Math 114 Homework 2

Michael Knopf

(due Thursday, 5 February)

1. (Exercise 2 in DF §13.2.) Let $g(x) = x^2 + x - 1$ and $h(x) = x^3 - x + 1$. Obtain fields of 4, 8, 9, and 27 elements by adjoining a root of $f(x)$ to the field F where $f(x)$ equals $g(x)$ or $h(x)$ and F equals $\mathbf{F}_2$ or $\mathbf{F}_3$. Write down the multiplication tables for the fields with four and nine elements and show that the nonzero elements form a cyclic group.

Proof. If $g(x)$ or $h(x)$ were reducible over either $\mathbb{F}_2$ or $\mathbb{F}_3$, then they would have a linear factor, thus a root in that field. However, in $\mathbb{F}_2$, $g(0) = g(1) = h(0) = h(1) = 1$; and in $\mathbb{F}_3$, $g(0) = h(0) = g(1) = h(1) = h(2) = 1$. So both polynomials are irreducible over both fields.

Let α and β be roots of $g(x)$ in some extensions of $\mathbb{F}_2$ and $\mathbb{F}_3$, respectively. The multiplication tables for the extensions $\mathbb{F}_2(\alpha)$ and $\mathbb{F}_2(\beta)$ are given below. They have 4 and 9 elements, respectively. This is not suprising, since $g(x)$ is irreducible over both $\mathbb{F}_2$ and $\mathbb{F}_3$, so both extensions are of degree 2. A vector space of dimension n over a finite field with p elements has cardinality p^n since, for each of the n basis vectors, we have p choices for its coefficient.

$\mathbb{F}_2(\alpha)$	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

$\mathbb{F}_3(\beta)$	0	1	2	β	2β	$1+\beta$	$1+2\beta$	$2+\beta$	$2+2\beta$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	β	2β	$1+\beta$	$1+2\beta$	$2+\beta$	$2+2\beta$
2	0	2	1	2β	β	$2+2\beta$	$2+\beta$	$1+2\beta$	$1+\beta$
β	0	β	2β	$1+2\beta$	$2+\beta$	1	$2+2\beta$	$1+\beta$	2
2β	0	2β	β	$2+\beta$	$1+2\beta$	2	$1+\beta$	$2+2\beta$	1
$1+\beta$	0	$1+\beta$	$2+2\beta$	1	2	$2+\beta$	β	2β	$1+2\beta$
$1+2\beta$	0	$1+2\beta$	$2+\beta$	$2+2\beta$	$1+\beta$	β	2	1	2β
$2+2\beta$	0	$2+2\beta$	$1+\beta$	2	1	$1+2\beta$	2	β	$2+\beta$

The nonzero elements of a field always form a multiplicative group. For a finite field, this group is always cyclic. In particular, the nonzero elements of $\mathbb{F}_2(\alpha)$ form a cyclic group generated by α, since $\alpha^2 = 1 + \alpha$. The nonzero elements of $\mathbb{F}_3(\beta)$ form a cyclic group generated by β: since $\beta^3 = 2 + 2\beta \neq 1$, we know β has order greater than 3, thus it must have order 9 (by Lagrange's Theorem).

Let γ and δ be roots of $h(x)$ in $\mathbb{F}_2$ and $\mathbb{F}_3$, respectively. Since $h(x)$ is irreducible over both fields, these elements both have degree 3. So the number of elements in $\mathbb{F}_2(\delta)$ and in $\mathbb{F}_3(\gamma)$ are $2^3 = 8$ and $3^3 = 27$, respectively.

□

2. (Exercise 13 in DF §13.2.) Suppose $F = \mathbf{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ where $\alpha_i^2 \in \mathbf{Q}$ for $i = 1, 2, \ldots, n$. Prove that $\sqrt[3]{2} \notin F$.

Proof. Let $F_0 = \mathbb{Q}$ and, for each $i = 1, 2, \ldots, n$, let $F_i = F_{i-1}(\alpha_i)$. By previous theorems, $F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n$ and $F_i = \mathbb{Q}(\alpha_1, \ldots, \alpha_i)$ for all i.

