Advanced Algebra II HW2

Sean Eli

January 30, 2022

Problem 1. Determine the splitting field of $p(x) = x^4 + 2$ over $\mathbb{Q}$. What is its degree over $\mathbb{Q}$? is i contained in this splitting field?

Proof. Let $\omega = e^{i\pi/4} \in \mathbb{C}$, so the roots for $p(x)$ in $\mathbb{C}$ are $\omega\sqrt[4]{2}, \omega^3\sqrt[4]{2}, \omega^5\sqrt[4]{2}$, and $\omega^7\sqrt[4]{2}$. These all belong to $\mathbb{Q}(\omega, \sqrt[4]{2})$. The polynomial $p(x)$ is irreducible over $\mathbb{Q}$ by Eisenstein, therefore $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$. Also we can check that $\omega = \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i$: since $\sqrt{2} \in \mathbb{Q}(\sqrt[4]{2})$, it follows that

$$\mathbb{Q}(\omega, \sqrt[4]{2}) = \mathbb{Q}(i, \sqrt[4]{2}).$$

Therefore $[\mathbb{Q}(i, \sqrt[4]{2}) : \mathbb{Q}] \leq 8$ and is divisible by 4. We also have that $\mathbb{Q}(\sqrt[4]{2}) \subsetneq \mathbb{Q}(i, \sqrt[4]{2})$ since the smaller field is contained in $\mathbb{R}$, therefore $[\mathbb{Q}(i, \sqrt[4]{2}) : \mathbb{Q}] = 8$.

To see that $\mathbb{Q}(i, \sqrt[4]{2})$ is minimal, notice the roots $\left\{\omega\sqrt[4]{2}, \omega^3\sqrt[4]{2}, \omega^5\sqrt[4]{2}, \omega^7\sqrt[4]{2}\right\}$ are the same numbers as $\left\{\pm\frac{1}{\sqrt[4]{2}} \pm \frac{1}{\sqrt[4]{2}}i\right\}$. By adding pairs of these we see that the splitting field of $p(x)$ over $\mathbb{Q}$ must contain $\sqrt[4]{2}$ and $\frac{i}{\sqrt[4]{2}}$, and therefore contains $\mathbb{Q}(i, \sqrt[4]{2})$. ∎

Problem 2. Let $\zeta_n = e^{2\pi i/n}$. Show $\zeta_5 \notin \mathbb{Q}(\zeta_7)$.

Proof. We have seen that $[\mathbb{Q}(\zeta_7) : \mathbb{Q}] = 6$ and $[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = 4$. If $\zeta_5 \in \mathbb{Q}(\zeta_7)$ then $\mathbb{Q}(\zeta_5, \zeta_7) = \mathbb{Q}(\zeta_7)$, and by the tower law

$$\begin{aligned} 6 = [\mathbb{Q}(\zeta_5, \zeta_7) : \mathbb{Q}] &= [\mathbb{Q}(\zeta_5, \zeta_7) : \mathbb{Q}(\zeta_5)]\ [\mathbb{Q}(\zeta_5) : \mathbb{Q}] \\ &= [\mathbb{Q}(\zeta_5, \zeta_7) : \mathbb{Q}(\zeta_5)] \cdot 4. \end{aligned}$$

Thus 4 divides 6, a contradiction. ∎

Problem 3. Let K/F be a finite field extension. Show that K is a splitting field over F iff every irreducible $p(x) \in F[x]$ with a root in K splits completely in $K[x]$.

Proof. ($\Leftarrow$) Suppose every irreducible $p(x) \in F[x]$ with a root in K splits completely in $K[x]$. Since K is a finite extension of F, there exists a basis $\alpha_1, ..., \alpha_n$ of K/F. Since each minimal polynomial $\min_{\alpha_i,F}(x)$ splits in $K[x]$, K contains all roots of

$$g(x) := \min_{\alpha_1,F}(x) \dots \min_{\alpha_n,F}(x).$$

K is the splitting field for $g(x)$ over F, since if L/F is any extension such that L contains all roots of $g(x)$, then L contains $F(\alpha_1, ..., \alpha_n) \cong K$.

($\Rightarrow$) Suppose K is the splitting field of a general polynomial $f(x) \in F[x]$, and let $p(x) \in F[x]$ be an irreducible polynomial with a root $\alpha \in K$. If β is another root of $p(x)$ (that lives in the splitting field for $p(x)$ over F) then there exists a field isomorphism $\phi : F(\alpha) \to F(\beta)$ which fixes F.

