irreducibles.

Since $F = Quot(R)$, as before clearing denominators in p_i's we get

$$d_i p_i(x) = q_i(x) \quad \text{with } q_i(x) \in R[x]$$

and $d_i \in F$ is a unit in F. Hence $q_i(x)$ are irreducible in $F[x]$.

By lemma 1.14 we factor the contents and write

$$f(x) = c\, g(x), \qquad q_i(x) = c_i\, q_i'(x)$$

with c, c_i's $\in R$, $g(x), q_i'(x) \in R[x]$ primitive.

Hence we get

$$d c\, g(x) = (c_1 \dots c_r) q_1'(x) \dots q_r'(x)$$

By Gauss Lemma $q_1' \dots q_r'$ is primitive.

By uniqueness part of Lemma 1.14

$$c_1 \dots c_r = dcu \quad \text{with some unit } u \text{ in } R$$

$$d f(x) = dc g(x) = dcu\, q_1' \dots q_r'$$

and $f(x) = c g(x) = cu\, q_1'(x) \dots q_r'(x)$

Since $q_1'(x) \dots q_r'(x)$ are irred. in $F[x]$ and primitive, they are also irred in $R[x]$

Thus $f(x)$ is a product of irreducibles in $R[x]$ ($cu \in R$ is a product of irreducibles)

For uniqueness, if $\deg f = 0$ we again have uniqueness since then $f \in R$, and R is a UFD.
We can assume wlog f is primitive if $\deg f > 0$.
(Since if not $f(x) = d f'(x)$ w/ f' primitive and d has unique factorization in R). Let $f = g_1 \cdots g_r = h_1 \cdots h_s$ with $g_1, \cdots g_r, h_1, \cdots h_s$ irred. polys in $R[X]$.
Since $\text{content}(f) = 1$, $\text{content}(h_i) = \text{content}(g_j) = 1$.
By Prop 1.16 they are irred in $F[X]$.
Since $F[X]$ is a UFD we have $r = s$ and after reordering if necessary g_i, h_i are associates in $F[X]$ for each i

Let $g_i = c_i h_i$ for some constant $c_i \in F$
where $c_i = \frac{a_i}{b_i}$, $a_i, b_i \in R$

Hence $b_i g_i = a_i h_i$, We have $\text{content}(g_i) = \text{content}(h_i) = 1$

By uniqueness in Lemma 1.14
$u b_i = a_i$ for some u unit in R.

Hence $g_i = u h_i$ for some $u \in R^\times$
Hence $g_i \sim h_i$ in $R[X]$ and hence the factorization in $R[X]$ is unique

$\blacksquare$

Next we look at irreducibility criteria

The following is used often.

Thm 1-18

Eisenstein's irreducibility criteria

let R be a UFD, with quotient field F.
let $f(X) = a_n X^n + \cdots + a_0 \in R[X]$, $n \geq 1$
$a_n \neq 0$.
If p is a prime in R such that $p \mid a_i$ $0 \leq i < n$
but $p \nmid a_n$ and $p^2 \nmid a_0$, then
f is irreducible over F.
If f is primitive then f is irreducible over R.

Proof. If we divide f by its content $= \gcd(a_n, \ldots a_0)$
and write $f = cf'$ with f' primitive
the hypothesis of the thm still holds.
ie if $f' = a_n' x^n + \cdots + a_0'$ then
$p \mid a_i'$ $\forall$ $0 \leq i < n$ but $p \nmid a_n'$ and $p^2 \nmid a_0$
To see this note
since $p \nmid a_n$ p cannot be a prime
factor of $c = \gcd(a_0, \ldots a_n)$, ie $p \nmid c$
but $p \mid a_i = c a_i'$ hence $p \mid a_i'$ $0 \leq i < n$
(Since $p \nmid a_n = c a_n'$, $p \nmid a_n'$, similarly $p^2 \nmid a_0 = c a_0' \Rightarrow p^2 \nmid a_0'$
Hence wlog we can assume f is primitive.
and prove that f is irreducible over R.

Assume $f = gh$ with

$g(x) = b_0 + \dots + b_r x^r$
$h(x) = c_0 + \dots c_s x^s$

If $r = 0$ then b_0 divides content$(f) = 1$ hence b_0 is a unit. Thus we can assume $r \geq 1$ and similarly $s \geq 1$.

