $x^2 + y^2 = 1$ and the x and y axes are given, so we are starting with $F = \mathbb{Q}$. If, after a finite number of steps, we have constructed a line through $(0, 0)$ having a 40° angle with respect to the x-axis, then by intersecting this line with the unit circle gives us the point $\left(\cos \frac{2\pi}{9}, \sin \frac{2\pi}{9}\right)$. Thus after n steps we have $\alpha \in F_n$ and

$$\mathbb{Q} \subseteq \mathbb{Q}[\alpha] \subseteq F_n.$$

By transitivity of degrees, $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 3$ must divide $[F_n : \mathbb{Q}]$. However, $[F_n : \mathbb{Q}]$ is a power of 2, a contradiction.