Lecture 5.1

Last time:

- A **prime ideal** $P \subsetneq A$ is an ideal with the property that for ideals $I, J \subseteq A$,

$$IJ \subseteq P \Rightarrow I \subseteq P \text{ or } J \subseteq P.$$

- $P \subseteq A$ is a prime ideal $\Leftrightarrow$ A/P is an integral domain.

Def Let A be a commutative ring.

- An element $m \in A$ is **irreducible** if

whenever we can write $m = ab$ for some $a, b \in A$, then a or b is a unit $(a \in A^\times$ or $b \in A^\times)$.

- An element $p \in A$ is **prime** if for any $a, b \in A$ such that $ab \in (p)$, we have $a \in (p)$ or $b \in (p)$.

Prop Let A be an integral domain. Then

(1) $p \in A$ is prime if and only if (p) is a prime ideal.

(2) $m \in A$ is irreducible if and only

if (m) is maximal among all principals.

(3) If A is a PID, then $m \in A$ is irreducible if and only if (m) is a maximal ideal.

(4) If A is a PID, then $p \in A$ is prime if and only if it's also irreducible.

Exercise 1: try to prove some parts yourself, and look it up in a textbook

if you get stuck.

Theorem If $\mathbb{F}$ is a field then $\mathbb{F}[x]$ is a PID.

Exercise 2: Prove $\mathbb{F}[x]$ is an integral domain. What about $A[x]$ if A is not a field?

Pf: Take an ideal $I \subseteq \mathbb{F}[x]$ and choose an element $f(x) \in I$ of minimal degree; that is, for all $g(x) \in I$,

$\deg g \geq \deg f$ or $g(x) = 0$.

We claim $I = (f)$.

For any $p(x) \in I$, we must show

$p(x) \in (f)$, i.e. f divides p.

Using the Polynomial Division Algorithm,

we can write

$$p(x) = f(x)q(x) + r(x) \quad \text{for}$$

$$q, r \in \mathbb{F}[x], \quad \deg r < \deg f.$$

Then $r(x) = \underbrace{p(x)}_{\in I} - \underbrace{f(x)q(x)}_{\in I} \in I.$

But $\deg r < \deg f$ so $r = 0$.

Hence $I \subseteq (f)$ so $I = (f)$. □

Corollary If $\mathbb{F}$ is a field, then the maximal and (nonzero) prime ideals are the same, and are of the form (f) for some irreducible element $f \in \mathbb{F}[x]$.

Remark: if A is not a field, then $A[x]$ does not have to be a PID.

For example, $\mathbb{Z}[x]$ is not a PID:

- $(x^2+1, x+2)$ is maximal but not principal

- (x) and (x^2+1) are prime but not maximal.

Lemma Let $\mathbb{F}$ be a field and suppose $f(x) \in \mathbb{F}[x]$ has degree ≥ 2 and $f(\alpha) = 0$ for some $\alpha \in \mathbb{F}$. Then $f(x)$ is reducible (= not irreducible).

Pf: We know that

$$(x-\alpha) = \{ p(x) \in \mathbb{F}[x] \mid p(\alpha) = 0 \}$$

so for $f(x)$ with root α,

$$f(x) \in (x-\alpha) \iff f(x) = (x-\alpha)q(x).$$

If $\deg f \geq 2$, we must have $\deg q \geq 1$, but the only units in $\mathbb{F}[x]$ have degree 0.

Therefore $f(x)$ is reducible. □

Corollary In $\mathbb{R}[x]$, the maximal/prime ideals are all of the form

(a) $(x-\alpha)$ for some $\alpha \in \mathbb{R}$, or

(b) (x^2+bx+c) for some $b, c \in \mathbb{R}$

with $b^2-4c < 0$.

Pf: Let $f(x) \in \mathbb{R}[x]$ be an irreducible polynomial, so (f) is maximal.