By hypothesis $p \mid a_0 = b_0 c_0$ but $p^2 \nmid a_0$. So p cannot divide both b_0 and c_0. Assume $p \nmid c_0$ so that $p \mid b_0$

Now $a_n = b_r c_s$ and by hyp $p \nmid a_n$ hence $p \nmid b_r$.

Let i be the smallest index s.t $p \nmid b_i$.
Then $1 \leq i \leq r < n$ since $r + s = n$, and $s \geq 1$

Now $a_i = b_0 c_i + \dots + b_i c_0$
by choice of i $p \mid b_0 c_i, \dots p \mid b_{i-1} c_1$
and $p \mid a_i$ by assumption
Hence $p \mid b_i c_0$. Hence $p \mid c_0$ since $p \nmid b_i$. But this contradicts our assumption $p \nmid c_0$ $\lightning$

$\blacksquare$.

Ex. ① $f(x) = x^4 - 9x + 3$ primitive, monic

We can apply Eisenstein criteria with $p = 3$, $p \nmid a_4$, $p \mid a_3, a_2, a_1, a_0$, $p^2 \nmid a_0$

Hence it irreducible in $\mathbb{Z}[x]$ and irreducible in $\mathbb{Q}[x]$.

② Let a be an integer divisibly by p but not by p^2. Then $x^n \pm a$ is irredubicle in $\mathbb{Z}[x]$.

e.g $x^{2024} + 6$ is irred in $\mathbb{Z}[x]$. hence in $\mathbb{Q}[x]$.

③ We cannot apply Eisenstein to say $x^4 + 1$ or can we?

Lemma 1.19 Let $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ be primitive.

Let $a \in \mathbb{Z}$. Then f is irred in $\mathbb{Z}[x]$ (and hence in $\mathbb{Q}[x]$) $\iff$ $f(x+a) := \sum a_i (x+a)^i$ is irred in $\mathbb{Z}[x]$

Proof: Check that the map
$$\varphi_a : \mathbb{Z}[x] \longrightarrow \mathbb{Z}[x]$$
$$g(x) \longmapsto g(x+a)$$

is an isom of rings, and hence g is irred $\Leftrightarrow$ $g(x+a)$ is irreducible ☒.

Ex ① $f(x) = x^4+1 \in \mathbb{Z}[x]$.

Let $g(x) = f(x+1) = (x+1)^4+1 = x^4+4x^3+6x^2+4x+2$ we can apply Eisenstein criteria to $g(x)$ w/ $p=2$ to get g is irreducible. Hence $f = x^4+1$ is irreducible

② Important example.

Let $\Phi_p(X) := \frac{x^p-1}{x-1} = x^{p-1}+x^{p-2}+ \cdots +x+1$

called the p-th cyclotomic polynomial.

Claim $\Phi_p(X)$ is irreducible in $\mathbb{Z}[x]$.

Proof $\Phi_p(X+1) = \frac{(x+1)^p-1}{x} = x^{p-1}+px^{p-2}+\cdots+\binom{p}{i}x^{i-1}+\cdots+p$

Then since $p \mid \binom{p}{i} = \frac{p!}{i!(p-i)!}$, by Eisenstein $\Phi_p(X)$ is irred. ☒.

Before we move on to field extentions we give few other simple lemmas which might help with the decision of reducibilty/irreducibilty of polynomials.

Recall that if F is a field, $a \in F$ $f(x) \in F[x]$. Then
$$f(a) = 0 \iff (x-a) \mid f(x) \text{ in } F[x].$$

A simple corollary of this is

Lemma 1.20 A polynomial of degree 2 or 3 over a field F is reducible if and only if it has a root in F

Pf. A poly of degree 2 or 3 is reducible $\iff$ it has at least one linear factor
$\iff$ it has at least one root in F ☒

Rmk: Note Lemma 1.9 is not true for polynomials of degree > 3.
eg. $(x^2+1)(x^2+1)$ is reducible in $\mathbb{Q}[x]$ (or $\mathbb{R}[x]$) but does not have a root in $\mathbb{Q}$ (or $\mathbb{R}$).

Another useful tool is to use the reduction homomorphism

Lemma 1.21 Let p be a prime, let $f = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ be a primitive polynomial. Assume $p \nmid a_n$.
Denote $\bar{a}_i$ the class of a_i in $\mathbb{Z}/p\mathbb{Z}$
and $\bar{f} := \sum_{i=0}^{n} \bar{a}_i x^i \in (\mathbb{Z}/p\mathbb{Z})[x]$.

