1. Terminology English/German

Unique factorisation domain - faktorieller Ring
Field - Körper
Field of fractions - Quotientenkörper
Principal ideal domain - Hauptidealbereich
Field extension - Körpererweiterung
Prime subfield of a field - Primkörper eines Körpers

2. UFD's and irreducible polynomials over integral domains

From the last lecture we have the following lemma and corollary:

Lemma 2.1 (Gauss' lemma). *Let R be a unique factorisation domain (in German: faktorieller Ring) with field of fractions F and $p(x) \in R[x]$. If $p(x) = A(x)B(x)$ for some non-constant polynomials $A(x), B(x) \in F[x]$ then there exist $r, s \in F$ such that $rA(x) = a(x)$ and $sB(x) = b(x)$ are both are in $R[x]$ and $p(x) = a(x)b(x)$.*

Corollary 2.2. *Let R be a unique factorisation domain with field of fractions F (in German: Quotientenkörper) and let $p(x) \in R[x]$. Suppose that the greatest common divisor of the coefficients of $p(x)$ is 1. Then $p(x)$ is irreducible in $R[x]$ if and only if it is irreducible in $F[x]$. In particular, if $p(x)$ is a monic polynomial that is irreducible in $R[x]$ then $p(x)$ is irreducible in $F[x]$.*

Theorem 2.3. *A ring R is a unique factorisation domain if and only if $R[x]$ is a unique factorisation domain.*

Proof. The reverse direction was covered in the last lecture.
Suppose R is a UFD (unique factorisation domain), F is the field of fractions of R and $p(x) \in R[x]$ is non-zero.
Let d be the greatest common divisor of the coefficients of $p(x)$ (NOTE: The greatest common divisor exists because R is a UFD) and write $p(x) = dq(x)$. The greatest common divisor of the coefficients of q is 1. Since R is a UFD, d can be factored in R into irreducibles and irreducibles in R remain irreducible in $R[x]$ (this is simply because if $d \in R\backslash\{0\}$ and $d = a(x)b(x)$ then $\deg(a(x)) = \deg(b(x)) = 0$; so $a(x), b(x) \in R$).
We now attempt to write $q(x)$ as a product of irreducibles in $R[x]$. Since $F[x]$ is a UFD, there exist $q_1(x), q_2(x), ..., q_n(x) \in F[x]$ irreducible in $F[x]$ such that $q(x) = q_1(x) \cdots q_n(x)$. Gauss' lemma means we may assume these factors are in $R[x]$. Since the greatest common divisor of the coefficients of $q(x)$ is 1, the greatest common divisor of the

coefficients of each of the q_is is also 1. Thus by corollary 2.2 each of these factors is irreducible in $R[x]$. Thus we can write p as a product of irreducible elements in $R[x]$:

$$d_1 \cdots d_m q_1(x) \cdots q_n(x)$$

where $d = d_1 \cdots d_m$ and each d_i is irreducible in R.
It remains to show that this factorisation is unique up to ordering and multiplication by units. This is UB4 exercise 4.

□

Corollary 2.4. *If R is a UFD then so is $R[x_1, ..., x_n]$.*

Proof. Use induction on n. □

We will give two methods for testing the irreducibility of a polynomial over an integral domain.

Proposition 2.5. *Let I be a proper ideal of an integral domain (in German: Integritätsbereich) R and let $p(x)$ be a non-constant monic (in German: normierte) polynomial in $R[x]$. If the image of $p(x)$ in $(R/I)[x]$ can't be factored in $(R/I)[x]$ into two polynomials of smaller degree, then $p(x)$ is irreducible.*

Proof. Suppose $p(x)$ is non-constant, monic and reducible. Then $p(x) = a(x)b(x) \in R[x]$ with $a(x), b(x)$ non-constant (if either $a(x)$ or $b(x)$ were constant then would be a unit, since $p(x)$ is monic). We may assume that $a(x)$ and $b(x)$ are monic since $p(x)$ is monic.
Let $\overline{p}(x)$, $\bar{a}(x)$ and $\bar{b}(x)$ be the images of $p(x)$, $a(x)$ and $b(x)$ in $(R/I)[x]$. Then $\bar{p}(x) = \bar{a}(x)\bar{b}(x)$ and since $a(x)$ and $b(x)$ are monic and non-constant, $\bar{a}(x)$ and $\bar{b}(x)$ are non-constant and monic. By comparing degrees $\overline{a}(x)$ and $\overline{b}(x)$ are polynomials of smaller degree than $\overline{p}(x)$. □