Write $f_\alpha(x) := f(x) \in F(\alpha)[x]$ and $f_\beta(x) := f(x) \in F(\beta)[x]$, and let K_α and K_β be splitting fields of $f_\alpha(x)$ and $f_\beta(x)$ over $F(\alpha)$ and $F(\beta)$, respectively. Since $\phi|_F = \mathrm{id}$, the ring isomorphism $F(\alpha)[x] \to F(\beta)[x]$ induced by ϕ sends $f_\alpha(x)$ to $f_\beta(x)$. By Theorem 27 in Dummit & Foote, ϕ extends to an isomorphism $\tilde{\phi} : K_\alpha \to K_\beta$ of the splitting fields. Since we assumed $\alpha \in K$, we have $F(\alpha) \subset K$, and by applying the argument above to the identity map $F(\alpha) \to F(\alpha)$ it follows that $K_\alpha \cong K$. To summarize, all rows are isomorphisms in the following:

$$\begin{tikzcd}
K \arrow[r, "\cong"] & K_\alpha \arrow[r, "\tilde{\phi}"] & K_\beta \\
F(\alpha) \arrow[u] \arrow[r, "\mathrm{id}"] & F(\alpha) \arrow[u] \arrow[r, "\phi"] & F(\beta) \arrow[u] \\
& F \arrow[ul] \arrow[u] \arrow[ur] &
\end{tikzcd}$$

Consider adjoining β to K:

$$\begin{tikzcd}
K(\beta) \arrow[r, dashed] & K_\beta(\beta) = K_\beta \\
K \arrow[u] \arrow[r, "\cong"] & K_\beta \arrow[u]
\end{tikzcd}$$

The isomorphism $K \to K_\beta$ induces an isomorphism of the extensions $K(\beta) \to K_\beta$, and it follows that $[K(\beta) : K] = [K_\beta : K_\beta] = 1$. Thus $\beta \in K$. This is true for any root of $p(x)$ so p splits over K. $\blacksquare$

Problem 4. Let K_1 and K_2 be finite extensions of a field F contained in a field K. Suppose K_1 and K_2 are both splitting fields. Show $K_1 \cap K_2$ and K_1K_2 are splitting fields over F.

Proof. Suppose K_1 and K_2 are splitting fields for polynomials $f_1(x), f_2(x) \in F[x]$, respectively. Let L be the splitting field for $p(x) = f_1(x)f_2(x)$; since K_1K_2 contains all roots of f_1 and f_2, $L \subset K_1K_2$. But since $f_1(x)$ splits over L, $K_1 \subset L$. Similarly $K_2 \subset L$ therefore $K_1K_2 \subset L$.

Notice $K_1 \cap K_2$ is a finite extension of F. To see that $K_1 \cap K_2$ is a splitting field, suppose $p(x) \in F[x]$ is irreducible over F, and has a root $\alpha \in K_1 \cap K_2$. Since K_1 and K_2 are splitting fields, $p(x)$ splits into linear factors over K_1 and over K_2, i.e. all roots of $p(x)$ are in $K_1 \cap K_2$. By the previous exercise, $K_1 \cap K_2$ is a splitting field. ■

Problem 5. Let $a \geq 2$ and let n, d be positive integers. Show $d|n$ iff $a^d - 1|a^n - 1$. Conclude that containment of finite fields $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^n}$ is possible iff $d|n$.

Proof.

■

Problem 6. Let p be a prime number. Show $f(x)^p = f(x^p)$ for any $f(x) \in \mathbb{F}_p[x]$.

Proof. The binomial theorem shows $(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k}$; the binomial coefficient is divisible by p iff $k \neq 0$ or p, so in $\mathbb{F}_p$ we have $(x+y)^p = x^p + y^p$. Thus if $f(x) = a_n x^n + ... + a_1 x + a_0 \in \mathbb{F}_p[x]$,

$$(a_n x^n + ... + a_1 x + a_0)^p = a_n^p (x^p)^n + a_{n-1}^p (x^p)^{n-1} + ... + a_0^p.$$

By Fermat's little theorem, $a^p \equiv a \bmod p$ whenever $a \in \mathbb{Z}$ and p is prime, thus $x^p = x$ in $\mathbb{F}_p$. This means the pth powers of coefficients above are just $a_n, ..., a_0$, and we have shown $f(x)^p = f(x^p)$. ■

Problem 7. Let K be a field of characteristic p which is not perfect, i.e. $K \neq K^p$. Prove there exists an irreducible inseparable polynomial in $K[x]$. Conclude there exists finite inseparable extensions of K.

Proof. If $K \neq K^p$ there exists $\alpha \in K$ which is not a p-th power: then the polynomial $f(x) = x^p - \alpha \in K[x]$ is inseparable, since $D_x f(x) = 0$, and thus α is a root of $f(x)$ and $D_x f(x)$. To see that $f(x)$ is irreducible,

■