MATH 4000/6000 – Homework #5

posted March 11, 2024; due by midnight on March 18, 2024

Algebra is but written geometry and geometry is but written algebra. – Sophie Germain

Assignments are expected to be neat and stapled. **Illegible work may not be marked**. Starred problems (*) are required for those in MATH 6000 and extra credit for those in MATH 4000.

1. By applying the Euclidean algorithm and then backtracking, determine $X(x), Y(x) \in \mathbb{Q}[x]$ with $(x^3+1)X(x)+(x^2+1)Y(x)=1$. Then repeat the exercise with $\mathbb{Q}[x]$ replaced by $\mathbb{Z}_5[x]$.

2. Let F be a field. Prove that the units in $F[x]$ are precisely the nonzero elements of F.

3. Let F be a field. Recall the definition of greatest common divisor (gcd) in $F[x]$: a gcd of $a(x), b(x)$ is a common divisor of $a(x)$ and $b(x)$ in $F[x]$ that is divisible by every common divisor in $F[x]$.

   Show that if $d(x) \in F[x]$ is a gcd of $a(x), b(x)$, then so is $c \cdot d(x)$ for every nonzero $c \in F$. Conversely, show that every gcd of $a(x), b(x)$ has the form $c \cdot d(x)$ for some nonzero $c \in F$.

4. Let F be a field. In class we showed that every nonconstant polynomial in $F[x]$ can be written as a product of irreducibles. Prove that this representation is unique in the sense discussed in class; that is, show the following claim.

   If $f(x) \in F[x]$ is nonconstant and

   $$\begin{aligned} f(x) &= p_1(x) \cdots p_k(x) \\ &= q_1(x) \cdots q_\ell(x), \end{aligned}$$

   with all the $p_i(x)$ and $q_j(x)$ irreducible, then $k=\ell$ and after rearranging there are nonzero constants $c_1, \dots, c_k$ with

   $$p_i(x) = c_i \cdot q_i(x) \quad \text{for all } i = 1, 2, 3, \dots, k.$$

   Hint. Imitate the proof of uniqueness in $\mathbb{Z}$. Proceed by contradiction, choosing a counterexample of smallest degree.

5. Later in the course we will construct a field K with 4 elements containing $\mathbb{Z}_2$ as subfield. In this exercise, *assume* K is such a field. Then in addition to $0, 1$ from $\mathbb{Z}_2$, the field K has two extra elements; call these α and β.

   (a) Show that $\alpha + 1 = \beta$.
   Hint. Try process of elimination.

   (b) Show that $\alpha^2 = \beta$.

   (c) Show that both α and β are roots of x^2+x+1 and deduce that $x^2+x+1 = (x-\alpha)(x-\beta)$ in $K[x]$.

6. Let F be a subfield of K, and let $\alpha \in K$. Suppose that α is a root of the irreducible polynomial $p(x) \in F[x]$. Let n be the degree of $p(x)$. Show that every element of $F[\alpha]$ has a *unique* representation in the form

   $$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1},$$

   where $a_0, a_1, \dots, a_{n-1} \in F$.

   Hint: We [will have] proved this in class without the uniqueness requirement. So your only job is to prove uniqueness.

7. (a) Let $\sqrt{2}, \sqrt{3}$ denote the positive real square roots of 2 and 3, respectively. Prove that $\sqrt{3} \notin \mathbb{Q}[\sqrt{2}]$.

   (b) Prove that $\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \mathbb{Q}[\sqrt{2} + \sqrt{3}]$.

   Hint: Show containment both ways. One direction is fairly easy: Since $\sqrt{2}, \sqrt{3} \in \mathbb{Q}[\sqrt{2}, \sqrt{3}]$, and $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ is closed under addition (being a ring), we have $\sqrt{2}+\sqrt{3} \in \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. Since $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ contains both $\mathbb{Q}$ and $\sqrt{2}+\sqrt{3}$, and is closed under addition and multiplication (being a ring), it follows that $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ contains $\mathbb{Q}[\sqrt{2} + \sqrt{3}]$. Can you find a similar argument for the other containment?

8. Let F be a subfield of K, and suppose $\alpha \in K$ is not algebraic over F.[1] Prove that α has no multiplicative inverse in $F[\alpha]$. Deduce that $F[\alpha]$ is not a field.

9. (***; MATH 6000 problem**) Let $R = \mathbb{Z}_m[x]$ where $m = 2^{2024}$.

   (a) Suppose $f(x) = \overline{a_0} + \overline{a_1}x + \cdots + \overline{a_n}x^n$ is a unit in R. Show that a_0 is odd and all of $a_1, \ldots, a_n$ are even.

   Hint. Each polynomial in $\mathbb{Z}_m[x]$ "reduces" (how?) to a polynomial in $\mathbb{Z}_2[x]$. You understand the units in $\mathbb{Z}_2[x]$ already.

   (b) Suppose that a_0 is odd and all of $a_1, \ldots, a_n$ are even. Show that $f(x) = \overline{a_0} + \overline{a_1}x + \cdots + \overline{a_n}x^n$ is a unit in R.

[1] Recall that α being algebraic over F means that there is a nonzero $f(x) \in F[x]$ with $f(\alpha) = 0$.