MATH 6303 - Modern Algebra
Homework 2

Joel Sleeba

February 16, 2025

1. **Solution:** We notice that the roots of $x^4 - 2$ are $\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}$. Thus the splitting field of $x^4 - 2$ is a subfield of $\mathbb{Q}(\sqrt[4]{2}, i)$. Moreover the splitting field must contain $\sqrt[4]{2}, i = (i\sqrt[4]{2})(\sqrt[4]{2})^{-1}$. Thus we see that the splitting field is precisely $\mathbb{Q}(\sqrt[4]{2}, i)$.

   Now to find the degree of the splitting field, we observe that x^4-2 is irreducible by the Eisenstein criteria. Hence

$$[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})][\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 2 \times 4 = 8$$

2. **Solution:** We notice that the roots of $x^4 + 2$ are $\sqrt[4]{2}\omega_8^1$, $\sqrt[4]{2}\omega_8^3$, $\sqrt[4]{2}\omega_8^5$, $\sqrt[4]{2}\omega_8^7$, where ω_n is a primitive nth root of unity. Clearly the splitting field must contain $\sqrt[4]{2}\omega_8^1$ and $\omega_8^2 = \omega_4$, since $\omega_4 = \omega_8^2 = (\sqrt[4]{2}\omega_8^1)^{-1}\sqrt[4]{2}\omega_8^3$. Moreover any field which contain $\sqrt[4]{2}\omega_8, \omega_4$ will contain all the other roots. Hence we see that the splitting field of $x^4 - 2$ is $\mathbb{Q}(\sqrt[4]{2}\omega_8, \omega_4)$.

   Without loss of generality, assume that $\omega_8 = \frac{1+i}{\sqrt{2}}$, and $\omega_4 = i$. As $\omega_4 = \omega_8^2$, clearly $\mathbb{Q}(\sqrt[4]{2}\omega_8, \omega_4) \subset \mathbb{Q}(\sqrt[4]{2}, \omega_8)$. Since

$$\omega_4 = i = (1 + i) - 1 = (\sqrt[4]{2})^2 \frac{(1 + i)}{\sqrt{2}} - 1 = \sqrt[4]{2}^2 \omega_8 - 1$$

   we get that

$$\sqrt[4]{2} = \frac{\omega_4 + 1}{\sqrt[4]{2}\omega_8} \in \mathbb{Q}(\sqrt[4]{2}\omega_8, \omega_4)$$

and

$$\omega_8 = \frac{(1+i)}{\sqrt{2}} = \frac{1+\omega_4}{\sqrt[4]{2}^2} \in \mathbb{Q}(\sqrt[4]{2}\omega_8, \omega_4) \tag{1}$$

Hence, we see that $\mathbb{Q}(\sqrt[4]{2}\omega_8, \omega_4) = \mathbb{Q}(\sqrt[4]{2}, \omega_8)$ is the splitting field of $x^4 - 2$

Again, clearly $\mathbb{Q}(\sqrt[4]{2}, \omega_4) \subset \mathbb{Q}(\sqrt[4]{2}, \omega_8)$ as $\omega_8^2 = \omega_4$. But Equation 1 gives the converse and hence $\mathbb{Q}(\sqrt[4]{2}, \omega_4) = \mathbb{Q}(\sqrt[4]{2}, \omega_8)$. Thus, the splitting field of $x^4 + 2$ is again $\mathbb{Q}(\sqrt[4]{2}, i)$, and from the previous question we see that the degree of the extension of again 8.

3. **Solution:** Since we are well aware of the roots of the polynomial $x^2 + x + 1$ to be ω, ω^2, where $\omega = e^{i\frac{2\pi}{3}}$. We see that the roots of the polynomial $x^4 + x^2 + 1$ are $\pm\omega, \pm\omega^2$, where $\omega = e^{i\frac{\pi}{3}}$. Thus we see that the splitting field of the polynomial $x^4 + x^2 + 1$ is $\mathbb{Q}(e^{i\frac{\pi}{3}})$.

