Theorem 24.1

If R is a PID then it is a UFD.

Lemma 24.2

If R is a PID and $I_1, I_2, \ldots$ are ideals of R such that

$$I_1 \subseteq I_2 \subseteq \ldots$$

then there exists $n \geq 1$ such that $I_n = I_{n+1} = \ldots$.

Lemma 24.3

Let R be a PID. An element $a \in R$ is irreducible if and only if $\langle a \rangle$ is a maximal ideal of R.

Proof of Theorem 24.1.

Corollary 24.4

If F is a field then the ring of polynomials $F[x]$ is a UFD.

Theorem 24.5 Fundamental Theorem of Algebra

If $p(x) \in \mathbb{C}[x]$ is a polynomial such that $\deg p(x) > 0$ then there is $a \in \mathbb{C}$ such $p(a) = 0$.

Corollary 24.6

A polynomial $p(x) \in \mathbb{C}[x]$ is irreducible if and only of $\deg p(x) = 1$.

Corollary 24.7

If $p(x) \in \mathbb{C}[x]$ is a polynomial and $\deg p(x) = n \geq 1$ then

$$p(x) = a_0(x - a_1)(x - a_2) \cdot \ldots \cdot (x - a_n)$$

for some $a_0, a_1, \ldots, a_n \in C$. Moreover, this decomposition is unique up to permutation of factors.

Definition 24.8

If $z = a + bi$ is a complex number then the *complex conjugate* of z is the complex number $\overline{z} = a - bi$.

Theorem 24.9

If $z_1 = a + bi$, $z_2 = c + di$ are a complex numbers then
1) $\overline{(z_1 + z_2)} = \overline{z}_1 + \overline{z}_2$
2) $\overline{(z_1 \cdot z_2)} = \overline{z}_1 \cdot \overline{z}_2$

Proof. Exercise. □

Corollary 24.10

Let $p(x) \in \mathbb{R}[x]$. If z is a complex number such that $p(z) = 0$, then $p(\overline{z}) = 0$.

Theorem 24.11

A polynomial $p(x) \in \mathbb{R}[x]$ is irreducible in $\mathbb{R}[x]$ if and only if either $\deg p(x) = 1$ or $\deg p(x) = 2$ and $p(x)$ has no roots in $\mathbb{R}$.

Corollary 24.12

If $p(x) \in \mathbb{R}[x]$ is a polynomial and $\deg p(x) \geq 1$ then

$$p(x) = a \cdot q_1(x) \cdot q_2(x) \cdot \ldots \cdot q_m(x)$$

where $a \in \mathbb{R}$ and for each $i = 1, \ldots, m$ either $q_i(x) = x - a_i$ for some $a_i \in \mathbb{R}$ or $q_i(x) = x^2 + b_i x + c_i$ for some $b_i, c_i \in \mathbb{R}$ such that $b_i^2 - 4c_i < 0$. Moreover, this decomposition is unique up to permutation of factors.

Definition 24.13

Let $p(x) = a_0 + a_1 x + \ldots + a_n x^n$ be a polynomial in $\mathbb{Z}[x]$. The *content* of $p(x)$ is the number

$$c(p) = \gcd(a_0, a_1, \ldots, a_n)$$

If $c(p) = 1$ then we say that $p(x)$ is a *primitive polynomial*.

Lemma 24.14

If $q_1(x), q_2(x) \in \mathbb{Z}[x]$ are primitive polynomials then $q_1(x) \cdot q_2(x)$ is primitive.

Theorem 24.15

Let $p(x) \in \mathbb{Z}[x]$. If $p(x)$ is irreducible in $\mathbb{Z}[x]$ then it is irreducible in $\mathbb{Q}[x]$.

Theorem 24.16 Eisenstein Irreducibility Criterion

Let $q(x) = a_0 + a_1 x + \ldots + a_n x^n$ be a polynomial in $\mathbb{Z}[x]$. Assume that there a prime number p such that p divides a_i for $i < n$, p does not divide a_n, and p^2 does not divide a_0. Then $q(x)$ is irreducible in $\mathbb{Q}[x]$.