If $\alpha_i \in F_{i-1}$, then α_i is the root of a linear polynomial over F_{i-1}, thus its minimal polynomial and hence, the degree of $F_i = F(\alpha_i)$ over F_i, is 1. Otherwise, it is a root of the degree 2 polynomial $x^2 - \alpha_i^2 \in \mathbb{Q}[x] \subseteq F_{i-1}$ (since $\alpha_i^2 \in \mathbb{Q}$). Since it is not the root of a linear polynomial, $x^2 - \alpha_i^2$ is its minimal polynomial, thus $F_i = F(\alpha_i)$ has degree 2 over F_{i-1}. Therefore, $[F : \mathbb{Q}] = [F_n : F_{n-1}][F_{n-1} : F_{n-2}] \cdots [F_1 : F_0] = 2^k$ for some integer k.

We know that $\sqrt[3]{2}$ has degree 3 over $\mathbb{Q}$, since $x^3 - 2$ is irreducible over $\mathbb{Q}$ by Eisenstein's Criterion ($2 \mid 2$, but $2 \nmid 1$ and $2^2 \nmid 2$). Assume, for a contradiction, that $\sqrt[3]{2} \in F$. Then $\mathbb{Q} \subset F(\sqrt[3]{2}) \subseteq F$, thus $[F(\sqrt[3]{2}) : \mathbb{Q}] = 3$ divides $[F : \mathbb{Q}] = 2^k$, a contradiction.

□

3. (Exercise 14 in DF §13.2.) Let E/F be an extension and $\alpha \in E$ an element algebraic over F. Prove that if $[F(\alpha) : F]$ is odd, then $F(\alpha) = F(\alpha^2)$.

Proof. Let the degree of $F(\alpha)$ over F be $2n+1$. The set $\{1, \alpha, \alpha^2, \ldots, \alpha^{2n+1}\}$ forms a basis for $F(\alpha)$ over F. Thus, the set $\{1, \alpha^2, \alpha^4, \ldots, \alpha^{2n}\}$ is also linearly independent over F.

Since $\alpha^2 \in F(\alpha)$, we know that $F(\alpha^2) \subseteq F(\alpha)$. So the degree of $F(\alpha^2)$ over F must divide that of $F(\alpha)$ over F, which is odd. Odd numbers have no even divisors, so $[F(\alpha^2) : F]$ is odd. Therefore, $\{1, \alpha^2, \alpha^4, \ldots, \alpha^{2n}\}$ does not span $F(\alpha^2)$, since $2n$ is even.

Thus, there must be some other vector α^k, from the given basis for $F(\alpha)$, which is in $F(\alpha)^2$ (this follows from the "Replacement Theorem" of linear algebra). Since all even powers of α from that basis are already represented in $\{1, \alpha^2, \alpha^4, \ldots, \alpha^{2n}\}$, we know that k is odd. This also implies $k-1$ is even, thus $\alpha^{k-1} \in F(\alpha^2)$. So $\dfrac{\alpha^k}{\alpha^{k-1}} = \alpha \in F(\alpha^2)$, which gives that $F(\alpha) \subseteq F(\alpha^2)$. Clearly, $F(\alpha^2) \subseteq F(\alpha)$. So $F(\alpha) = F(\alpha^2)$.

□

4. (Exercise 16 in DF §13.2.) Let K/F be an algebraic extension and let R be a subring of K containing F. Show that R is a subfield of K containing F.

Proof. Since R is a subring of K, all we need to show is that it is closed under multiplicative inverses. Let α be a nonzero element of R. We know α is algebraic over F because R is contained within an algebraic extension of F. So α has a minimal polynomial $p(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0 \in F[x]$. If $c_0 = 0$, then either $p(x) = x$, implying that $\alpha = 0$ (which we have assumed is not the case), or $p(x) = xq(x)$ for some nonconstant polynomial $q(x) \in F[x]$, contradicting that $p(x)$ is irreducible. So $\frac{1}{c_0} \in F$.

We have

$$\begin{aligned} &\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0 = 0 \\ \implies &\alpha(c_n\alpha^{n-1} + \cdots + \alpha c_2 + c_1) = -c_0 \\ \implies &\frac{1}{\alpha} = -\frac{1}{c_0}(c_n\alpha^{n-1} + \cdots + \alpha c_2 + c_1). \end{aligned}$$

Since $\frac{1}{c_0}, c_1, \ldots, c_n \in F \subseteq R$ and $\alpha \in R$, the right hand side is an element of R, thus $\frac{1}{\alpha} \in R$.

□

5. (Exercise 17 in DF §13.2.) Let $f(x)$ be an irreducible polynomial of degree n over a field F. Let $g(x)$ be any polynomial in $F[x]$. Prove that every irreducible factor of the composite polynomial $f(g(x))$ has degree divisible by n.

