MATH 5591H HOMEWORK 9

BRENDAN WHITAKER

13.1 Exercises

3. *Show that $x^3 + x + 1$ is irreducible over $\mathbb{F}_2$ and let θ be a root. Compute the powers of θ in $\mathbb{F}_2(\theta)$.*

Proof. Suppose $p(x) = x^3 + x + 1$ were reducible over $\mathbb{F}_2$. Then since it has degree 3, we would have $(x-1)|p(x)$ or $x|p(x)$. Since we have a nonzero constant term, we know the second of these two options does not hold. Also note $p(1) = 1^3 + 1 + 1 = 1 + 1 + 1 = 1 \neq 0$, so $(x-1) \nmid p(x)$. Thus it must be irreducible over $\mathbb{F}_2$ since this field only has these two elements. □

Now consider $\mathbb{F}_2(\theta) = \left\{ a + b\theta + c\theta^2 : a, b, c \in \mathbb{F}_2 \right\}$, since θ is a root of degree 3. Note $\theta^3 = -\theta - 1$. We have:

$$\begin{aligned}
\theta^0 &= 1 \\
\theta^1 &= \theta \\
\theta^2 &= \theta^2 \\
\theta^3 &= -\theta - 1 \\
\theta^4 &= \theta^2 - \theta \\
\theta^5 &= (-\theta - 1) - \theta^2 \\
&= -\theta^2 - \theta - 1 \\
\theta^6 &= \theta + 1 - \theta^2 - \theta \\
&= 1 - \theta^2 \\
\theta^7 &= \theta - (-\theta - 1) \\
&= 1.
\end{aligned} \tag{1}$$

13.2 Exercises

8. *Let F be a field of characteristic $\neq 2$. Let D_1 and D_2 be elements of F, neither of which is a square in F. Prove that $F(\sqrt{D_1}, \sqrt{D_2})$ is of degree 4 over F if $D_1 D_2$ is not a square in F and is of degree 2 over F otherwise. When $F(\sqrt{D_1}, \sqrt{D_2})$ is of degree 4 over F, the field is called a* ***biquadratic extension of*** *F.*

Proof. Assume $D_1 D_2$ is not a square. Suppose $\sqrt{D_1}, \sqrt{D_2}$ are linearly dependent. Then we have $\sqrt{D_1} = \alpha\sqrt{D_2} + \beta$ for some $\alpha, \beta \in F$. Suppose for contradiction that $\beta = 0$. Then we have:

$$\begin{aligned}
\sqrt{D_1} &= \alpha\sqrt{D_2} \\
D_1 &= \alpha^2 D_2 \\
D_1 D_2 &= \alpha^2 D_2^2.
\end{aligned} \tag{2}$$

But we said $D_1 D_2$ is not a square, so we have a contradiction, so we must have that $\beta \neq 0$. And $\alpha \neq 0$ since otherwise $\sqrt{D_1} \in F \Rightarrow D_1$ is a square in F.

Then:

$$D_1 = (\alpha\sqrt{D_2} + \beta)^2 = \alpha^2 D_2 + 2\alpha\beta\sqrt{D_2} + \beta^2,$$

Date: SP18.

and since we are over a field of characteristic $\neq 2$, we know that $2 \neq 0 \Rightarrow 2\alpha\beta \neq 0$, so we must have that $\sqrt{D_2} \in F$ which means that D_2 is a square in F, contradiction, so $\sqrt{D_1}, \sqrt{D_2}$ must be linearly independent over F. Thus $m_{\sqrt{D_1},F(\sqrt{D_2}} = x^2 - D_1$, and so the degree of $F(\sqrt{D_1}, \sqrt{D_2})$ over $F(\sqrt{D_2})$ is 2. Since D_2 is not a square in F, we know $m_{\sqrt{D_2},F} = x^2 - D_2$, which as degree 2, so $F(\sqrt{D_2})$ has degree 2 over F, and note these are both finite extensions. Recall that if E/K, K/F are finite, then E/F is finite, and we have $[E : F] = [E : K][K : F]$. So $[F(\sqrt{D_1}, \sqrt{D_2}) : F] = 4$.

