UFD properties of polynomial rings

Last time: Applied ED $\Rightarrow$ PID $\Rightarrow$ UFD to $\mathbb{Z}[i]$.

Q: Beyond PID and UFD?

E.g. $R = \mathbb{Z}[\sqrt{-5}]$, $N: R \to \mathbb{Z}_{\geq 0}$

$$N(x+y\sqrt{-5}) = x^2+5y^2$$

So no elements of R have norm $= 2, 3, 7, \cdots$

Consider $21 = 3 \times 7 = 1+20 = (1+2\sqrt{-5})(1-2\sqrt{-5})$ (*)

- Note: no elements have norm $3, 7 \Rightarrow 3, 7, 1\pm 2\sqrt{-5}$ are irreducible

So R is not a UFD $\Rightarrow$ not a PID.

Q: How to do arithmetic in such a ring?

Recall in $\mathbb{Z}$: $(a,b) = (\gcd(a,b))$

Imagine the reason for (*) is: $3 = a \cdot b$, $7 = c \cdot d$

$$1+2\sqrt{-5} = a \cdot c, \quad 1-2\sqrt{-5} = b \cdot d$$

So maybe $a =$ "$\gcd(3, 1+2\sqrt{-5})$"

Claim. As ideals in $\mathbb{Z}[\sqrt{-5}]$, we have

$$(3) = (3, 1+2\sqrt{-5})(3, 1-2\sqrt{-5}), \quad (7) = (7, 1+2\sqrt{-5})(7, 1-2\sqrt{-5}), \cdots$$

Check: $(3, 1+2\sqrt{-5})(3, 1-2\sqrt{-5}) = (9, 3+6\sqrt{-5}, 3-6\sqrt{-5}, 21) = (3)$

generate 3

Replacement of UFD properties:

$K = \mathbb{Q}(\alpha) \supseteq \mathcal{O}_K$ = "ring of integers" $\mathcal{O}_K$ is a Dedekind domain (戴德金整环)

| fin. ext'n | |

$\mathbb{Q} \supseteq \mathbb{Z}$

namely, every nonzero, proper ideal can be written as products of prime ideals, unique up to permutations.

So: can always factor as prime ideals but need to deal with nonprincipal ideals.

more on Number Theory series ....

Theorem. An integral domain R is a UFD if and only if $R[x]$ is a UFD.

Cor. R UFD $\Rightarrow R[x_1, \cdots, x_n]$ is a UFD (e.g. $R = \mathbb{Z}$, field, $\mathbb{Z}[i]$)

Proof: View $R \subseteq R[x]$ as the constant polynomials.

Step 0 A constant $a \in R$ is a unit in $R \iff$ unit in $R[x]$

irreducible in $R \iff$ irreducible in $R[x]$

b/c $a = bc \Rightarrow b$ & c are constants

From this, we see that $R[x]$ UFD $\Rightarrow R$ UFD

Next, assume R is UFD. Write $F = \mathrm{Frac}(R)$. Then $F[x]$ is ED $\Rightarrow$ PID $\Rightarrow$ UFD

Will relate polynomials of degree ≥ 1 to $F[x]$.

Step 1 (Gauss' Lemma) Let $p(x) \neq 0 \in R[x]$

If $p(x)$ is reducible in $F[x]$, then $p(x)$ is reducible in $R[x]$

i.e. if $p(x) = A(x)B(x)$ for $A(x), B(x) \in F[x]$ non-constant

then $\exists\, r \in F^\times$ s.t. $a(x) = rA(x)$ and $b(x) = r^{-1}B(x)$ are both in $R[x]$.