Proof. Let $h(x) \in F[x]$ be an irreducible factor of $f(g(x))$ in $F[x]$. Since $f(x)$ and $h(x)$ are both irreducible, the degrees of the extensions $\dfrac{F[x]}{\big(f(x)\big)}$ and $\dfrac{F[x]}{\big(h(x)\big)}$ over F are the respective degrees of $f(x)$ and $h(x)$ as polynomials. Therefore, it suffices to show that $\dfrac{F[x]}{\big(f(x)\big)} \subseteq \dfrac{F[x]}{\big(h(x)\big)}$, since this will imply that $n \mid \left[\dfrac{F[x]}{\big(f(x)\big)} : F\right]\left[\dfrac{F[x]}{\big(h(x)\big)} : \dfrac{F[x]}{\big(f(x)\big)}\right] = \left[\dfrac{F[x]}{\big(h(x)\big)} : F\right] = \deg(h(x))$. This only requires finding an isomorphic copy of $\dfrac{F[x]}{\big(f(x)\big)}$ within $\dfrac{F[x]}{\big(h(x)\big)}$.

Define a map $\varphi : \dfrac{F[x]}{\big(f(x)\big)} \to \dfrac{F[x]}{\big(h(x)\big)}$ by $\overline{p(x)} \mapsto \overline{p(g(x))}$. To show this map is well-defined, assume $p(x) \in \big(f(x)\big)$, so that $p(x) = r(x)f(x)$ for some $r(x) \in F[x]$. Thus, $p(g(x)) = r(g(x))f(g(x)) \in \big(h(x)\big)$ because $h(x) \mid f(g(x))$.

It is clear that φ is a ring homomorphism: for any $p(x), q(x), r(x) \in F[x]$ we have $\varphi(p(x)q(x) + r(x)) = p(g(x))q(g(x)) + r(g(x)) = \varphi(p(x))\varphi(q(x)) + \varphi(r(x))$.

Now, assume for a contradiction that φ is the zero map. Then for the polynomial $p(x) = 1$, we have $\varphi(\overline{p(x)}) = \overline{p(g(x))} = \overline{1} = \big(h(x)\big)$. So $h(x)$ is a unit in $F[x]$ and thus a constant polynomial, contraditing that it is irreducible. So φ is injective, and thus an isomorphism onto a subfield of $\dfrac{F[x]}{\big(h(x)\big)}$. By the argument in the first paragraph, this completes the proof.

□

6. (Exercise 2 in DF §13.4.) Find a splitting field K for X^4+2 over $\mathbf{Q}$, and determine $[K:\mathbf{Q}]$.

Proof. We can form the splitting field K by adjoining all of the complex fourth roots of -2 to $\mathbb{Q}$. One of these is $\sqrt[4]{2}e^{i\pi/4} = \frac{1+i}{\sqrt[4]{2}}$. The others are $-\frac{1+i}{\sqrt[4]{2}}$ and $\pm i\frac{1+i}{\sqrt[4]{2}} = \pm\frac{-1+i}{\sqrt[4]{2}}$, where $\sqrt[4]{2}$ is taken to be the positve, real fourth root of 2. However, i can be formed by dividing two of these roots, and similarly any of the roots can be formed by multiplying $\frac{1+i}{\sqrt[4]{2}}$ by -1 or $\pm i$. Therefore, $K = \mathbb{Q}\left(\frac{1+i}{\sqrt[4]{2}}, i\right)$.

Since $\frac{1+i}{\sqrt[4]{2}}$ is a root of the irreducible polynomial x^4+2 (again, this can be shown to be irreducible by applying Eisenstein's criterion with $p=2$), we know that $\left[\mathbb{Q}\left(\frac{1+i}{\sqrt[4]{2}}\right):\mathbb{Q}\right] = 4$. If we can find the degree of K over $\mathbb{Q}\left(\frac{1+i}{\sqrt[4]{2}}\right)$, we can multiply it by 4 to obtain the degree of K over $\mathbb{Q}$.

