In this lecture all rings are commutative with 1.

Main Problem: Let \( R \) be a domain and \( p(x) \in R[x] \) a non-constant polynomial. We want to find sufficient conditions for \( p(x) \) to be irreducible in \( R[x] \).

We are mostly interested in the case when \( R \) is a UFD, in which case \( R[x] \) is also a UFD by Theorem 23.1.

24.1. Irreducibility in \( F[x] \) where \( F \) is a field. Throughout this subsection \( F \) is a field and \( p(x) \in F[x] \).

Observation A. Suppose that \( \deg p(x) = 1 \), that is, \( p(x) = ax + b \) with \( a \neq 0 \). Then \( p(x) \) is always irreducible and has a root in \( F \), namely \( -\frac{b}{a} \).

Observation B. Let \( \alpha \in F \). Then \( (x - \alpha) \mid p(x) \iff p(\alpha) = 0 \).

Corollary 24.1. Suppose that \( \deg p(x) \geq 2 \) and \( p(x) \) is irreducible. Then \( p(x) \) has no roots in \( F \).

Corollary 24.2. Suppose that \( \deg p(x) = 2 \) or 3. Then \( p \) is irreducible \( \iff p \) has no roots in \( F \).

Proof. “\( \Rightarrow \)” holds by Corollary 24.1.

“\( \Leftarrow \)” Suppose that \( p(x) \) is not irreducible, so \( p(x) = g(x)h(x) \) with \( g, h \) non-units in \( F[x] \). Then \( 1 \leq \deg g(x), \deg h(x) \) and \( \deg g(x) + \deg h(x) \leq 3 \). Hence \( \deg g(x) = 1 \) or \( \deg h(x) = 1 \), so \( g \) or \( h \) has a root in \( F \), whence \( p \) has a root in \( F \). \( \square \)

24.2. Reduction modulo an ideal.

Proposition 24.3. Let \( R \) be a domain and \( I \) a prime ideal of \( R \), so that \( R/I \) is also a domain. Given \( f(x) \in R[x] \), denote by \( \overline{f}(x) \in (R/I)[x] \) the reduction of \( f(x) \mod I \). Let \( p(x) \in R[x] \) be a non-constant polynomial such that

(i) The leading coefficient of \( p(x) \) does not lie in \( I \)
(ii) \( \text{cont}(p) = 1 \)
(iii) \( \overline{p}(x) \) is irreducible in \( (R/I)[x] \).

Then \( p(x) \) is irreducible in \( R[x] \).
Proof. Suppose $p(x)$ is not irreducible in $R[x]$. First note that since $R$ is a domain and $p(x)$ is non-constant, it cannot be a unit in $R[x]$. Thus,

$$p(x) = g(x)h(x) \quad (\ast\ast)$$

where $g, h$ are non-units of $R[x]$. Note that $g$ and $h$ must be non-constant; otherwise $cont(p) \neq 1$, contrary to (ii).

Since the reduction map $f(x) \mapsto \overline{f}(x)$ is a ring homomorphism, applying it to both sides of $(\ast\ast)$, we get

$$\overline{p}(x) = \overline{g}(x)\overline{h}(x) \quad (!!!)$$

Note that $\deg \overline{p}(x) = \deg p(x)$ by assumption (i). Hence $(\ast\ast)$ and $(!!)$ imply that $\deg \overline{g}(x) = \deg g(x) > 0$ and $\deg \overline{h}(x) = \deg h(x) > 0$. Since $R/I$ is a domain, this implies that $\overline{h}$ and $\overline{g}$ are non-units if $(R/I)[x]$. Thus, $\overline{p}(x)$ is reducible in $(R/I)[x]$, contrary to (iii). \hfill $\square$

Remark: (a) Conditions (i) and (ii) hold automatically if $p(x)$ is monic, that is, the leading coefficient of $p(x)$ is equal to 1.

(b) The above proof does not fully use the assumption that $R$ and $R/I$ are domains. All we needed is that for $S = R$ or $S = R/I$ non-constant polynomials in $S[x]$ are not units. However, this property holds under the weaker assumption that $S$ has no nilpotent elements (exercise: prove this).

Thus, Proposition 24.3 remains true if we only assume that $R$ and $R/I$ have no nilpotent elements.

The following application of Proposition 24.3 is a homework problem.

**Corollary 24.4.** Let $F$ be a field, $f(x,y) \in F[x,y]$, and write $f(x,y) = f_n(y)x^n + \ldots + f_0(y)$ where $f_i(y) \in F[y]$. Assume that there exists $\alpha \in F$ such that

(i) $f_n(\alpha) \neq 0$

(ii) $\gcd(f_0(y), \ldots, f_n(y)) = 1$

(iii) $f(x,\alpha)$ is irreducible in $F[x]$.

Then $f(x,y)$ is irreducible in $F[x,y]$.

**Sample application:** $f(x,y) = x^2 - y^2 - 4$ is irreducible in $\mathbb{Q}[x,y]$ (e.g. apply the above corollary with $\alpha = 1$).
24.3. Eisenstein criterion.

