Shashank Singh
sss1@andrew.cmu.edu

21-373 Honors Algebraic Structures, Fall 2011
Assignment 10
Due: Tuesday, December 6

Exercise 64: Let $n \in \mathbb{N}$ with $n \geq 1$, and let $P = -1 + (x-1)(x-2)\dots(x-n)$. Suppose, for sake of contradiction, that P is reducible in $\mathbb{Z}[x]$; in particular, suppose that $P = AB$, for some non-constant $A, B \in \mathbb{Z}[x]$. Let k_1 be the degree of A, and let k_2 be the degree of B. Then, $\forall i \in \mathbb{N}$ with $1 \leq i \leq n$, $AB(i) = P(i) = -1$. The only integers whose product is (-1) are 1 and (-1); thus, $\forall i \in \mathbb{N}$, either $A(i) = 1$ and $B(i) = -1$, or $A(i) = -1$ and $B(i) = 1$. In either case, $A(i) + B(i) = 0$, so that $(A + B)$ has at least n roots. Thus, either $(A+B)$ is of degree $m \geq n$, or $(A+B) = 0$. Since $k_1, k_2 \geq 1$ and $n = k_1 + k_2$, $k_1, k_2 < n$, so that, since $m = \max\{k_1, k_2\} < n$, the first case is impossible. Thus, $(A+B) = 0$, so that $A = -B$. Then, noting that $k_1 = k_2$, if a is the coefficient of x^{k_1} in A and b is the coefficient of x^{k_1} in B, $a = -b$, so that $ab < 0$ (as $a, b \neq 0$, by definition of degree). However, this is a contradiction, since ab is the coefficient of x^n in P, which is 1. Thus, P is irreducible in $\mathbb{Z}[n]$. ■

Exercise 65: Let $n \geq 2$, and let $P = 1 + x + \ldots + x^{n-1}$. Then, $P = \frac{x^n - 1}{x-1}$, so that the roots of P are precisely those n^{th} roots of unity which are not 1. Suppose p is composite. Then, by Lemma 34.12, since $P = \prod_{d|n}$, P is not irreducible.

Suppose, on the other hand, that n is prime. Then, as noted in Remark 34.13, $P = \Phi_n$, where Φ_n denotes the n^{th}. By Lemma 35.1, then, P is irreducible. ■

Exercise 66: i. Let $P_1 = x^4 - 2 = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x - i\sqrt[4]{2})(x + i\sqrt[4]{2})$.

Since 2 divides 2 but not 1, and 2^2 does not divide 2, by Eisenstein's Criterion, P is irreducible. Let $E = \mathbb{Q}(\sqrt[4]{2})$, and let $F = E(i\sqrt[4]{2})$. Since any field containing $\sqrt[4]{2}$ contains $-\sqrt[4]{2}$, and any field containing $i\sqrt[4]{2}$ contains $-i\sqrt[4]{2}$, F is a splitting field extension for P_1 over $\mathbb{Q}[x]$. Since P is irreducible and monic, P is the minimal polynomial for $\sqrt[4]{2}$ over $\mathbb{Q}$, so that $[E : \mathbb{Q}] = 4$. Since $i\sqrt[4]{2} \notin \mathbb{R}$ and $E \subseteq \mathbb{R}$, $i\sqrt[4]{2} \notin E$, so that $[F : E] \geq 2$. Furthermore, $x^2 + (\sqrt[4]{2})^2 \in E[x]$ is a degree 2 polynomial, so that $[F : E] \leq 2$, and thus $[F : E] = 2$. Therefore, $[F : \mathbb{Q}] = [F : E][E : \mathbb{Q}] = 8$. ■

ii. Let $P_2 = x^4 + 2 = (x - \sqrt[4]{-2})(x + \sqrt[4]{-2})(x - i\sqrt[4]{-2})(x + i\sqrt[4]{-2})$.

Let $F = \mathbb{Q}(\sqrt[4]{-2}, i\sqrt[4]{-2})$, and let $E = \mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2})$, so that F is a splitting field extension for P_2 over $\mathbb{Q}[x]$. Since any field containing $\mathbb{Q}$ contains $\sqrt[4]{-2}$ and $i\sqrt[4]{-2}$ if and only if it contains $\sqrt[4]{2}$ and $i\sqrt[4]{2}$, $F = E$, so that $[F : \mathbb{Q}] = [E : \mathbb{Q}]$. As shown in part i., $[E : \mathbb{Q}] = 8$, so that $[F : \mathbb{Q}] = 8$. ■

iii. Let ξ Let $P_3 = x^4 + x^2 + 1 = (x^2 + x + 1)(x^2 - x + 1) = (x - \sqrt[3]{-1})(x + \sqrt[3]{-2})(x - (-1)^{2/3})(x + (-1)^{2/3}$.