If $\deg f = 0$, then $f(x) = a_0 \in \mathbb{F}$

and either:

- $a_0 = 0 \Rightarrow \mathbb{F}[x]/(f) = \mathbb{F}[x]$ which is not a field, or

$a_0 a_0^{-1} = 1$

- $a_0 \in \mathbb{F}^\times \Rightarrow (a_0) = (1)$ which is not maximal. $(M \subsetneq A)$

If $\deg f = 1$, we can divide out the leading term to get $(f) = (x - \alpha)$ for some $\alpha \in \mathbb{R}$.

If $\deg f = 2$, then f has a real root (and is therefore reducible by the lemma) if and only

$$f(x) = ax^2 + bx + c \quad \text{and} \quad b^2 - 4ac \geq 0$$

by the quadratic formula.

If f doesn't have a real root, we can again divide by a to get

$$(f) = (x^2 + b'x + c'x) \text{ with}$$

$$(b')^2 - 4c' < 0.$$

Finally, suppose $\deg f \geq 3$.

View $\mathbb{R}[x] \subseteq \mathbb{C}[x]$ as a subring.

By the Fundamental Theorem of Algebra, $f(x)$ has a complex root, say $\alpha \in \mathbb{C}$.

Case 1: $\alpha \in \mathbb{R}$. Then $f(x)$ is reducible by the Lemma.

Case 2: $\alpha \notin \mathbb{R}$, say $\alpha = s + it$ for $s, t \in \mathbb{R}$. Then

$$f(\bar{\alpha}) = f(s - it) = 0.$$

So $\underbrace{(x-\alpha)(x-\bar{\alpha})}_{\in \mathbb{C}[x]} \mid \underbrace{f(x)}_{\in \mathbb{R}[x]}$

But $(x-\alpha)(x-\bar{\alpha}) =$

$$= x^2 - (\alpha + \bar{\alpha})x + \alpha\bar{\alpha}$$

$$= x^2 - 2sx + (s^2 + t^2) \in \mathbb{R}[x]$$

So $f(x) = (x^2 - 2sx + (s^2+t^2))\, g(x)$.

So $f(x)$ is reducible. □

Ex ① Over different fields, there are irreducible polynomials of degree ≥ 3.

For example,

$x^3 - x - 2 \in \mathbb{F}_3[x]$ (HW 4)

$x^4 + x^3 + x^2 + x + 1 \in \mathbb{F}_7[x]$

$x^5 - x + 1 \in \mathbb{F}_5[x]$

$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \in \mathbb{F}_{17}[x]$

Exercise 3: Prove these are irreducible.

Galois Theory: Motivation

In $\mathbb{R}[x]$, the quadratic formula

$$x = \frac{-b \pm \sqrt{b^2-4ac}}{2a} \quad \text{if} \quad ax^2+bx+c = 0$$

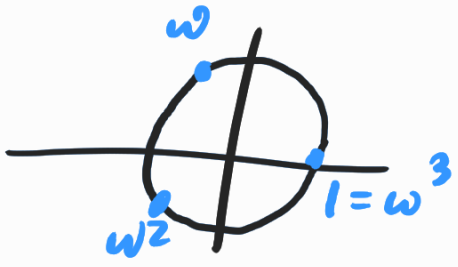
was useful for classifying irreducible polynomials.

For cubic and quartic equations, we have:

Theorem Let $f(x)$ be a polynomial of degree 3 or 4. Then

(1) If $f(x) = x^3 + bx^2 + cx + d$, the roots of f are

$$x = -\left(b + \omega^k R + \frac{b^2 - 3c}{\omega^k R}\right)$$



where $\omega = e^{2\pi i/3}$ is a primitive 3rd root of unity

$0 \le k \le 2$ (so $\omega^k = 1, \omega, \omega^2$ are the 3rd roots of unity)

and

$$R = \sqrt[3]{\frac{(2b^3 - 9bc + 27d) \pm \sqrt{(2b^3 - 9bc + 27d)^2 - 4(b^2 - 3c)^3}}{2}}$$