The most common application of this result is to prove that a polynomial over $\mathbb{Z}$ is irreducible. For instance consider the polynomial $X^4 + 9X^3 + 10X^2 + 22X + 1 \in \mathbb{Z}[X]$.
Its image in $\mathbb{Z}_2[X]$ is $X^4 + X^3 + 1$. It is clear that this polynomial does not have a root in $\mathbb{Z}_2$ (check 0 and 1). Thus if it were irreducible, it must factor as a product of two polynomials in $\mathbb{Z}_2[x]$ of degree 2. If $p(x) \in \mathbb{Z}_2[X]$ is irreducible of degree 2 then its leading term is 1 and its constant term is also 1 since 0 is not a root. The polynomial $X^2 + 1$ has root 1. Therefore, there is only one irreducible polynomial of degree 2 in $\mathbb{Z}_2[X]$. That is $X^2 + X + 1$ (check it has no roots). But $(X^2 + X + 1)^2 = X^4 + X^2 + 1$. So $X^4 + X^3 + 1$ is irreducible over $\mathbb{Z}_2$.
Thus $X^4 + 9X^3 + 10X^2 + 22X + 1$ is irreducible over $\mathbb{Z}$.
Unfortunately this does not always work.

Proposition 2.6. *(Eisenstein's Criterion) Let $\mathfrak{p}$ be a prime ideal of an integral domain R, $n \geq 1$ and let $f(x) = x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0$ be a polynomial in $R[x]$. Suppose $a_{n-1}, ..., a_0 \in \mathfrak{p}$ and $a_0 \notin \mathfrak{p}^2$. Then $f(x)$ is irreducible in $R[x]$.*

Proof. **Claim**: If $a(x), b(x)$ are non-constant polynomials over an integral domain R with $a(x)b(x) = x^n$ and $n > 0$ then $b(0) = a(0) = 0$.
Proof of claim: Since R is an integral domain either $a(0) = 0$ or $b(0) = 0$. Suppose $a(0) = 0$. Let m be maximal such that $a(x) = x^m a'(x)$ for some $a'(x) \in R[x]$. Thus $a'(0) \neq 0$. So now $a'(x)b(x) = x^{n-m}$. Since $b(x)$ is non-constant $n - m > 0$. Therefore $a'(0)b(0) = 0$. So $b(0) = 0$. So we have proved the claim.
Suppose $f(x) = a(x)b(x)$ in $R[x]$ where $a(x)$ and $b(x)$ are non-constant polynomials. It is easy to see that the constant term of $f(x)$ is the product of the constant term of $a(x)$ and the constant term of $b(x)$.
Let $\bar{f}(x), \bar{a}(x), \bar{b}(x)$ be the images of $f(x), a(x)$ and $b(x)$ in $(R/\mathfrak{p})[x]$. Then $x^n = \bar{f}(x) = \bar{a}(x)\bar{b}(x)$. Thus $\bar{a}(0) = \bar{b}(0) = 0$ since $R/\mathfrak{p}$ is an integral domain. But this means that the constant terms of $a(x)$ and $b(x)$ are in $\mathfrak{p}$. Thus the constant term of $f(x)$ is in $\mathfrak{p}^2$ contradicting our assumptions. Therefore $f(x)$ is irreducible.

□

Corollary 2.7. *Let p be a prime in $\mathbb{Z}$, $n \geq 1$ and let $f(x) := x^n + a_{n-1}x^{n-1} + ... + a_0 \in \mathbb{Z}[x]$. Suppose that p divides a_i for all $0 \leq i \leq n-1$ but p^2 does not divide a_0. Then $f(x)$ is irreducible in both $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$.*

Proof. Apply Eisenstein at the prime ideal $\langle p \rangle$. □

The polynomial $X^5 7 + 10X^4 + 25X^2 + 35 \in \mathbb{Z}[X]$ is irreducible by Eisenstein's theorem applied at 5.
Extra example:
Consider the polynomial $f(X) := X^4 + 1\mathbb{Z}[x]$. We can't apply Eisenstein's theorem directly. Let $g(X) = f(X+1)$. So $g(X) = X^4 + 4X^3 + 6X^2 + 4X + 2$. Now, by Eisenstein applied at 2, $g(x)$ is irreducible and if f could be factored as a product of non-constant polynomials then so could g. Thus f is irreducible.