If D_1D_2 is a square, we would have $\sqrt{D_1}\sqrt{D_2} = a$ for some integer a. Thus $\sqrt{D_1} = \frac{a}{\sqrt{D_2}}$, and so $F(\sqrt{D_1}, \sqrt{D_2}) = F(\sqrt{D_2})$. Then we showed $F(\sqrt{D_2})$ has degree 2 over F, so $[F(\sqrt{D_1}, \sqrt{D_2}) : F] = 2$. □

9. *Let F be a field of characteristic $\neq 2$. Let a, b be elements of the field F with b not a square in F. Prove that a necessary and sufficient condition for $\sqrt{a + \sqrt{b}} = \sqrt{m} + \sqrt{n}$ for some m and n in F is that $a^2 - b$ is a square in F. Use this to determine when the field $\mathbb{Q}(\sqrt{a + \sqrt{b}})(a, b \in \mathbb{Q})$ is biquadratic over $\mathbb{Q}$.*

Proof. Let $a^2 - b$ be a square in F. Then:

$$\left(\sqrt{a + \sqrt{b}}\right)^2 \left(\sqrt{a - \sqrt{b}}\right)^2 = (a + \sqrt{b})(a - \sqrt{b}) = a^2 - b = c^2, \tag{3}$$

for some $c \in F$. Then we have $\sqrt{a^2 - b} \in F$. Define $m = \frac{a+\sqrt{a^2-b}}{2}$ and $n = \frac{a-\sqrt{a^2-b}}{2}$, which are well defined since we said the characteristic of our field is not 2. Then we have:

$$\begin{aligned} m &= \frac{2a + 2\sqrt{a^2 - b}}{4} \\ &= \frac{(a + \sqrt{b}) + 2\sqrt{a^2 - b} + (a - \sqrt{b})}{4} \\ &= \left(\frac{\sqrt{a + \sqrt{b}} + \sqrt{a - \sqrt{b}}}{2}\right)^2 \\ \Rightarrow \sqrt{m} &= \frac{\sqrt{a + \sqrt{b}} + \sqrt{a - \sqrt{b}}}{2}. \end{aligned} \tag{4}$$

Similarly, we have:

$$\sqrt{n} = \frac{\sqrt{a + \sqrt{b}} - \sqrt{a - \sqrt{b}}}{2} \tag{5}$$

Thus:

$$\sqrt{m} + \sqrt{n} = \frac{\sqrt{a + \sqrt{b}} + \sqrt{a - \sqrt{b}}}{2} + \frac{\sqrt{a + \sqrt{b}} - \sqrt{a - \sqrt{b}}}{2} = \sqrt{a + \sqrt{b}}. \tag{6}$$

So we have shown the claim holds in the first direction.

Assume we have the following:

$$\begin{aligned} \sqrt{a + \sqrt{b}} &= \sqrt{m} + \sqrt{n} \\ a + \sqrt{b} &= m + n + 2\sqrt{mn}. \end{aligned} \tag{7}$$

Now we claim we must have $a = m + n$ and $b = 4mn$. Suppose $\sqrt{b} = c + 2\sqrt{mn}$ for some $c \in F$. Then $b = c^2 + 4c\sqrt{mn} + 4mn$. Since $\mathrm{char}F \neq 2$, and $b \in F$, we know we must have either $\sqrt{mn} \in F$, or $c = 0$. If $\sqrt{mn} \in F$, then $\sqrt{b} \in F$, which means b is a square, contradiction. So we must have $c = 0$, thus the claim holds. Then we have:

$$\begin{aligned} a^2 - b &= (a + \sqrt{b})(a - \sqrt{b}) \\ &= (m + n + 2\sqrt{mn})(m + n - 2\sqrt{mn}) \\ &= m^2 + mn - 2m\sqrt{mn} + mn + n^2 - 2n\sqrt{mn} + 2m\sqrt{mn} + 2n\sqrt{mn} - 4mn \\ &= m^2 + n^2 - 2mn \\ &= (m - n)^2. \end{aligned} \tag{8}$$

Thus if $a^2 - b$ is a square, then we have:

$$\mathbb{Q}(\sqrt{a+\sqrt{b}}) = \mathbb{Q}(\sqrt{m}+\sqrt{n}) = \mathbb{Q}(\sqrt{m},\sqrt{n}). \tag{9}$$

Clearly the degree is either 2 or 4, but if it is 2, then we would have $m = n$ which would give us b is a square, contradiction, so the degree is 4. So $\mathbb{Q}(\sqrt{a+\sqrt{b}})$ is biquadratic. □

13. *Suppose $F = \mathbb{Q}(\alpha_1, \alpha_2, ..., \alpha_n)$ where $\alpha_i^2 \in \mathbb{Q}$ for $i = 1, 2, ..., n$. Prove that $\sqrt[3]{2} \notin F$.*