If $\bar{f}$ is irreducible in $(\mathbb{Z}/p\mathbb{Z})[x]$ then f is irreducible in $\mathbb{Z}[x]$. (and hence also in $\mathbb{Q}[x]$).

Proof: Suppose f is reducible in $\mathbb{Z}[x]$
Since f is primitive
$f = gh$ with $\deg g$, $\deg h < n$

and $\bar{f} = \bar{g}\bar{h}$ with $\deg \bar{g}$, $\deg \bar{h} < n$

As $\deg \bar{f} = n$ $(p \nmid a_n)$ it follows that $\deg(\bar{g})$, $\deg(\bar{h}) \geq 1$ (Since otherwise one of $\deg \bar{g}$ or $\deg \bar{h} = n$)
and then $\bar{f}$ is reducible

$\blacksquare$

Rmk ① Note Lemma 1.20 does <u>not</u> say that
$\left\{ \begin{array}{l} \text{If } \bar{f} \text{ is reducible for some } p \text{ then} \\ f \text{ is reducible.} \end{array} \right\}$ not true

In fact there are polynomials f that are reducible $\forall p$ but f is irreducible over $\mathbb{Z}$.

e.g. x^4+1 is irreducible in $\mathbb{Z}[x]$ but is reducible in $(\mathbb{Z}/p\mathbb{Z})[x]$ for every prime p.
We will see a proof of this when we study finite fields.

Rmk 2 Lemma 1.21 is true for a general I.D R, and I proper ideal.
ie Let $p(x) \in R[x]$ monic polynomial.
if $\bar{p}(x) \in (R/I)[x]$ cannot be factored in $(R/I)[x]$ into 2 polys of smaller degree, then $p(x)$ is irreducible in $R[x]$.

Ex: We can use Lemma 1.21 to prove irreducibility of $f = x^2+x+1 \in \mathbb{Z}[x]$

In $\mathbb{Z}_2[x]$ $\bar{f} = x^2+x+1$ is irreducible since it has no roots in $\mathbb{Z}_2$

$\bar{f}(0) = 1$
$\bar{f}(1) = 1$

Finally the following lemma allows finding the rational zeroes of a polynomial in $\mathbb{Z}[x]$

Lemma 1.22 Let $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$

If $\frac{r}{s} \in \mathbb{Q}$ with $(r,s)=1$ is a root of $f(x)$ then $r \mid a_0$ and $s \mid a_n$

In particular if $f(x)$ is monic and if for all $d \mid a_0$, $f(d) \neq 0$, then f has no zeroes in $\mathbb{Q}$.

Pf. Exercise : clear out denominators in $f(\frac{r}{s}) = 0$.

Ex: $f(x) = x^3 - 3x + 1$ is irred in $\mathbb{Z}[x]$ since it has no roots in $\mathbb{Q}$.

If $\frac{r}{s}$ is a root then $r = \pm 1$, $s = \pm 1$, hence

$\frac{r}{s} = \pm 1$ But $f(1) = 1 - 3 + 1 \neq 0$
$f(-1) = -1 + 3 + 1 \neq 0$.

§2 Fields and Field extentions

Goal: To set the stage for Galois theory which was historically motivated by a very natural question.

Namely given a polynomial

$$f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$$

Can we solve the equation $f(x)=0$ by a formula given in terms of the coefficients a_i and by the operations $+, -, \times, \div$ and also by n-th roots $n = 2, 3, 4 \dots$

The quadratic formula goes back to Babylonians. By the middle of 16th century the cubic, and quartic formulas were known.

Abel in 1824 proved that $\exists$ a quintic polynomial whose roots cannot be given by such a formula (Following Lagrange)

In 1829 Abel gave a sufficient condition that a polynomial (of any degree) have such a formula

in 1831 Galois gave a necessary and sufficient condition completely settling the problem

Galois's main idea was to look at symmetries of the polynomial, which form a group called the Galois group of f. The solution of the polynomial equation is related to properties of its Galois group.

We'll see how the theory of (algebraic) field extensions can be applied to problems of distinguished history

1) Doubling the cube. Is it possible to construct using only straightedge and compass, a cube with precisely twice the volume of a given cube?

2) Trisecting an angle. Is it possible, using only SE and compass to trisect any given angle θ?

3) Squaring the circle. Is it possible to construct a square whose area is precisely the area of a given circle?

These questions go back to Greeks