Recall: A principal ideal domain (PID) is a ring R which is an integral domain, such that every ideal $I \triangleleft R$ is principal, i.e. $I = \langle a \rangle$ for some $a \in R$.

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 $I_n = I_{n+1} = \ldots$.

Proof. Take $J = \bigcup_{i=1}^{\infty} I_i$. One can check that J is an ideal of R. Since R is a PID we have $J = \langle a \rangle$ for some $a \in J$. Take $n \geq 1$ such that $a \in I_n$. Then we get

$$J \subseteq I_n \subseteq I_{n+1} \subseteq \ \ldots \ \subseteq J$$

It follows that $I_n = I_{n+1} = \ \ldots \ = J$. □

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. Exercise. □

Proof of Theorem 24.1. Let R be a PID. By Theorem 23.5 it suffices to show that

1) Every non-zero, non-unit element of R is a product of irreducible elements.

2) Every irreducible element in R is a prime element.

1) We argue by contradiction. Assume that $a_0 \in R$ is a non-zero, non-unit element that is not a product of irreducibles. This implies that $a_0 = a_1 b_1$ for some non-zero, non-unit elements $a_1, b_1 \in R$.

If both a_1 and b_1 were products of irreducibles, then a_0 would be also a product of irreducibles, contradicting our assumption. We can then assume that a_1 is not a product of irreducibles, and so in particular we have $a_1 = a_2 b_2$ for some non-zero, non-unit elements $a_2, b_2 \in R$.

By induction we obtain that for $i = 1, 2, \dots$ there exists non-zero, non-unit elements $a_i, b_i \in R$ such that $a_i = a_{i+1} b_{i+1}$ for all $i \geq 0$.

Consider the chain of ideals

$$\langle a_0 \rangle \subseteq \langle a_1 \rangle \subseteq \dots$$

By Lemma Lemma 24.3 we obtain that $\langle a_n \rangle = \langle a_{n+1} \rangle$ for some $n \geq 0$. This means that $a_n = a_{n+1} u$ for some unit $u \in R$ (check!). As a consequence $a_{n+1} b_{n+1} = a_n = a_{n+1} u$ and so $b_{n+1} = u$. This is a contradiction, since b_{n+1} is not a unit.

2) Let $a \in R$ be an irreducible element and let $a \mid (bc)$. We need to show that either $a \mid b$ or $a \mid c$.

Assume that $a \nmid b$. This implies that $b \notin \langle a \rangle$ and so $\langle a \rangle \neq \langle a \rangle + \langle b \rangle$

Since by Lemma 24.3 the ideal $\langle a \rangle$ is a maximal ideal, we obtain then that $\langle a \rangle + \langle b \rangle = R$, and so in particular $1 \in \langle a \rangle + \langle b \rangle$. Therefore $1 = ar + bs$ for some $r, s \in R$, and so $c = a(rc) + (bc)s$ Since $a \mid a(rc)$ and $a \mid (bc)s$ we obtain from here that $a \mid c$. □

Corollary 24.4

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

Proof. Follows from Theorem 24.1 and Theorem 21.13 □

Corollary 24.4 Applies in particular to the rings $\mathbb{C}[x]$, $\mathbb{R}[x]$, and $\mathbb{Q}[x]$. Next, we will look at the irreducible elements in this rings.

In the ring $\mathbb{C}[x]$ irreducible polynomials can be characterized using the following theorem, the proof of which is omitted:

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 $\deg p(x) = 1$.

Proof. If $\deg p(x) = 0$ i.e. $p(x) = a_0$ for some $a_0 \neq 0$, then $p(x)$ is a unit in $\mathbb{C}[x]$.

If $\deg p(x) = 1$ and $p(x) = q_1(x)q_2(x)$ for some $q_1(x), q_2(x) \in \mathbb{C}[x]$ then either $\deg q_1(x) = 0$ or $\deg q_2(x) = 0$. It means that either $q_1(x)$ or $q_2(x)$ is unit. This shows that $p(x)$ is irreducible.

If $p(x) > 1$ then by Theorem 24.5 there is $a \in \mathbb{C}$ such that $p(a) = 0$. By Theorem 21.8 we obtain that $p(a) = (x - a)q(x)$ where $\deg q(x) \geq 1$, and so $p(x)$ is not irreducible. □

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.

Proof. This follows from Corollary 24.4 and Corollary 24.6 □

Next, we will look at irreducible polynomials in $\mathbb{R}[x]$.

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 $p(\overline{z}) = 0$.