Proof. Since these roots are all quadratic, we know that the degree of $\mathbb{Q}(\alpha_i)$ over $\mathbb{Q}(\alpha_1, ..., \alpha_{i-1})$ is at most 2, and if α_i is generated by $\alpha_1, ..., \alpha_{i-1}$ then the degree is 1. Thus these are all finite extensions, and then by induction, we know that $F/\mathbb{Q}$ has finite degree, and it's degree is the product of all the extensions $\mathbb{Q}(\alpha_i)/\mathbb{Q}(\alpha_1, ..., \alpha_{i-1})$. Since these are all 1 or 2, we know $[F : \mathbb{Q}] = 2^k$ for some integer positive integer k (positive since the first extension has degree 2 over $\mathbb{Q}$). But $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, and if $\sqrt[3]{2} \in F$, then we would have $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] | 2^k$, which is not the case. Thus $\sqrt[3]{2} \notin F$. □

16. *Let K/F be an algebraic extension and let R be a ring contained in K and containing F. Show that R is a subfield of K containing F.*

Proof. Since K/F is algebraic, we know that $\forall \alpha \in K$, α is algebraic over F. So α is the root of some polynomial $p(x) \in F[x]$. So let $r \in R$, nonzero, we wish to construct an inverse r^{-1} for r. Then we have:

$$\begin{aligned} p(r) &= a_n r^n + \cdots + a_1 r + a_0 = 0 \\ a_0 &= -a_n r^n - \cdots - a_2 r^2 - a_1 r \\ 1 &= -\frac{a_n}{a_0} r^n - \cdots - \frac{a_2}{a_0} r^2 - \frac{a_1}{a_0} r \\ \frac{1}{r} &= -\frac{a_n}{a_0} r^{n-1} - \cdots - \frac{a_2}{a_0} r - \frac{a_1}{a_0}. \end{aligned} \tag{10}$$

This is well defined since r is nonzero. Thus we have found r^{-1}, and it is an element of r since $a_i \in F \subseteq R$, and since we have additive and multiplicative closure in R. Thus we have inverses in R and it is a field. □

20. *Show that if the matrix of the linear transformation "multiplication by α" considered in the previous exercise is A then α is a root of the characteristic polynomial of A. This gives an effective procedure for determining an equation of degree n satisfied by an element α in an extension of F of degree n. Use this procedure to obtain the monic polynomial of degree 3 satisfied by $\sqrt[3]{2}$ and by $1 + \sqrt[3]{2} + \sqrt[3]{4}$.*

Proof. Let $c_A = a_n x^n + \cdots + a_1 x + a_0$ be the characteristic polynomial of the matrix A of multiplication by α. Then we know:

$$c_A(A) = a_n A^n + \cdots + a_1 A + a_0 = 0, \tag{11}$$

where 0 represents the 0 matrix. Then replacing A with α, we have:

$$c_A(\alpha) = a_n \alpha^n + \cdots + a_1 \alpha + a_0 = 0, \tag{12}$$

which makes sense since α must be an eigenvalue of A since $Ar = \alpha r$. So it must be a root by definition. □

Now we find a monic polynomial of degree 3 satisfied by $\sqrt[3]{2}$. We have a basis $\{ 1, \sqrt[3]{2}, \sqrt[3]{4} \}$. We set $k = \begin{pmatrix} a \\ b \\ c \end{pmatrix}$. We solve for A knowing:

$$\begin{aligned} A \begin{pmatrix} a \\ b \\ c \end{pmatrix} &= \sqrt[3]{2} \begin{pmatrix} a \\ b \\ c \end{pmatrix} \\ &= (\sqrt[3]{2}a + \sqrt[3]{4}b + 2c) \\ \Rightarrow A &= \begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}. \end{aligned} \tag{13}$$

And the characteristic polynomial of A is $x^3 - 2$.

Using the exact same basis, we find that for $\alpha = 1 + \sqrt[3]{2} + \sqrt[3]{4}$,

$$A = \begin{pmatrix} 1 & 2 & 2 \\ 1 & 1 & 2 \\ 1 & 1 & 1 \end{pmatrix} \tag{14}$$

Thus the characteristic polynomial is given by $x^3 - 3^2 - 3x - 1$.

13.4 Exercises

2. *Find the splitting field and its degree over $\mathbb{Q}$ for $x^4 + 2$.*

We have four roots in the plane. Observe:

$$\begin{aligned} x^4 &= -2 \\ x^2 &= \pm i\sqrt{2} \\ x &= \pm\sqrt{i\sqrt{2}}, \pm i\sqrt{i\sqrt{2}} \\ &= \pm\sqrt{i}\sqrt[4]{2}, \pm i\sqrt{i}\sqrt[4]{2}. \end{aligned} \tag{15}$$

We adjoin them and this will be the splitting field. It is $\mathbb{Q}(\sqrt{i}\sqrt[4]{2}, i)$. The first root $\sqrt{i}\sqrt[4]{2}$ is of degree 4 since $x^4 + 2$ has degree 4 and it is a root of this irreducible polynomial. And i has degree 2 and is linearly independent, so we know the splitting field has degree 8 over $\mathbb{Q}$.