Proof: First take $d_1, d_2 \in R$ s.t. $d_1 d_2 p(x) = \underbrace{d_1 A(x)}_{\text{in } R[x]} \cdot \underbrace{d_2 B(x)}_{\text{in } R[x]}$

$\rightsquigarrow$ rewrite as $d \cdot p(x) = a_1(x) \cdot a_2(x)$

- If $d \in R^\times$, $p(x) = \left(d^{-1} a_1(x)\right) \cdot a_2(x)$.
- Otherwise, take a prime factor q of d,

then $R[x]/(q) = R/qR[x]$ is an integral domain

$$0 = \overline{d\,p(x)} = \overline{a_1(x)} \cdot \overline{b_1(x)}$$

So either $\overline{a_1(x)} = 0$ or $\overline{b_1(x)} = 0$

WLOG $\overline{a_1(x)} = 0 \Rightarrow$ all coeffs of $a_1(x)$ are divisible by q

So write $d = qd_2$, $a_2(x) = q^{-1}a_1(x) \in R[x]$. $b_2(x) = b_1(x)$

$\Rightarrow d_2\, p(x) = a_2(x)\, b_2(x)$. Continue this process. $\square$

Step 2. The irreducible elements in $R[x]$ are:

- constants $a \in R$ s.t. a is irreducible in R
- a polynomial $a(x) \in R[x]$ of deg ≥ 1

  s.t. ① gcd (coeffs of $a(x)$) $= 1$

  ② $a(x)$ is irreducible in $F[x]$

Pf: Step 0 $\Rightarrow$ case of deg $= 0$ polynomials

Now, $a(x) \in R[x]$ of deg ≥ 1

- If gcd (coeffs of $a(x)$) $= g$ is not a unit, $a(x) = g \cdot (g^{-1}a(x))$ not irreducible.
- If $a(x) = A(x)B(x)$ is reducible in $F[x] \xRightarrow{\text{Gauss Lemma}} a(x)$ is reducible in $R[x]$

Conversely, if $a(x)$ satisfies ① and ② and $a(x) = b(x)\,c(x)$ for $R[x]$

- If deg $b \geq 1$, deg $c \geq 1 \Rightarrow$ ② doesn't hold.
- So WLOG deg $b = 0$. But if $b \in R$ is not a unit, ① doesn't hold.

So b is a unit in R ✓ $\square$

Step 3 Existence of the factorization in $R[x]$

Given $a(x) \in R[x]$, if a is a constant $\rightsquigarrow$ reduce to the UFD property of R

Now, deg $a(x) \geq 1$. Let $d :=$ gcd (coeffs of $a(x)$) $=$ product of irreducibles

$\Rightarrow a(x) = d \cdot a_1(x)$ for some $a_1(x) \in R[x]$

Factor $a_1(x) = A_1(x) \cdots A_r(x)$ in $F[x]$

By Gauss' Lemma, may adjust so that each $A_i(x) \in R[x]$

Moreover, for each i, $\gcd(\text{coeffs of } A_i(x)) = 1$ o/w, $\gcd(\text{coeffs of } a_1(x)) \neq 1$

Thus, all $A_i(x)$ are irreducible elements

Step 4 Uniqueness of the factorization

Suppose $a(x) = p_1(x) \cdots p_m(x) = q_1(x) \cdots q_n(x)$

First view this in $F[x]$, each $p_i(x)$ with deg ≥ 1 corresponds to some $q_j(x)$

s.t. $p_i(x) = r \cdot q_j(x)$ for some $r = \frac{a}{b} \in F^\times$ with $\gcd(a,b) = 1$

So $b p_i(x) = a q_j(x)$. By Step 2 ① $\Rightarrow$ a, b are both units

So $p_i(x) = \text{unit} \cdot q_j(x)$

Removing all factors of degree ≥ 1, we are reduced to $a(x) \in R \subseteq R[x]$.

Use uniqueness of factorization in R. $\square$

Question: How to test whether a polynomial is irreducible or not?

① If F is a field, a polynomial $f \in F[x]$ of degree 2 or 3 is irreducible if and only if it does not have a root in F.

② (for $\mathbb{Z}$) If $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ is a polynomial s.t. $p\left(\frac{r}{s}\right) = 0$ for $r, s \in \mathbb{Z}$, $\gcd(r,s) = 1$

then $r \mid a_0$, $s \mid a_n$

Proof: $a_n \cdot \left(\frac{r}{s}\right)^n + a_{n-1}\left(\frac{r}{s}\right)^{n-1} + \cdots + a_0 = 0$

$a_n \cdot r^n + a_{n-1} r^{n-1} s + \cdots + a_0 s^n = 0$

$\Rightarrow \begin{cases} r \mid a_0 \cdot s^n & \text{so } r \mid a_0 \\ s \mid a_n \cdot r^n & \text{so } s \mid a_n. \end{cases}$ $\square$

Application. $f(x) = x^3 - x - 2 \in \mathbb{Z}[x]$ is irreducible. b/c $\pm 1, \pm 2$ are not zeros of $f(x)$.

