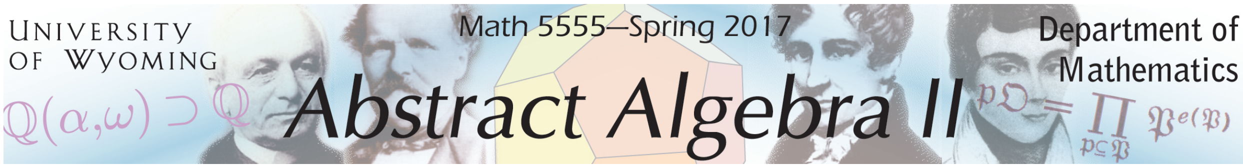

Finite Extension Fields

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 $\in \{2, 3, \ldots, n-1\}$; 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: