Math 121, Winter 2023, Homework 3 Solutions

Section 9.4

Problem 2d. *Let p be an odd prime. Prove that the polynomial $f(x) = \frac{(x+2)^p - 2^p}{x}$ is irreducible in $\mathbb{Z}[x]$.*

Solution. First notice that f is indeed a polynomial since the numerator has zero constant term. In fact, by the binomial theorem,

$$f(x) = \sum_{j=1}^{p} \binom{p}{j} x^{j-1} 2^{p-j}.$$

This is a monic polynomial where every lower-degree coefficient is a multiple of p, and the constant term is $2^{p-1}p$, which since p is odd is not a multiple of p^2. Therefore, $f(x)$ satisfies the conditions for Eisenstein's criterion, so is irreducible.

Problem 10. *Prove that the polynomial $p(x) = x^4 - 4x^2 + 8x + 2$ is irreducible over the quadratic field $F = \mathbb{Q}(\sqrt{-2}) = \{a + b\sqrt{-2} | a, b \in \mathbb{Q}\}$.*

Solution. See the hint in Dummit & Foote. By Gauss' Lemma (technically, by Corolalry 6 in Chapter 9), we only need to show that $p(x)$ is irreducible over $R = \mathbb{Z}(\sqrt{-2})$. Since R is a UFD, we can apply similar reasoning to Proposition 11 in Chapter 9. If $\alpha \in R$ is a root of p, then we have

$$2 = -\alpha^4 + 4\alpha^2 - 8\alpha = \alpha(-\alpha^3 + 4\alpha - 8),$$

so $\alpha | 2$ in R. The only elements of R dividing 2 are $\pm 1, \pm\sqrt{2}, \pm 2$, so these are the only possible roots of $p(x)$. To see this consider the multiplicative group homomorphism $\phi : R^\times \to \mathbb{Z}^\times$, $\phi(a) = a^2$; we have $\phi(2) = 4$, and $\pm 1, \pm\sqrt{-2}, \pm 2$ are the only elements of R with squared-absolute-value equal to a divisor of 4). Plugging these in, we see that none of them is a root.

To show that $p(x)$ can't be factored as a product of quadratics, assume it can i.e. $p(x) = (x^2 + ax + b)(x^2 + cx + d)$ with $a, b, c, d \in R$ (the fact that these factors can be assumed monic is a consequence of Gauss' Lemma that was mentioned in class). Multiplying this out, we see that $bd = 2$, $ad + bc = 8$, $ac + b + d = -4$, and $a + c = 0$. Therefore, $c = -a$, so $a(d - b) = 8$, so $\frac{-64}{(d-b)^2} + b + d = 4$, and note that $b, d \in \{\pm 1, \pm\sqrt{-2}, \pm 2\}$. Since $\frac{-64}{(d-b)^2} \in \mathbb{Z}$, so must be $b+d$, so either $b = -d = \pm\sqrt{-2}$ or $b, d \in \mathbb{Z}$. In the first case, plugging in shows the equation is not satisfied, and in the second case, $\frac{-64}{(d-b)^2} < 0$, and since $b + d \leq 4$, the equation is still not satisfied.

Problem 12. *Prove that $f(x)x^{n-1} + x^{n-2} + \cdots + x + 1$ is irreducible over $\mathbb{Z}$ if and only if n is a prime.*

Solution. The case $n = 1$ is trivial, since constant functions are units, and not considered irreducible. See Example 4 on page 310 for the case where n is prime. If n is composite, say $p = ab$, $f(x)$ factors as

$$f(x) = (x^{a-1} + x^{a-2} + \ldots + x + 1)(x^{a(b-1)} + x^{a(b-2)} + \ldots + x^a + 1).$$

Section 13.4

Problem 1. *Determine the splitting field and its degree over $\mathbb{Q}$ for $f(x) = x^4 - 2$.*

Solution. Let K be the desired splitting field. As usual, let $\sqrt[4]{2}$ be the positive real fourth root of 2. Then, using polar coordinates, the roots for $f(x)$ are $e^{2\pi ia/4} \cdot \sqrt[4]{2}, 0 \leq a < 4$ i.e. $\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}$. This means that $i = \frac{i\sqrt[4]{2}}{\sqrt[4]{2}} \in K$, and conversely, $i\sqrt[4]{2} \in \mathbb{Q}(\sqrt[4]{2}, i)$. Therefore, $K = \mathbb{Q}(\sqrt[4]{2}, i)$.

Using the tower law,

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt[4]{2})][\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}].$$

The latter factor is 4 since $x^4 - 2$ is irreducible. The former factor is ≤ 2 since the minimal polynomial for i over $\mathbb{Q}$ is $x^2 + 1$, so the minimal polynomial for i over $\mathbb{Q}(\sqrt[4]{2})$ must divide this. However, $i \notin \mathbb{Q}(\sqrt[4]{2})$ since $\mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{R}$, so the degree must be 2. Therefore, $[K : \mathbb{Q}] = 8$.

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

Solution. Let K be the desired splitting field. Surprisingly, $K = \mathbb{Q}(\sqrt[4]{2}, i)$, so the answer is the same as the previous problem.

Let ζ be a primitive 8th root of unity (we could make the process go faster by using coordinates, but I want to emphasize that knowledge of the roots isn't always necessary). Then $\zeta\sqrt[8]{4} = \zeta\sqrt[4]{2}$ is a root of $x^8 - 4 = (x^4 + 2)(x^4 - 2)$, but $\zeta^4 = -1$ (since it can't equal 1), so $\zeta\sqrt[4]{2}$ must be a root of x^4+2. Thus, the four roots of this polynomial are $\zeta^a\sqrt[4]{2}$, $a = 1, 3, 5, 7$.

To show that $K = \mathbb{Q}(\sqrt[4]{2}, i)$, note that $\frac{\zeta^3\sqrt[4]{2}}{\zeta\sqrt[4]{2}} = \zeta^2 = \pm i$, so $i \in K$, and $\sqrt{2} = \pm i \cdot (\zeta\sqrt[4]{2})^2 \in K$

a well. Also, $(\zeta + \zeta^7)^4 = \zeta^4 + 4\zeta^{10} + 6\zeta^{16} + 4\zeta^{22} + \zeta^{28} = 4$, so

$$\frac{1}{\sqrt{2}}(\zeta\sqrt[4]{2} + \zeta^7\sqrt[4]{2}) = \frac{\zeta}{\sqrt[4]{2}} + \frac{\zeta^7}{\sqrt[4]{2}}$$

is a 4th root of 2. After multiplication by a power of ζ^2, we see that $\sqrt[4]{2} \in K$.

On the other hand, one can check that $\sqrt[4]{2} + i\sqrt[4]{2}$ is a primitive 8th root of unity, and by multiplying by powers of i, $\mathbb{Q}(\sqrt[4]{2})$ contains all four primitive 8th roots of unity, so $K = \mathbb{Q}(\sqrt[4]{2})$.

Problem 3. *Determine the splitting field and its degree over* $\mathbb{Q}$ *for* $f(x) = x^4 + x^2 + 1$.

Solution. Let $g(x) = x^2+x+1$. Then $f(x) = g(x^2)$. Since $g(x)$ is the cyclotomic polynomial of primitive cube roots of 1, its roots are $e^{\pm 2\pi i/3}$, so the roots of f are sixth roots of unity that square to these i.e. the roots of f are $e^{\pm 2\pi i/3}$ and $e^{\pm 2\pi i/6}$. Noting that some of these roots are primitive, the splitting field for f is the cyclotomic extension $\mathbb{Q}(\zeta_6) = \mathbb{Q}(e^{2\pi i/6})$. The minimal polynomial for $e^{2\pi i/6}$ is the cyclotomic polynomial $\Phi_6(x) = x^2 - x + 1$, so the extension is degree 2.

Problem 5. *Let* K *be a finite extension of* F. *Prove that* K *is a splitting field over* F *if and only if every irreducible polynomial in* $F[x]$ *that has a root in* K *splits completely in* $K[x]$.

Solution. Certainly, the second condition implies the first. Note that this result holds even in the case where $K = F$, since F is the splitting field for all linear polynomials, but has no roots of irreducible polynomials of higher degree.

For the other direction, assume that K is a splitting field over F for the irreducible polynomial $g(x) \in F[x]$. Let $f(x) \in F[x]$ be irreducible, and let $\alpha \in K$ be a root of f. Let β be any root of f. Then by Theorem 8 of Dummit and Foote, there is a field isomorphism $\varphi : F(\alpha) \to F(\beta)$ fixing F (and therefore f) and sending α to β. Let K' be a splitting field for g over $F(\beta)$, and note that K is a splitting field for g over $F(\alpha)$. Then by Theorem 27 of Dummit and Foote, there is an isomorphism between K and K' extending φ (so fixing F). On the other hand, $K(\beta)$ is a splitting field for g over $F(\beta)$, so again by Theorem 27 there is an isomorphism between $K(\beta)$ and K' fixing F and β. This means that there is an isomorphism between K and $K(\beta)$ fixing F, so the degrees $[K(\beta) : F] = [K : F]$, so, we must have $K = K(\beta)$ and $\beta \in K$.

Problem 6. *Let* K_1 *and* K_2 *be finite extensions of* F *contained in the field* K, *and assume both are splitting fields over* F.

a. *Prove that their composite* K_1K_2 *is a splitting field over* F.

Solution. If K_1 is a splitting field (over F) for f_1 and K_2 is a splitting field for f_2, then the splitting field E for $f_1 f_2$ is the intersection of all fields containing F and all the roots of both f_1 and f_2. E must contain K_1 since it is the intersection of all fields containing F and the roots of f_1, and similarly for K_2. On the other hand, $f_1 f_2$ splits over any field containing both K_1 and K_2, so E is the smallest field containing K_1 and K_2, which by definition is the composite $K_1 K_2$.

b. *Prove that $K_1 \cap K_2$ is a splitting field over F.*

Solution. Let $g(x)$ be an irreducible polynomial in $F[x]$ with a root in $K_1 \cap K_2$. We will show that $g(x)$ splits over $K_1 \cap K_2$, so by the previous problem, $K_1 \cap K_2$ is a splitting field. Since K_1 and K_2 are splitting fields containing a root of $g(x)$, it must be the case that $g(x)$ splits in both K_1 and K_2. But since $K[x]$ is a UFD, these factorizations must be identical (up to units and order), so every factor must be contained in $(K_1 \cap K_2)[x]$, so g splits over $K_1 \cap K_2$.