Suppose, for a contradiction, that $i \in \mathbb{Q}\left(\frac{1+i}{\sqrt[4]{2}}\right) = \text{span}\left\{1, \frac{1+i}{\sqrt[4]{2}}, \left(\frac{1+i}{\sqrt[4]{2}}\right)^2, \left(\frac{1+i}{\sqrt[4]{2}}\right)^3\right\}$ (over $\mathbb{Q}$). Then there exist rational numbers a, b, c, and d such that

$$\begin{aligned} i &= a + b\left(\frac{1+i}{\sqrt[4]{2}}\right) + c\left(\frac{1+i}{\sqrt[4]{2}}\right)^2 + d\left(\frac{1+i}{\sqrt[4]{2}}\right)^3 \\ &= a + b\left(\frac{1+i}{\sqrt[4]{2}}\right) + c\sqrt{2}i + d\sqrt[4]{2}(-1+i). \\ &= a + b\frac{1}{\sqrt[4]{2}} + b\frac{1}{\sqrt[4]{2}}i + c\sqrt{2}i - d\sqrt[4]{2} + d\sqrt[4]{2}i \\ &= \left(a + b\frac{1}{\sqrt[4]{2}} - d\sqrt[4]{2}\right) + \left(b\frac{1}{\sqrt[4]{2}} + c\sqrt{2} + d\sqrt[4]{2}\right)i \end{aligned}$$

Since 1 and i are linearly independent over $\mathbb{R}$, the real part must equal 0 and the imaginary part must equal 1. Multiplying $a + b\frac{1}{\sqrt[4]{2}} - d\sqrt[4]{2} = 0$ through by $\sqrt[4]{2}$ gives

$$b + 2^{\frac{1}{4}}a - 2^{\frac{2}{4}}d = 0.$$

Since x^4-2 is irreducible over $\mathbb{Q}$, and $2^{\frac{1}{4}}$ is a root of this polynomial, we know that $\{1, 2^{\frac{1}{4}}, 2^{\frac{2}{4}}\}$ is linearly independent over $\mathbb{Q}$. Therefore, $a = b = d = 0$. Setting the imaginary part equal to 1 and substiting 0 for b and d gives $c\sqrt{2} = 1$, a contradiction because $\frac{1}{\sqrt{2}}$ is not rational.

Therefore, the degree of $K = \mathbb{Q}\left(\frac{1+i}{\sqrt[4]{2}}, i\right)$ over $\mathbb{Q}\left(\frac{1+i}{\sqrt[4]{2}}\right)$ is greater than 1. However, its degree does not exceed 2 since $\left[\mathbb{Q}\left(\frac{1+i}{\sqrt[4]{2}}\right)(i) : \mathbb{Q}\left(\frac{1+i}{\sqrt[4]{2}}\right)\right] \leq [\mathbb{Q}(i):\mathbb{Q}] = 2$. Therefore, the degree of K over $\mathbb{Q}\left(\frac{1+i}{\sqrt[4]{2}}\right)$ is 2. So

$$[K:\mathbb{Q}] = \left[K : \mathbb{Q}\left(\frac{1+i}{\sqrt[4]{2}}\right)\right]\left[\mathbb{Q}\left(\frac{1+i}{\sqrt[4]{2}}\right):\mathbb{Q}\right] = 4 \cdot 2 = 8.$$

□

7. (Exercise 3 in DF §13.4.) Find a splitting field K for X^4+X^2+1 over $\mathbf{Q}$, and determine $[K:\mathbf{Q}]$.

Proof. Descarte's rule of signs reveals that this polynomial has no real roots. However, we can apply the quadratic formula to find that $x^2 = \frac{-1\pm\sqrt{-3}}{2} = \zeta_3, \zeta_3^2$. The solutions to this equation give the set of roots of x^4+x^2+1: $\{\zeta_6, \zeta_6^2, \zeta_6^4, \zeta_6^5\} = \left\{\frac{\pm 1 \pm \sqrt{-3}}{2}\right\}$. We now see that $x^4+x^2+1 = (x-\zeta_6)(x-\zeta_6^5)(x-\zeta_6^4)(x-\zeta_6^2) = (x-\zeta_6)(x-\overline{\zeta_6})(x+\zeta_6)(x+\overline{\zeta_6}) = \left(x^2+x+1\right)\left(x^2-x+1\right)$ is reducible, although both of these quadratic factors are irreducible.

The splitting field K must be $\mathbb{Q}(\zeta_6)$, since K must contain ζ_6, but the other roots are powers of this element. The minimal polynomial for K is x^2+x-1, since its roots are ζ_6 and ζ_6^5, neither of which are rational (so this degree 2 polynomial has no linear factors, and is thus irreducible over $\mathbb{Q}$). Thus K has degree 2 over $\mathbb{Q}$.

□