Proof. Let $p(x) = a_0 + a_1 x + \cdots + a_n x^n$. Notice, that since $a_i \in \mathbb{R}$, thus $\overline{a}_i = a_i$. We have:

$$\begin{aligned}
p(\overline{z}) &= a_0 + a_1\overline{z} + a_2\overline{z}^2 + \ldots + a_n\overline{z}^n \\
&= \overline{a}_0 + \overline{a}_1\overline{z} + \overline{a}_2\overline{z}^2 + \ldots + \overline{a}_n\overline{z}^n \\
&= \overline{a}_0 + \overline{a_1 z} + \overline{a_2 z^2} + \ldots + \overline{a_n z^n} \\
&= \overline{a_0 + a_1 z + a_2 z^2 + \ldots + a_n z^n} \\
&= \overline{p(z)}
\end{aligned}$$

Since $p(z) = 0$ and $\overline{0} = 0$, we obtain $p(\overline{z}) = 0$. □

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 $\mathbb{R}$.

Note. Recall that if $p(x) = a_0 + a_1 x + a_2 x^2$ is a polynomial in $\mathbb{R}[x]$, then $p(x)$ has no roots in $\mathbb{R}$ if and only if $a_1^2 - 4a_2 a_0 < 0$.

Proof of Theorem 24.11. Let $p(x) \in \mathbb{R}[x]$ and $p(x) \neq 0$.

If $\deg p(x) = 0$, then $p(x)$ is a unit in $\mathbb{R}[x]$.

If $\deg p(x) = 1$ and $p(x) = q_1(x)q_2(x)$ for some $q_1(x), q_2(x) \in \mathbb{R}[x]$ then either $\deg q_1(x) = 0$ or $\deg q_2(x) = 0$, so either $q_1(x)$ or $q_2(x)$ is unit. This means that $p(x)$ is irreducible.

If $\deg p(x) = 2$ then $p(x)$ is reducible if and only if $p(x) = q_1(x)q_2(x)$ for some $q_1(x), q_2(x) \in \mathbb{R}[x]$ such that $\deg q_1(x) = \deg q_2(x) = 1$. If $q_1(x) = a_0 + a_1x$ then for $b = -\frac{a_0}{a_1}$ we have $q_1(b) = 0$, and so $p(b) = q_1(b)q_2(b) = 0$. This means that $p(x)$ is reducible if and only if it has a root in $\mathbb{R}$.

Finally, assume that $\deg p(x) \geq 2$. By Theorem 24.5 there is $z \in \mathbb{C}$ such that $p(z) = 0$. If $z \in \mathbb{R}$ then $p(x) = (x - z)q(x)$ where $\deg q(x) \geq 1$ and $(x - z)$ and $q(x)$ are polynomials in $\mathbb{R}[x]$. This means that $p(x)$ is reducible. If $z \notin \mathbb{R}$ then $\overline{z} \neq z$, and by Corollary 24.10 we have $p(\overline{z}) = 0$. This gives

$$p(x) = (x - z)(x - \overline{z})q(x)$$

for some $q(x) \in \mathbb{C}[x]$, $\deg q(x) \geq 1$. Denote $h(x) = (x - z)(x - \overline{z})$. Notice that if $z = a + bi$ then

$$h(x) = x^2 - 2ax + (a^2 + b^2)$$

so $h(x) \in \mathbb{R}[x]$. This implies that also $q(x) \in \mathbb{R}[x]$, since otherwise some coefficient of $p(x) = h(x)q(x)$ would not be a real number (exercise). Thus we obtain that $p(x)$ is a product of two polynomials in $\mathbb{R}[x]$ of degree greater than 0, so $p(x)$ is reducible. □

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 $q_i(x) = x^2 + b_ix + c_i$ 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.

Proof. This follows from Corollary 24.4 and Theorem 24.11 □

Finally, we will have a look at irreducible polynomials in $\mathbb{Q}[x]$. This will require looking at polynomials in $\mathbb{Z}[x]$.

Definition 24.13

Let $p(x) = a_0 + a_1x + \ldots + a_nx^n$ 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.*

Note. Notice that any non-zero polynomial $p(x) \in \mathbb{Z}[x]$ can be uniquely written as $p(x) = c(p) \cdot q(x)$ where $q(x)$ 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.

