Math 418, Spring 2024 – Homework 3

Due: Wednesday, February 7th, at 9:00am via Gradescope.

Instructions: Students should complete and submit all problems. Textbook problems are from Dummit and Foote, *Abstract Algebra, 3rd Edition.* All assertions require proof, unless otherwise stated. Typesetting your homework using LaTeX is recommended, and will gain you 2 bonus points per assignment.

1. **Dummit and Foote #9.3.2:** *Prove that if $f(x)$ and $g(x)$ are polynomials with rational coefficients whose product $f(x)g(x)$ has integer coefficients, then the product of any coefficient of $g(x)$ with any coefficient of $f(x)$ is an integer.*

   Proof. By Gauss' Lemma, since $p(x) := f(x)g(x)$ factors over $\mathbb{Q}$, it factors over $\mathbb{Z}$, and moreover, there exists $\frac{m}{n} \in \mathbb{Q}$ such that $\frac{m}{n}f(x) \in \mathbb{Z}[x]$ and $\frac{n}{m} \in \mathbb{Z}[x]$. Let a be any coefficient of $f(x)$ and b be any coefficient of $g(x)$. Then $\frac{m}{n} \cdot a \in \mathbb{Z}$ and $\frac{n}{m} \cdot b \in \mathbb{Z}$, so $ab = \frac{m}{n}a\frac{n}{m}b \in \mathbb{Z}$. □

2. **Dummit and Foote #9.4.2d:** *Let p be an odd prime. Prove that the polynomial $f(x) = \frac{(x+2)^p - 2^p}{x}$ is irreducible in $\mathbb{Z}[x]$.*

   Proof. 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. □

3. **Dummit and Foote #9.4.10:** *Prove that the polynomial $p(x) = x^4 - 4x^2 + 8x + 2$ is irreducible over the quadratic field $F = \mathbb{Q}(\sqrt{-2}) = \{a + b\sqrt{-2} | a, b \in \mathbb{Q}\}$.*

   Proof. See the hint in Dummit & Foote. By Gauss' Lemma (technically, by Corollary 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. □

4. **Dummit and Foote #9.4.12:** *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.*

   Proof. 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

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

   □

5. **Dummit and Foote #13.1.1:** *Show that* $p(x) = x^3 + 9x + 6$ *is irreducible in* $\mathbb{Q}[x]$. *Let* θ *be a root of* $p(x)$. *Find the inverse of* $1 + \theta$ *in* $\mathbb{Q}(\theta)$ *as a polynomial in* θ

   Solution. By Proposition 9.10 of Dummit and Foote, $p(x)$ is reducible in $\mathbb{Q}[x]$ if and only if it has a root in $\mathbb{Q}$. By the Rational Root Theorem, if $r = a/b \in \mathbb{Q}$, then a divides the constant term, 6, of p, and b divides the coefficient, 1, of the top degree term of p. Therefore, r must equal $\pm 1, \pm 2, \pm 3$, or ± 6. Plugging these values into $p(x)$ shows that none of them are roots, so p is irreducible.

   Alternatively, we can use Eisenstein's criterion. All coefficients in $p(x)$ are divisible by 3 except for the top degree term, and the constant term is not divisible by 9. Therefore, $p(x)$ satisfies the hypotheses of Eisenstein's criterion, so is irreducible.

   Now, the inverse of $1 + \theta$ in $\mathbb{Q}(\theta)$ is some $\mathbb{Q}$-linear combination $a + b\theta + c\theta^2$ of $1, \theta$, and θ^2, since these form a basis for $\mathbb{Q}(\theta)$ over $\mathbb{Q}$. Since θ is a root of p, $\theta^3 = -9\theta - 6$, so

   $$(1 + \theta)(a + b\theta + c\theta^2) = a + (a + b)\theta + (b + c)\theta^2 + c\theta^3 = a - 6c + (a + b - 9c)\theta + (b + c)\theta^2.$$

   For $a + b\theta + c\theta^2$ to be the inverse of $1 + \theta$, this expression must equal 1, and solving the resulting system of equations gives $a = \frac{5}{2}, b = -\frac{1}{4}, c = \frac{1}{4}$, so $\theta^{-1} = \frac{5}{2} - \frac{1}{4}\theta + \frac{1}{4}\theta^2$.

6. **Dummit and Foote #13.1.3:** *Show that $p(x) = x^3 + x + 1$ is irreducible over $\mathbb{F}_2$ and let θ be a root. Compute the powers of θ in $\mathbb{F}_2(\theta)$ as polynomials in θ.*

   Solution. Once again, $p(x)$ is irreducible unless it has a root. $\mathbb{F}_2$ only has two elements, so we plug them both in and find that neither is a root: $p(0) = p(1) = 1$. Therefore, $p(x)$ is irreducible.

   To compute the powers of θ, note that θ is a root of p, so $\theta^3 = -\theta - 1 = \theta + 1$, since in $\mathbb{F}_2$, 1 and -1 are equal!. Then

$$\theta^4 = \theta(\theta + 1) = \theta^2 + \theta, \qquad \theta^5 = \theta(\theta^2 + \theta) = \theta^2 + \theta + 1,$$

$$\theta^6 = \theta(\theta^2 + \theta + 1) = \theta^2 + 1, \qquad \theta^7 = \theta(\theta^2 + 1) = 1,$$

   and the powers of θ repeat from there via the relationship $\theta^n = \theta^7\theta^{n-7} = \theta^{n-7}$, so that $\theta^{7i+j} = \theta^j$.

7. **Dummit and Foote #13.1.4:** *Prove directly that the map $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ is an isomorphism of $\mathbb{Q}(\sqrt{2})$ with itself.*

   Solution. Let φ be the given map. Since $\varphi(\varphi(a + b\sqrt{2})) = \varphi(a - b\sqrt{2}) = a + b\sqrt{2}$, $\varphi \circ \varphi$ is the identity map, so it is its own inverse, and therefore a bijection.

   The following computations show that φ is a ring homomorphism:

$$\varphi((a+b\sqrt{2})+(c+d\sqrt{2})) = \varphi(a+c+(b+d)\sqrt{2}) = a+c-(b+d)\sqrt{2} = \varphi(a+b\sqrt{2})+\varphi(c+d\sqrt{2}),$$

$$\varphi((a+b\sqrt{2})(c+d\sqrt{2})) = \varphi(ac+2bd+(ad+bc)\sqrt{2}) = ac+2bd-(ad+bc)\sqrt{2} = \varphi(a+b\sqrt{2})\varphi(c+d\sqrt{2}),$$

   and we don't need to check that $\varphi(1) = 1$ since $\mathbb{Q}(\sqrt{2})$ is a field.

   Note that φ is the isomorphism given in Theorem 8.