Theorem (Eisenstein criterion). Let $R$ be a domain, $p \in R$ a prime element, and let $f(x) = a_n x^n + \ldots + a_0 \in R[x]$. Assume that

(i) $p \nmid a_n$  
(ii) $p \mid a_i$ for $0 \leq i \leq n - 1$  
(iii) $p^2 \nmid a_0$  
(iv) cont$(f) = 1$.

Then $f(x)$ is irreducible in $R[x]$.

Remark: If $R$ is a UFD, combining Eisenstein criterion with Gauss lemma, we deduce that any $f(x) \in R[x]$ satisfying (i)-(iv) is irreducible in $F[x]$, where $F$ is the field of fractions of $R$.

Proof. Suppose not. Arguing as in Proposition 24.3, we deduce that $f(x)$ cannot by unit, so $f(x) = g(x)h(x)$ with $\deg g > 0$ and $\deg h > 0$.

Consider the reduction mod $p$ homomorphism $R[x] \to R/(p)[x]$. As in Proposition 24.3 the image of a polynomial $u(x) \in R[x]$ under this homomorphism is denoted by $\overline{u}(x)$.

We have $\overline{f}(x) = \overline{g}(x)\overline{h}(x)$ and $\deg \overline{g}, \deg \overline{h} > 0$ as in Proposition 24.3. Condition (ii) implies that $\overline{f}(x) = a_n x^n$. Thus $\overline{g}(x) \cdot \overline{h}(x) = a_n x^n$.

Claim. $\overline{g}$ and $\overline{h}$ are (non-constant) monomials, that is, $\overline{g}(x) = \beta x^m$ and $\overline{h}(x) = \gamma x^l$ for some $\beta, \gamma \in R/(p)$ and $m, l > 0$.

Proof of the claim. Suppose that $\overline{g}$ and $\overline{h}$ are not monomials. We will consider the case when both of them are not monomials (the case when exactly one of them is not a monomial is similar). Then we can write

$$\overline{g}(x) = \beta x^m + \ldots + \delta x^s \quad \text{and} \quad \overline{h}(x) = \gamma x^l + \ldots + \varepsilon x^t$$

where $\beta x^m$ and $\gamma x^l$ are highest degree terms and $\delta x^s$ and $\varepsilon x^t$ are (nonzero) lowest degree terms. By our assumption $s < m$ and $t < l$. Multiplying these expressions we get

$$\overline{f}(x) = \overline{g}(x)\overline{h}(x) = \beta \gamma x^{m+l} + \ldots + \delta \varepsilon x^{s+t}.$$ 

Since $R/(p)$ is a domain, $\beta \gamma \neq 0$ and $\delta \varepsilon \neq 0$. Thus, the above equality implies that $\overline{f}(x)$ is not a monomial, which is a contradiction.

The claim implies that $g(x) = bx^m + pu(x)$ and $h(x) = cv^l + pv(x)$ for some $b, c \in R$ and $u(x), v(x) \in R[x]$. But then

$$f(x) = g(x)h(x) = bc x^m v(x) + pv(x)x^m + pu(x)x^l + p^2 u(x)v(x).$$

Note that the first three summands on the right hand side are divisible by $x$. Thus, the constant term of $f(x)$ is equal to the constant term of $p^2 u(x)v(x)$ and thus divisible by $p^2$. This contradicts hypothesis (iii).
Standard applications of Eisenstein criterion.

1. \( f(x) = x^n - p \) is irreducible in \( \mathbb{Z}[x] \) (hence also in \( \mathbb{Q}[x] \)) for any \( n \geq 1 \) and prime \( p \). This is clear.

2. If \( p \) is a prime, the Eisenstein polynomial \( E_p(x) = x^{p-1} + x^{p-2} + \ldots + 1 \) is irreducible in \( \mathbb{Z}[x] \). This can be proved as follows.
   
   First note that \( E_p(x) \) is irreducible \( \iff \) \( E_p(x+1) \) is irreducible (this is very easy). We can write \( E_p(x) = \frac{x^{p-1}}{x-1} \), treating \( \frac{x^{p-1}}{x-1} \) as an element of the field of fractions of \( \mathbb{Z}[x] \). Then
   
   \[
   E_p(x + 1) = \frac{(x + 1)^p - 1}{x} = \frac{1}{x} \sum_{k=1}^{p} \binom{p}{k} x^k = x^{p-1} + \sum_{k=1}^{p-1} \binom{p}{k} x^{k-1}
   \]

   Since \( p \mid \binom{p}{i} \) for \( 0 < i < p \) and \( \binom{p}{p-1} = p \) is not divisible by \( p^2 \), the polynomial \( E_p(x + 1) \) is irreducible by the Eisenstein criterion.

3. \( f(x, y) = x^4 + x^3 y^2 + x^2 y^3 + y \) is irreducible in \( \mathbb{Q}[x, y] \). This can be proved by treating \( \mathbb{Q}[x, y] \) as \( (\mathbb{Q}[y])[x] \) and applying the Eisenstein criterion with \( p = y \).

Remark: Irreducibility of \( E_p(x) \) in \( \mathbb{Z}[x] \) can also be proved by combining the result of Problem\#8 on the final exam and Proposition 24.3.