(2) If $f(x) = ax^4 + bx^3 + cx^2 + dx + e$, then the roots of f are

$$x_1 = -\frac{b}{4a} - \frac{1}{2}\sqrt{\frac{b^2}{4a^2} - \frac{2c}{3a} + \frac{q\sqrt[3]{2}}{3a\sqrt[3]{p + \sqrt{-4q^3 + p^2}}} + \frac{\sqrt[3]{p + \sqrt{-4q^3 + p^2}}}{3a\sqrt[3]{2}}} - \frac{1}{2}\sqrt{\frac{b^2}{2a^2} - \frac{4c}{3a} - \frac{q\sqrt[3]{2}}{3a\sqrt[3]{p + \sqrt{-4q^3 + p^2}}} - \frac{\sqrt[3]{p + \sqrt{-4q^3 + p^2}}}{3a\sqrt[3]{2}} - \frac{\left(-\frac{b^3}{a^3} + \frac{4bc}{a^2} - \frac{8d}{a}\right)}{4\sqrt{\frac{b^2}{4a^2} - \frac{2c}{3a} + \frac{q\sqrt[3]{2}}{3a\sqrt[3]{p + \sqrt{-4q^3 + p^2}}} + \frac{\sqrt[3]{p + \sqrt{-4q^3 + p^2}}}{3a\sqrt[3]{2}}}}}}$$

$$x_2 = -\frac{b}{4a} - \frac{1}{2}\sqrt{\frac{b^2}{4a^2} - \frac{2c}{3a} + \frac{q\sqrt[3]{2}}{3a\sqrt[3]{p + \sqrt{-4q^3 + p^2}}} + \frac{\sqrt[3]{p + \sqrt{-4q^3 + p^2}}}{3a\sqrt[3]{2}}} + \frac{1}{2}\sqrt{\frac{b^2}{2a^2} - \frac{4c}{3a} - \frac{q\sqrt[3]{2}}{3a\sqrt[3]{p + \sqrt{-4q^3 + p^2}}} - \frac{\sqrt[3]{p + \sqrt{-4q^3 + p^2}}}{3a\sqrt[3]{2}} - \frac{\left(-\frac{b^3}{a^3} + \frac{4bc}{a^2} - \frac{8d}{a}\right)}{4\sqrt{\frac{b^2}{4a^2} - \frac{2c}{3a} + \frac{q\sqrt[3]{2}}{3a\sqrt[3]{p + \sqrt{-4q^3 + p^2}}} + \frac{\sqrt[3]{p + \sqrt{-4q^3 + p^2}}}{3a\sqrt[3]{2}}}}}}$$

$$x_3 = -\frac{b}{4a} - \frac{1}{2}\sqrt{\frac{b^2}{4a^2} - \frac{2c}{3a} + \frac{q\sqrt[3]{2}}{3a\sqrt[3]{p + \sqrt{-4q^3 + p^2}}} + \frac{\sqrt[3]{p + \sqrt{-4q^3 + p^2}}}{3a\sqrt[3]{2}}} - \frac{1}{2}\sqrt{\frac{b^2}{2a^2} - \frac{4c}{3a} - \frac{q\sqrt[3]{2}}{3a\sqrt[3]{p + \sqrt{-4q^3 + p^2}}} - \frac{\sqrt[3]{p + \sqrt{-4q^3 + p^2}}}{3a\sqrt[3]{2}} + \frac{\left(-\frac{b^3}{a^3} + \frac{4bc}{a^2} - \frac{8d}{a}\right)}{4\sqrt{\frac{b^2}{4a^2} - \frac{2c}{3a} + \frac{q\sqrt[3]{2}}{3a\sqrt[3]{p + \sqrt{-4q^3 + p^2}}} + \frac{\sqrt[3]{p + \sqrt{-4q^3 + p^2}}}{3a\sqrt[3]{2}}}}}}$$