3. Fields

A reminder from linear algebra:

Definition 3.1. *The characteristic of a field F, denoted char(F) is the smallest strictly positive integer n such that $n \cdot 1_F$. If such an integer does not exist we say the characteristic is zero.*

Note that the characteristic of a field will always be zero or a primes (Check you know why?).

Definition 3.2. *The prime subfield (Primkörper eines Körpers) of a field F is the smallest subfield of F. Note that the prime subfield is always $\mathbb{Q}$ (when F has characteristic zero) or $\mathbb{F}_p$ (when F has positive characteristic p).*

Note that a field of characteristic p may well have infinitely many elements. For example consider the field of fractions of $\mathbb{F}_p[x]$.

Definition 3.3. *If K is a field containing a subfield F then K is called an extension field (in German: Körpererweiterung) of F, denoted K/F. We refer to F as the base field.*
If K/F is a field extension, then the multiplication defined in K makes K as a vector space over F.
The degree of a field extension (Grad einer Körpererweiterung) K/F, denoted $[K : F]$, is the dimension of K as a vector space over F. The extension is called finite if $[K : F]$ is finite and is called infinite otherwise.

Examples: The field extension $\mathbb{C}/\mathbb{R}$ has degree 2. Every element of $\mathbb{C}$ can be written as a linear combination of 1 and i and if $a + bi = 0$ then $a^2 + b^2 = (a + bi)(a - bi) = 0$; so $a = b = 0$. So $1, i$ are a basis for $\mathbb{C}$ as a vector space over $\mathbb{R}$.

Remark 3.4. *A homomorphism of fields is always injective.*

Proof. Let $\varphi : F \to K$ be a homomorphism between fields F and K. The kernel of φ is an ideal of F. The only ideals of F are $\{0\}$ and F. Since $\varphi(1_F) = 1_K \neq 0$, $\ker \varphi = 0$. So φ is injective. □

Theorem 3.5. *Let F be a field and $p(x) \in F[x]$ be irreducible. There exists a field K extension F of K in which $p(x)$ has a root.*

Proof. Consider the quotient $F[x]/\langle p(x)\rangle$. Since $p(x)$ is irreducible and $F[x]$ is a PID (Hauptidealbereich), the ideal generated by $p(x)$ is maximal. Therefore $F[x]/\langle p(x)\rangle$ is a field.
Let $\varphi : F[x] \to F[x]/\langle p(x)\rangle$ be the canonical homomorphism. The restriction of φ to F is a homomorphism of fields and thus is injective. Thus F is isomorphic to its image $\varphi(F)$ in $F[x]$. We may now identify F with its image in $F[x]/\langle p(x)\rangle$.
This is a subtle point: what does it mean to identify F with its image in $F[x]/\langle p(x)\rangle$?
If $\psi : F \to K$ is a homomorphism of fields (with K and F disjoint as sets) we simply relabel each element $\varphi(f)$ for $f \in F$ as f. We can do

this because ψ is injective; i.e. if $\psi(f) = \psi(g)$ then $f = g$. Now F as a set is a subset of K. Because ψ is a homomorphism $\psi(0) = 0$, $\psi(1) = 1$ and for all $f, g \in F$, $f + g = \psi(f) + \psi(g)$ and $f \cdot g = \psi(f) \cdot \psi(g)$. Thus F is also a subfield of K.

Back to the proof: Let $\bar{x}$ be the image of x in $F[x]/\langle p(x) \rangle$. We now have that $p(\overline{x}) = \overline{p(x)}$ since φ is a homomorphism. But $p(x) \in \langle p(x) \rangle$, so $\overline{p(x)} = 0$. Thus $\overline{x}$ is a root of the polynomial $p(x)$ in K. $\square$