Proof. We argue by contradiction. Assume that $q_1(x)$ and $q_2(x)$ are primitive, but $f(x) = q_1(x) \cdot q_2(x)$ is not. Then there is a prime number p such that every coefficient of $f(x)$ is divisible by p. On the other hand, there are some coefficients of $q_1(x)$ and $q_2(x)$ that are not divisible by p. Consider the function

$$\Phi\colon \mathbb{Z}[x] \to \mathbb{Z}_p[x]$$

given by $\Phi(a_0 + a_1x + \ldots + a_nx^n) = \overline{a}_0 + \overline{a}_1x + \ldots + \overline{a}_nx^n$ where $\overline{a}_i = a_i \mod p$. This function if a ring homomorphism, so $\Phi(f(x)) = \Phi(q_1(x)) \cdot \Phi(q_2(x))$. However, $\Phi(f(x)) = 0$ while $\Phi(q_1(x)) \neq 0$ and $\Phi(q_2(x)) \neq 0$. This means that $\Phi(q_1(x)), \Phi(q_2(x))$ are zero divisors in $\mathbb{Z}_p[x]$. This is impossible, since $\mathbb{Z}_p[x]$ is an integral domain. □

Theorem 24.15

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

Proof. We argue by contradiction. Assume that $p(x) \in \mathbb{Z}[x]$ it irreducible in $\mathbb{Z}[x]$ but reducible in $\mathbb{Q}[x]$. Then $p(x) = q_1(x) \cdot q_2(x)$ for some $q_i(x) \in \mathbb{Q}[x]$ such that $\deg q_i(x) > 0$ for $i = 1, 2$. Let a_1, a_2 be non-zero integers such that $a_1q_1(x), a_2q_2(x) \in \mathbb{Z}[x]$. Let c_i be the content of $a_iq_i(x)$. Then $a_iq_i(x) = c_iq_i'(x)$ where $q_i'(x) \in \mathbb{Z}[x]$ is a primitive polynomial. We obtain:

$$\begin{aligned} a_1a_2 \cdot p(x) &= a_1q_1(x) \cdot a_2q_2(x) \\ &= c_1c_2 \cdot q_1'(x) \cdot q_2'(x) \end{aligned}$$

Since $p(x)$ is irreducible in $\mathbb{Z}[x]$, it is primitive and so the content of $a_1a_2 \cdot p(x)$ is a_1a_2. Also, by Lemma 24.14 $q_1'(x) \cdot q_2'(x)$ is primitive, so the content of $c_1c_2 \cdot q_1'(x) \cdot q_2'(x)$ is c_1c_2. This shows that $a_1a_2 = c_1c_2$, and so we obtain

$$p(x) = q_1'(x) \cdot q_2'(x)$$

for $q_i'(x) \in \mathbb{Z}[x]$, $\deg q_i'(x) > 1$. This contradicts the assumption that $p(x)$ is irreducible in $\mathbb{Z}[x]$. $\square$

Theorem 24.16 Eisenstein Irreducibility Criterion

Let $q(x) = a_0 + a_1x + \ldots + a_nx^n$ 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 $\mathbb{Q}[x]$.

Proof. Assume first that $q(x)$ is a primitive polynomial. If $q(x)$ is reducible, then by Theorem 24.15 we have $q(x) = q_1(x) \cdot q_2(x)$, where $q_i(x) \in \mathbb{Z}[x]$ and $\deg q_i(x) \geq 1$. Let $q_1 = b_0 + b_1x + \ldots + b_rx^r$ and $q_1 = c_0 + c_1x + \ldots + c_sx^s$. Since $a_0 = b_0c_0$ is divisible by p but not by p^2, thus p divides either b_0 or c_0, but not both. We can assume that p divides b_0. Also, since p does not divide $a_n = b_rc_s$, that means that p does not divide b_r. Let t be the smallest index such that p does not divide b_t. Notice that $t \leq r \leq n$. We have: $a_t = b_tc_0 + b_{t-1}c_1 + \ldots + b_0c_t$ Since p divides a_t and it divides b_i for $i < t$, thus it must divide b_tc_0, which is impossible.

If $q(x)$ is not primitive, then $q(x) = c(q) \cdot q'(x)$ where $c(q) \in \mathbb{Z}$ is the content of $q(x)$ and $q'(x) \in \mathbb{Z}[x]$ is primitive. Since $c(q)$ is a unit in $\mathbb{Q}$ and $q'(x)$ is irreducible in $\mathbb{Q}[x]$ by the above argument, thus $q(x)$ is irreducible in $\mathbb{Q}[x]$. $\square$

Note. Theorem 24.16 indicates that factorization of polynomials into irreductibles is much more difficult in $\mathbb{Q}[x]$ than in $\mathbb{C}[x]$ or $\mathbb{R}[x]$. While in $\mathbb{C}[x]$ irreducible polynomials are of degree 1, and in $\mathbb{R}[x]$ they can be of degree 1 and 2, in $\mathbb{Q}[x]$ there are irreducible polynomials of any degree.

Note. Theorem 24.16 does not identify all irreducible polynomials in $\mathbb{Q}[x]$. For example, one can check that if p is a prime number then the polynomial

$$q(x) = x^{p-1} + x^{p-2} + \ldots + x + 1$$

is irreducible in $\mathbb{Q}[x]$, even though it does not satisfy the assumptions of Theorem 24.16.