Previously.

- Polynomial Rings
- The Division Algorithm
- The Factor Theorem
- The Remainder Theorem

This Section.

- Factoring degree 2 and 3 polynomials
- Unique Factorization
- Factoring in $\mathbb{C}[x]$, $\mathbb{R}[x]$, $\mathbb{Q}[x]$, $\mathbb{Z}[x]$

Definition. Let F be a field and $p \neq 0$ in $F[x]$ a polynomial. We call p `irreducible over F` if $\deg(p) \geq 1$ and

$$\text{if } p = fg \text{ for } f, g \in F[x], \text{ then either} \deg(f) = 0 \text{ or } \deg(g) = 0.$$

Otherwise we call p `reducible`.

Theorem 4.2.1. Let F be a field and consider p in $F[x]$ where $\deg(p) \geq 2$.

1. If p is irreducible, then p has no root in F.

2. If $\deg(p)$ is 2 or 3, then p is irreducible if and only if it has no root in F.

Example. (a) $x^2 + 1$ is irreducible in $\mathbb{R}[x]$

(b) $x^2 - 2$ is irreducible over $\mathbb{Q}$

(c) $p = x^3 + 3x^2 + x + 2$ is irreducible over $\mathbb{Z}_5$

Unique Factorization Theorem (4.2.12). Let F be a field, and f be a nonconstant polynomial in $F[x]$. Then

1. $f = ap_1p_2\cdots p_m$, where $a \in F$ and $p_1, p_2, \ldots, p_m$ are monic and irreducible in $F[x]$.

2. The factorization is unique up to the order of the factors.

Note. The proof for (1) is a pretty straight-forward induction proof.
The proof for (2) uses the fact that if

$$p|q_1q_2\cdots q_n,$$

where $p, q_1, q_2, \ldots, q_n$ are irreducible, then $p|q_i$ for some i.

Remark. If F is a field, we call $F[x]$ a `unique factorization domain` because it is a domain and the elements factor uniquely.

Factorization over $\mathbb{C}$

Fundamental Theorem of Algebra (Theorem 4.2.2). If $f \in \mathbb{C}[x]$ with $\deg f > 0$, then f has at least one root in $\mathbb{C}$.

Theorem 4.2.3. **1.** If $\deg f = n \geq 1$, $f \in \mathbb{C}[x]$, then f factors completely as

$$f = u(x - a_1)(x - a_2)\cdots(x - a_n),$$

for $u \neq 0$, $a_1, a_2, \ldots, a_n \in \mathbb{C}$.

2. The only irreducible polynomials in $\mathbb{C}[x]$ are linear.

Exercise 1. Complex conjugation is a ring homomorphism. So let's assume that $z = a + bi$ is a root of a polynomial $f \in \mathbb{R}[x]$.
Prove that $\bar{z} = a - bi$ is also a root of f.

Factorization over $\mathbb{R}$

Theorem 4.2.4. Every nonconstant polynomial $f \in \mathbb{R}[x]$ factors as

$$f = u(x - r_1)(x - r_2) \cdots (x - r_m) q_1 q_2 \cdots q_k,$$

where $r_1, r_2, \ldots, r_m$ are the real roots of f and $q_1, q_2, \ldots, q_k$ are monic irreducible quadratics in $\mathbb{R}[x]$.

Corollary. The irreducible polynomials in $\mathbb{R}[x]$ are either linear or quadratic.

Factoring over $\mathbb{Q}$

Gauss' Lemma (Theorem 4.2.5). Let $f = gh$ in $\mathbb{Z}[x]$. If a prime $p \in \mathbb{Z}$ divides every coefficient of f, then p divides every coefficient of g or p divides every coefficient of h.

Theorem 4.2.6. Let $f \in \mathbb{Z}[x]$ be a non-constant polynomial.

1. If $f = gh$ with $g, h \in \mathbb{Q}[x]$, then $f = g_0 h_0$ where $g_0, h_0 \in \mathbb{Z}[x]$, $\deg g = \deg g_0$, and $\deg h = \deg h_0$.
2. f is irreducible in $\mathbb{Q}[x]$ if and only if $f = ag$ where $a \in \mathbb{Z}$ are the only factorizations of f in $\mathbb{Z}[x]$.

Exercise 2. Consider

$$4x^8 + 2x^7 - 4x^6 - 5x^5 - 6x^4 - 7x^3 - 3x^2 - x - 1 = \left(\frac{20}{3}x^3 + \frac{10}{3}x^2 + \frac{5}{3}\right)\left(\frac{3}{5}x^5 - \frac{3}{5}x^3 - \frac{3}{5}x^2 - \frac{3}{5}x - \frac{3}{5}\right).$$

Write this polynomial as a product of polynomials in $\mathbb{Z}[x]$.

Reduction mod p. Using the mod p map, $\mathbb{Z} \to \mathbb{Z}_p$, we induce a map from $\mathbb{Z}[x]$ to $\mathbb{Z}_p[x]$ given by

$$f = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \mapsto \bar{f} = \bar{a}_0 + \bar{a}_1x + \bar{a}_2x^2 + \cdots + \bar{a}_nx^n.$$

We call $\bar{f}$ the reduction of f modulo p. This map is in fact an onto ring homomorphism.

Modular Irreducibility (Theorem 4.2.7). Let $0 \neq f \in \mathbb{Z}[x]$ and suppose that a prime p exists such that

1. p does not divide the leading coefficient of f.

2. The reduction, $\bar{f}$ of f modulo p is irreducible in $\mathbb{Z}_p[x]$.

Then f is irreducible over $\mathbb{Q}$.

Exercise 3. Show that $f = 32x^3 - 51x^2 - 2x + 25$ is irreducible over $\mathbb{Q}$.
(Hint: Check mod 3.)

Eisenstein's Criterion (Theorem 4.2.8). Consider $f = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ in $\mathbb{Z}[x]$, where $n \geq 1$ and $a_0 \neq 0$. Let $p \in \mathbb{Z}$ be a prime number satisfying

1. p divides each of $a_0, a_1, a_2, \ldots, a_{n-1}$.

2. p does not divide a_n.

3. p^2 does not divide a_0.

Then f is irreducible in $\mathbb{Q}[x]$.

Exercise 4. Show that $x^5 - 3x^2 + 6x - 12$ is irreducible in $\mathbb{Q}[x]$.

Exercise 5. Show that $f = x^n - 2$ is irreducible in $\mathbb{Q}[x]$ for all n.

So What's the Point?. If $f \in \mathbb{Q}[x]$ and we want to find the roots, we can think of $f_1 \in \mathbb{Z}[x]$.

Polynomials in $\mathbb{Z}[x]$ are "easier" than those in $\mathbb{Q}[x]$.

Polynomials in $\mathbb{Z}_p[x]$ are way easier than those in $\mathbb{Q}[x]$!!