$$x_4 = -\frac{b}{4a} + \frac{1}{2}\sqrt{\frac{b^2}{4a^2} - \frac{2c}{3a} + \frac{q\sqrt[3]{2}}{3a\sqrt[3]{p + \sqrt{-4q^3 + p^2}}} + \frac{\sqrt[3]{p + \sqrt{-4q^3 + p^2}}}{3a\sqrt[3]{2}}} + \frac{1}{2}\sqrt{\frac{b^2}{2a^2} - \frac{4c}{3a} - \frac{q\sqrt[3]{2}}{3a\sqrt[3]{p + \sqrt{-4q^3 + p^2}}} - \frac{\sqrt[3]{p + \sqrt{-4q^3 + p^2}}}{3a\sqrt[3]{2}} + \frac{\left(-\frac{b^3}{a^3} + \frac{4bc}{a^2} - \frac{8d}{a}\right)}{4\sqrt{\frac{b^2}{4a^2} - \frac{2c}{3a} + \frac{q\sqrt[3]{2}}{3a\sqrt[3]{p + \sqrt{-4q^3 + p^2}}} + \frac{\sqrt[3]{p + \sqrt{-4q^3 + p^2}}}{3a\sqrt[3]{2}}}}}}$$

$$x_4 = -\frac{b}{4a} - \frac{1}{2}\sqrt{\frac{b^2}{4a^2} - \frac{2c}{3a} + \frac{q\sqrt[3]{2}}{3a\sqrt[3]{p+\sqrt{-4q^3+p^2}}} + \frac{\sqrt[3]{p+\sqrt{-4q^3+p^2}}}{3a\sqrt[3]{2}}} + \frac{1}{2}\sqrt{\frac{b^2}{2a^2} - \frac{4c}{3a} - \frac{q\sqrt[3]{2}}{3a\sqrt[3]{p+\sqrt{-4q^3+p^2}}} - \frac{\sqrt[3]{p+\sqrt{-4q^3+p^2}}}{3a\sqrt[3]{2}} + \frac{\left(-\frac{b^3}{a^3} + \frac{4bc}{a^2} - \frac{8d}{a}\right)}{4\sqrt{\frac{b^2}{4a^2} - \frac{2c}{3a} + \frac{q\sqrt[3]{2}}{3a\sqrt[3]{p+\sqrt{-4q^3+p^2}}} + \frac{\sqrt[3]{p+\sqrt{-4q^3+p^2}}}{3a\sqrt[3]{2}}}}}}$$

Perhaps more surprisingly,

Theorem There is no algebraic formula

(i.e. using $+, -, \times, \div, (\,)^n$ and $\sqrt[n]{\ }$)

for the roots of a general polynomial

$f(x)$ of degree ≥ 5.

Idea behind all the proofs: finding

solutions to $f(x) = 0$ is equivalent to

studying homomorphisms

$$\varphi : \mathbb{F}[x] \longrightarrow K$$

where $f \in \ker(\varphi)$ and K is a field.

For such a K, there is a map

$$\mathbb{F} \hookrightarrow K$$

and a group $G = \mathrm{Aut}(K/\mathbb{F})$

that acts on the roots of polynomials

in a way that makes it easier

to study the roots algebraically.

When $\deg f = 2, 3, 4,$ G is a subgroup of S_2, S_3 or S_4 and the group theory of S_n allows one to find algebraic formulas for the roots of f.

When $\deg f \geq 5$, $G \leq S_n$ for $n \geq 5$ and no such formulas exist!

Évariste Galois (1811–1832) was a French mathematician who devised some of these algebraic techniques

for the purposes of studying roots of polynomials and some related questions.

Galois Theory, named in his honor, reaches much further and allows mathematicians to study field extensions like K/F using group theory.

Next time: field extensions.