Let $F = \mathbb{Q}(\sqrt[3]{-1})$. Then, clearly, $-\sqrt[3]{-2} \in F$, and $(\sqrt[3]{-1})^2 = (-1)^{2/3} \in F$, so that $-(-1)^{2/3} \in F$. Thus, F is a splitting field extension of $\mathbb{Q}$. Furthermore, $\sqrt[3]{-1}$ is a root of the degree 2 polynomial $x^2 - x + 1 \in \mathbb{Q}[x]$, so that $[F : \mathbb{Q}] \leq 2$. Since $(-1)^{2/3} \in F$ and $(-1)^{2/3} \notin \mathbb{Q}$, $[F : \mathbb{Q}] \geq 2$, so that $[F : \mathbb{Q}] = 2$. ■

iv. Let $P_4 = (x^3 + 2)(x^3 - 2) = (x - \sqrt[3]{2})(x + \sqrt[3]{2})(x - \sqrt[3]{-2})(x + \sqrt[3]{-2})(x - (-1)^{2/3}\sqrt[3]{2})(x + (-1)^{2/3}\sqrt[3]{-2}$. Let $E = \mathbb{Q}(\sqrt[3]{2})$, and let $F = E((-1)^{2/3}\sqrt[3]{2})$, so that F is a splitting field extension for P_4 over $\mathbb{Q}$. Since $\sqrt[3]{2}$ is a root of the degree 3 polynomial $x^3 - 2 \in mathbbQ[x]$, $[E : \mathbb{Q}] = 3$. However, since $E \subseteq \mathbb{R}$, and $(-1)^{2/3}\sqrt[3]{2} \notin \mathbb{R}$, $(-1)^{2/3}\sqrt[3]{2} \notin E$, so that $[F : E] \geq 2$. However, $(-1)^{2/3}\sqrt[3]{2}$ is a root of the degree 2 polynomial $(x^2 + 2^{1/3}x + 2^{2/3}) \in E[x]$, so that $[F : E] \leq 2$, and thus $[F : E] = 2$. Therefore, $[F : \mathbb{Q}] = [F : E][E : \mathbb{Q}] = 6$. ■

Exercise 67: Let E be a field. Let $S = E \backslash \{0, 1, -1\}$. Suppose $x \in E$, with $x^2 = 1$. Then, $x^2 + x = x + 1$, so that $x(x+1) = x + 1$. Therefore, $x \in \{1, -1\}$. Thus, $\forall y \in S$, $y \neq n^{-1}$. As a consequence, $\prod_{y \in S} y = 1$, since each term in the product can be paired with its inverse in the product.

Thus, since $\prod_{x \in E} x = (1)(-1) \prod_{x \in S} x = -1$. ■

Exercise 68: Polynomials of degrees 2 and 3 in $\mathbb{Z}_3[x]$ are reducible if and only if they have roots in $\mathbb{Z}_3$. Thus, the monic reducible polynomials of degree 2 in $\mathbb{Z}_3[x]$ can be counted by counting the number of ways of choosing the roots. In the case that the roots are distinct, there are $\binom{3}{2} = 3$ polynomials; otherwise, there are $\binom{3}{1} = 3$ polynomials, so that, of the $3^2 = 9$ monic degree 2 polynomials in $\mathbb{Z}_3[x]$, 6 are reducible, and 3 are irreducible.

Reducible polynomials of degree 3 in $\mathbb{Z}_3$ either have 3 roots in $\mathbb{Z}_3$, or are the product of a linear and an irreducible quadratic polynomial in $\mathbb{Z}_3$. In the first case, the polynomials can be counted by counting their roots. There is 1 polynomial with 3 distinct roots, there are $3 * 2 = 6$ polynomials with 2 distinct roots, and there are $\binom{3}{1} = 3$ polynomials with 1 distinct root, so that there are 10 such monic reducible degree 3 polynomials. In the second case, since there are 3 irreducible degree 2 polynomials and 3 linear polynomials, there are $3 * 3 = 9$ such monic reducible degree 3 polynomials. Thus, of the $3^3 = 27$ monic degree 3 polynomials in $\mathbb{Z}_3[x]$, 19 are reducible and 8 are irreducible.

A degree 4 polynomial in $\mathbb{Z}_3[x]$ is reducible if and only if it is a product of two irreducible degree 2 polynomials, or it has exactly 1, 2, or 4 roots in $\mathbb{Z}_3$. There are $3^2 = 9$ degree 4 polynomials which are products of two irreducible degree 2 polynomials. If a degree 4 polynomial in $\mathbb{Z}_3[x]$ has exactly one root in $\mathbb{Z}_3$, it is the product of one linear and one irreducible degree 3 polynomial. Thus, there are $3 * 8 = 24$ degree 4 polynomials with exactly one root in $\mathbb{Z}_3$. If a degree 4 polynomial in $\mathbb{Z}_3[x]$ has exactly two roots in $\mathbb{Z}_3$, it is the product of two linear and one irreducible degree 2 polynomial. Thus, there are $3 * \binom{3}{2} = 9$ degree 4 polynomials with exactly 1 root in $\mathbb{Z}_3$. Lastly, there are 21 degree 4 polynomials in $\mathbb{Z}_3[x]$ with 4 roots in $\mathbb{Z}_3$ (0 with 4 distinct roots, $3 * 3 = 9$ with 3 distinct roots, 3 with 2 distinct roots of the same multiplicity, 6 with 2 distinct roots of different multiplicity, and 3 with one distinct root).

Thus, there are $81 - (9 + 24 + 9 + 21) = 18$ irreducible monic polynomials of degree 4 in $\mathbb{Z}_3$. ■