Paul Gustafson
Texas A&M University - Math 416
Instructor: Dr. Papanikolas

HW 2

27.18 Is $\mathbb{Q}[x]/(x^2 - 5x + 6)$ a field? Why?

Proof. No, $x - 2$ and $x - 3$ are zero divisors. $\square$

27.19 Is $K := \mathbb{Q}[x]/(x^2 - 6x + 6)$ a field? Why?

Proof. Yes, $x^2 - 6x + 6$ is irreducible over $\mathbb{Q}$ by Eisenstein's criterion ($p = 2$). Hence, $\langle p(x) \rangle$ is maximal by Theorem 27.25. Hence, K is a field. $\square$

27.30 Prove that if F is a field, every proper nontrivial prime ideal of $F[x]$ is maximal.

Proof. Let $N \subset F[x]$ be a proper nontrivial prime ideal of $F[x]$. By Theorem 27.24, N is principal; let $p(x)$ be a generator of N.

To see that $p(x)$ is irreducible, suppose $p(x) = q(x)r(x)$ for q, r of degree less than p. Then since $N = \langle p(x) \rangle$ is a prime ideal, either q or r is a multiple of p. This contradicts the assumption that both q and r have degree less than p. Hence, $p(x)$ is irreducible. Hence, since $N \neq 0$, Theorem 27.25 implies N is maximal. $\square$

27.33 Use the fact that, for any field F, $F[x]$ is a PID to show TFAE:

1. Every nonconstant polynomial in $\mathbb{C}[x]$ has a zero in $\mathbb{C}$.
2. Let $f_1(x), \ldots, f_r(x) \in \mathbb{C}[x]$ and suppose that every $\alpha \in \mathbb{C}$ that is a zero of all r of these polynomials is also a zero of a polynomial $g(x)$ in $\mathbb{C}[x]$. Then some power of $g(x)$ is in the smallest ideal of $\mathbb{C}[x]$ that contains the r polynomials $f_1(x), \ldots, f_r(x)$.

Proof. Suppose 1 holds. Let $N \subset \mathbb{C}[x]$ be the ideal generated by $\{f_i\}_{i=1}^r$. Let $p(x)$ generate N. If p is constant, then $N = \mathbb{C}[x]$, so the conclusion holds. Otherwise, by 1, p has a root $\beta \in \mathbb{C}$. Since p generates N, β is a root of every element of N. In particular, β is a root of every f_i. Conversely, suppose α is a root of f_i for all i. Then since the f_i generate N, α must be a root of p. Thus, the roots of p are precisely the simultaneous roots of the f_i.

By repeated application of 1 and the division algorithm, $p(x) = \prod_{i=1}^n (x - \alpha_i)^{e_i}$ where the α_i are distince. Let $e = \max_i e_i$. By repeated application of the division algorithm, $\prod_{i=1}^n (x - \alpha_i) \mid g(x)$. Hence, $p(x) \mid \prod_{i=1}^n (x - \alpha_i)^e \mid (g(x))^n$.

For the converse, suppose 2 holds. Suppose $f \in \mathbb{C}[x]$ has no zeros in $\mathbb{C}$. Then, by 2, if $g(x) = 1$, some power of g is in $N := \langle f \rangle$, i.e. $1 \in N$. But then $f(x) \mid 1$, so $\deg(f) = 0$. $\square$

29.30 Let E be an extension field of a finite field F, where F has q elements. Let $\alpha \in E$ be algebraic over F of degree n. Prove that $F(\alpha)$ has q^n elements.

Proof. This follows immediately from Theorem 29.18, which says that $F(\alpha)$ is an n dimensional vector space over F. Each coordinate has q choices, so there are q^n total elements in $F(\alpha)$. $\square$

29.31

1. Show that there exists an irreducible polynomial of degree 3 in $\mathbb{Z}_3[x]$.
2. Show from part (1) that there exists a finite field of 27 elements. (Hint: use 30)

Proof. Let $p(x) = x^3 - x + 1$. Since p has no roots in $\mathbb{Z}_3$, it cannot have linear factors, so must be irreducible. Part 2 follows directly from 30. $\square$

29.34 Show that $S := \{a + b(\sqrt[3]{2}) + c(\sqrt[3]{2})^2 | a, b, c \in \mathbb{Q}\}$ is a subfield of $\mathbb{R}$ by using Theorem 29.18.

Proof. By Eisenstein's criterion with $p = 2$, $x^3 - 2$ is irreducible over $\mathbb{Q}$. Hence, since $\sqrt[3]{2}$ is of degree 3 over $\mathbb{Q}$, Theorem 29.18 states that the elements of $Q[\sqrt[3]{2}]$ are precisely the elements of S. $\square$