   Now since the degree of the extension is the same as the degree of the minimal polynomial in $\mathbb{Q}[x]$ for $e^{i\frac{\pi}{3}}$, we look for the minimal polynomial of $e^{i\frac{\pi}{3}}$. We know that to be $x^2 - x + 1$. Hence we see that the splitting field of $x^4 + x^2 + 1$ is of degree 2 over $\mathbb{Q}$.

4. **Solution:** We notice that the roots of $x^6 - 4$ are $\pm\sqrt[3]{2}, \pm\sqrt[3]{2}\omega, \pm\sqrt[3]{2}\omega^2$, where $\omega = e^{i\frac{2\pi}{3}}$. Thus the splitting field of $x^6 - 4$ is $\mathbb{Q}(\sqrt[3]{2}, \omega)$.

   Now to find the degree of the splitting field, we observe that $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ as $x^3 - 2$ is irreducible in $\mathbb{Q}$. Moreover $x^2 + x + 1$ is irreducible in $\mathbb{Q}(\sqrt[3]{2})$ as the polynomial only have complex roots, ω, ω^2. Hence we get that $[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}(\sqrt[3]{2})] = 2$. Now using the tower law, we get the degree of the splitting field to be 6.

5. **Solution:** Let $x \in \mathbb{F}_{p^s}$ be an n-th root of unity where $n = p^k m$ with $\gcd(p, m) = 1$. Then

$$x^{p^k m} = (x^m)^{p^k} = 1$$

   Since we'll show that $x \to x^p$ is a Field isomorphism in the next question, we see that this implies $x^m = 1$. Thus every n-th root of unity is an m-th root of unity. Converse is easy to see as if $x^m = 1$, then $x^n = (x^m)^{p^k} = 1$. Thus n-th roots of unity in $\mathbb{F}_{p^s}$ are precisely the m-th roots of unity. Thus every

n-th root of unity are precisely the roots of the polynomial $f(x) = x^m - 1$. As $\gcd(m, p) = 1$, the only root of $D_f(x) = mx^{m-1}$ is 0, and 0 is not a root of f, we see that f is separable. Hence f has m distinct roots, which gives a proof for the statement.

6. **Solution:** Since we have shown in class that $(a+b)^p = a^p + b^p$ for fields of characteristic p, and $(ab)^p = a^p b^p$ by the commutativity of the ring operation, we see that the map $\phi : x \mapsto x^p$ is a field endomorphism on $\mathbb{F}_{p^n}$. Again since $\mathbb{F}_{p^n}$ is an integral domain, $x^p = 0$ forces $x = 0$. Hence the map is an injective endomorphism. Since an injective endomorphism between finite spaces are bijective, $x \mapsto x^p$ is a field automorphism.

   Now let $\phi^m : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n} := x \mapsto x^{p^m}$ for some $m \in \mathbb{N}$. We'll show that ϕ^m is the identity map if and only if $n|m$. Since we know that the multiplicative group of $\mathbb{F}_{p^n}$ has $p^n - 1$ elements, from group theory, we get that $x^{p^n-1} = 1$ for all $x \in \mathbb{F}^*_{p^n}$. Thus $x^{p^n} = x$ for all $x \in \mathbb{F}_{p^n}$. Thus, ϕ^n is the identity map, and ϕ^{kn} is an identity map for all $k \in \mathbb{N}$.

   Since we know that the mulitiplicative group of a finite field is cyclic, let $F^*_{p^n} = \langle x_0 \rangle$. Now, if for some $m \in \mathbb{N}$, $x^{p^m} = x$ for all $x \in \mathbb{F}_{p^n}$, then this would force $x_0^{p^m-1} = 1$, while $|x_0| = p^n - 1$. Thus $(p^n - 1)|(p^m - 1)$, which happens only if $n|m$