Announcement: midterm moving to evening (details TBD)

Today: Crash course in polynomial irreducibility

D&F Chapter 9

R: integral domain F: field of fractions of R

$R[x] \leftarrow$ poly rings $\rightarrow F[x]$

Reducible: equals product of two elts. that are not units.

Irreducible: no such factorization

e.g. $3x-6 = 3(x-6)$ is irred. over $\mathbb{Q}[x]$ since $3 = \left(\frac{1}{3}\right)^{-1}$ is a unit in $\mathbb{Q}[x]$, but red. over $\mathbb{Z}[x]$

To avoid this issue, keep our polys. monic

Unique factorization domain (UFD): integral domain R s.t. every $x \in R$ can be written as a product

$$x = p_1 \cdots p_n \qquad p_i\text{: irreds.}$$

and this prod. is <u>unique</u> up to units and rearrangement

<u>Facts:</u>

- Every Euclidean domain is a PID (Prop. 8.1)
- Every PID is a UFD (Thm. 8.14)
- A poly. ring over a field is a Euclidean domain (Thm. 9.3)

Gauss' Lemma: (Thm 5/Cor 6): R: UFD, F: field of fractions

$p(x) \in R[x]$ monic

$$p \text{ irred. in } R[x] \Leftrightarrow p \text{ irred. in } F[x]$$

Let $p(x) \in F[x]$

a) (Prop 9): p has a factor of deg 1 $\Leftrightarrow$ p has a root in F

b) (Prop 10): If deg $p = 2$ or 3,

p is reducible $\Leftrightarrow$ p has a root

Now set $R = \mathbb{Z}$, $F = \mathbb{Q}$

$p(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$

Three tools for proving irreducibitity over $\mathbb{Q}$

1) Rational Root Theorem (Prop 11)

If $\frac{r}{s} \in \mathbb{Q}$ is a root of p w/ $\gcd(r,s) = 1$,

then $r \mid a_0$ and $s \mid a_n$.

2) Reduction mod primes (Prop. 12)

Let $q \in \mathbb{Z}$ be prime. Let $\bar{p}(x)$ be the image of $p(x)$ under the map $\mathbb{Z} \longrightarrow \mathbb{Z}/(q) \cong \mathbb{F}_q$ $\quad x \longmapsto x$

$$a \longmapsto a \bmod q$$

Then if $\bar{p}(x)$ is irred over $\mathbb{F}_q$, and $\deg p = \deg \bar{p}$, then $p(x)$ is irred over $\mathbb{Q}$

e.g. a) x^2+x+1 is irred. over $\mathbb{F}_2$ since neither 0 nor 1 is a root.

Let $p(x) = ax^2+bx+c$ where a,b,c are all odd.

Then $\bar{p}(x) = x^2+x+1$ is irred over $\mathbb{F}_2$, so p is irred. / $\mathbb{Q}$.

b) $p(x) = x^4+5x^2-2x-3 \equiv (x^2+x+1)^2 \bmod 2$

$$\equiv x(x^3+2x+1) \bmod 3$$

So $p(x)$ is irred. since both factorizations are irred.

Note: Converse is not true

e.g. x^4+1 is reducible over every $\mathbb{F}_q$,

but irred. over $\mathbb{Q}$

3) Eisenstein's Criterion (Prop 13, Cor. 14):

Let $q \in \mathbb{Z}$ be prime. Suppose:

$$q \mid a_{n-1},\ q \mid a_{n-2}, \dots, q \mid a_0, \quad \text{but} \quad q \nmid a_n \text{ and } q^2 \nmid a_0$$

Then $p(x)$ is irred. $/\mathbb{Q}$.

e.g. a) $x^4 + 10x + 5$ is irred. $/\mathbb{Q}$ $\quad (q = 5)$

b) Let q be prime, and let

$$\Phi_q(x) = \frac{x^q - 1}{x - 1} = x^{q-1} + x^{q-2} + \dots + x + \underline{1} \quad \left(\begin{array}{c}\text{Cyclotomic} \\ \text{poly.}\end{array}\right)$$

Consider

$$p(x) := \Phi_q(x+1) = \frac{(x+1)^q - 1}{x} = x^{q-1} + q x^{q-2} + \dots + \frac{q(q-1)}{2} x + q$$

p is irred. $/\mathbb{Q}$ by Eis. crit. w/ prime q,

So Φ_q is irred. $/\mathbb{Q}$ as well.

Pf of Eisenstein's Criterion (if time): Suppose $p(x)$ is reducible: $p(x) = a(x)\,b(x)$. Reducing mod q gives

$$\bar{a}(x)\,\bar{b}(x) = \bar{p}(x) = a_n x^n.$$

In particular, $a_0 = b_0 = 0 \mod p$ since

$$p_0 = a_0 b_0 = 0 \mod p$$

$$p_1 = a_1 b_0 + a_0 b_1 = 0 \mod p$$

$$p_2 = a_2 b_0 + a_1 b_1 + a_0 b_2 = 0 \mod p$$

$$\vdots$$

$$p_{n-1} = a_{m-1} b_r + a_m b_{r-1} = 0 \mod p$$

$$p_n = a_m b_r \neq 0 \mod p$$

But then $a_0 b_0 = 0 \mod p^2$, a contradiction.