MATH 320 Unit 4 Exercises

Factorization in $R[x]$

Let R be a commutative ring with identity, and let $a, b \in R$. We say that a is an *associate* of b if there is some unit $u \in R$ with $a = ub$. If $a \in R$ is not a unit and not 0_R, we call a *irreducible* if all of its divisors are units and associates (otherwise we call a *reducible*). We call nonzero nonunit $a \in R$ *prime* if it satisfies $\forall b, c \in R$, if $a|bc$ then $\big(a|b$ or $a|c\big)$.

$\mathbb{F}[x]$ cancellative property: Let $f, g, h \in \mathbb{F}[x]$, where $\mathbb{F}$ is a field and $f \neq 0$. If $fg = fh$ then $g = h$.

Unique Factorization Theorem: Let $R \in \{\mathbb{Z}, \mathbb{F}[x]\}$, and let $n \in R$ where $n \neq 0_R$ and n is not a unit in R. Then n has a factorization into primes, which is unique up to order and up to associates.

Let R be a commutative ring, and $f(x) \in R[x]$. Then $f(x) = a_n x^n + \cdots + a_1 x + a_0$ *induces* a function $f : R \to R$ via $f(r) = a_n r^n + \cdots + a_1 r + a_0$. We call $a \in R$ a *root* of $f(x)$ if $f(a) = 0_R$, that is if the induced function maps a to 0_R.

Remainder Theorem: Let $\mathbb{F}$ be a field, $f(x) \in \mathbb{F}[x]$, and $a \in \mathbb{F}$. The remainder when $f(x)$ is divided by the polynomial $x - a$ is the constant polynomial $f(a)$. That is, $(f(x), x-a) \to DA \to (q(x), f(a))$.

Factor Theorem: Let $\mathbb{F}$ be a field, $f(x) \in \mathbb{F}[x]$, and $a \in F$. Then a is a root of $f(x)$ if and only if $x - a$ is a factor of $f(x)$, in $\mathbb{F}[x]$. (u is a factor of v means $u|v$)

Max Root Theorem: Let $\mathbb{F}$ be a field, $f(x) \in \mathbb{F}[x]$ with[a] $deg(f(x)) = n$. Then $f(x)$ has at most n roots in $\mathbb{F}$.

[a] In particular, $f(x) \neq 0_{\mathbb{F}}$, since its degree exists.

For Oct. 23:

1. Let p be a positive prime integer, and let $f(x) \in \mathbb{Z}_p[x]$ be nonzero. Prove that $f(x)$ has exactly $p - 1$ associates.
2. Prove that $x^2 + 1$ is irreducible in $\mathbb{Q}[x]$, and reducible in $\mathbb{C}[x]$.
3. Find at least three different finite fields $\mathbb{F}$, such that $x^2 + 1$ is reducible in $\mathbb{F}[x]$.
4. Find all monic irreducible polynomials of degree at most 2, in $\mathbb{Z}_3[x]$.
   HINT: There are only so many possibilities, just test them all.

For Oct. 28:

5. Prove that $x^3 - [3]$ is irreducible in $\mathbb{Z}_7[x]$.
6. Express $x^4 - 4$ as a product of irreducibles in $\mathbb{Q}[x]$, in $\mathbb{R}[x]$, and in $\mathbb{C}[x]$.
7. Let $f(x) = x^3 + x^2 + [1]$ and $g(x) = x^4 + x + [1]$, polynomials in $\mathbb{Z}_3[x]$. Prove that, although they are clearly not equal polynomials, they induce the same function.
8. Find a polynomial of degree 5 in $\mathbb{Z}_2[x]$ that induces the zero function on $\mathbb{Z}_2$.

For Oct. 30:

9. Let $\mathbb{F}$ be a field, and let $f(x) \in \mathbb{F}[x]$ be a polynomial of degree 2 or 3. Prove that $f(x)$ is irreducible in $\mathbb{F}[x]$ if and only if $f(x)$ has no roots in $\mathbb{F}$.

10. Prove the Remainder Theorem.

11. Prove the Factor Theorem.

12. Prove the Max Root Theorem. HINT: Induction.

Extra:

13. Let $\mathbb{F}$ be a field, and let $f(x) \in \mathbb{F}[x]$ be prime. Without using the Unique Factorization Theorem, prove that if $f(x)|a_1(x)a_2(x)\cdots a_n(x)$, then there is at least one $i \in \{1, 2, \ldots, n\}$ with $f(x)|a_i(x)$.

14. Factor $x^4 - [4]$ as a product of irreducibles in $\mathbb{Z}_5[x]$.

15. Let $\mathbb{F}$ be a field, and let $p(x), q(x) \in \mathbb{F}[x]$. Suppose that $p(x), q(x)$ are each irreducible, and that they are not associates. Prove that $\gcd(p(x), q(x)) = 1_{\mathbb{F}}$.

16. Let $\mathbb{F}$ be a field, and let $c \in \mathbb{F}$ be nonzero. Suppose that c is a root of $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{F}[x]$. Prove that c^{-1} is a root of $a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n$.

17. Let $\mathbb{F}$ be a field. Prove existence of the Unique Factorization theorem for $\mathbb{F}[x]$. That is prove that for every nonzero nonunit $n(x) \in \mathbb{F}[x]$, there are primes $p_1(x), p_2(x), \ldots, p_k(x) \in \mathbb{F}[x]$ with $n(x) = p_1(x)p_2(x)\cdots p_k(x)$.

18. Let $\mathbb{F}$ be a field. Prove uniqueness of the Unique Factorization theorem for $\mathbb{F}[x]$. That is prove that for every nonzero nonunit $n(x) \in \mathbb{F}[x]$, if there are primes $p_1(x), p_2(x), \ldots, p_k(x)$, $q_1(x), q_2(x), \ldots, q_j(x) \in \mathbb{F}[x]$ with $n(x) = p_1(x)p_2(x)\cdots p_k(x) = q_1(x)q_2(x)\cdots q_j(x)$, then $j = k$ and we can reorder the $q_i(x)$'s so that $p_1(x)$ is an associate of $q_1(x)$, $p_2(x)$ is an associate of $q_2(x)$, and so on, until $p_k(x)$ is an associate of $q_k(x)$.