③ (Eisenstein's criterion)

Let P be a prime ideal of an integral domain R. $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0 \in R[x]$.

Suppose that (1) $c_0, c_1, \cdots, c_{n-1} \in P$

(2) $c_0 \notin P^2$

Then $f(x)$ is irreducible.

Proof: May assume that $\deg f(x) \geq 2$

Suppose $f(x) = a(x) \cdot b(x)$ with $\deg(a) \geq 1$, $\deg(b) \geq 1$

Then the leading coefficients of $a(x)$ and $b(x)$ are units

Modulo $P \Rightarrow \bar{f}(x) = \bar{a}(x) \cdot \bar{b}(x)$ in $R/p[x]$

$\bar{f}(x) = x^n$

Claim: The constant term $\bar{a}_0$ and $\bar{b}_0$ are zero (In fact, can prove that $\bar{a}(x) = x^{\deg \bar{a}}$ and $\bar{b}(x) = x^{\deg \bar{b}}$)

If $\bar{a}_0 \neq 0$, take $\bar{b}_i$ = minimal term that is $\neq 0$

$\Rightarrow \bar{a}(x)\bar{b}(x)$ has the term $\bar{a}_0 \bar{b}_i x^i$. Contradiction! ✓

$\Rightarrow \bar{a}_0 = \bar{b}_0 = 0 \Rightarrow a_0, b_0 \in P \Rightarrow c_0 \in P^2$ Contradition. □

Typical application If p is a prime number, the cyclotomic polynomial

$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + 1$ is irreducible in $\mathbb{Z}[x]$

This is because $\Phi_p(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} = x^{p-1} + \underbrace{px^{p-2} + \binom{p}{2}x^{p-3} + \cdots + p}_{\text{div. by } p}$ ↖ not div by p^2

Proposition Let F be a field.

(1) A polynomial $f(x)$ is irreducible if and only if $F[x]/(f(x))$ is a field

$f(x)$ irreducible $\overset{F[x] \text{ UFD}}{\iff}$ $f(x)$ prime element $\iff$ $(f(x))$ prime ideal

$\Updownarrow$ $F[x]$ PID

$F[x]/(f(x))$ field $\iff$ $(f(x))$ maximal ideal

We will later use this to construct "field extensions" of F

E.g. x^3+2x-1 is irreducible in $\mathbb{F}_3[x]$ (why?)

Then $\mathbb{F}_3[x]/(x^3+2x-1) \cong \{a+bx+cx^2 \,;\, a,b,c \in \mathbb{F}_3\}$ is the field of 27 elements.

(2) If $f(x) = p_1(x)^{n_1} \cdots p_r(x)^{n_r}$ is the factorization of $f(x)$ in $F[x]$

then $F[x]/(f(x)) \cong F[x]/(p_1(x)^{n_1}) \times \cdots \times F[x]/(p_r(x)^{n_r})$

This follows from Chinese remainder theorem as $p_i^{n_i}$'s are all coprime $\Rightarrow$ comaximal

$(p_i(x)^{n_i}, p_j(x)^{n_j}) = (\gcd(p_i(x)^{n_i}, p_j(x)^{n_j})) = (1)$.

(3) If $f(x) \in F[x]$ has distinct zeros $\alpha_1, \cdots, \alpha_n$, then $f(x)$ is divisible by $(x-\alpha_1)\cdots(x-\alpha_n)$

In particular, a degree n polynomial can have at most n zeros.

Corollary If F is a field and G a finite subgroup of $F^\times$, then G is cyclic

Proof: Say $\#G = n$. By classification of finite abelian groups,

$$G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r} \quad \text{with } n_1 | n_2 | \cdots | n_r \ \& \ n = n_1 \cdots n_r$$

If G is not cyclic, all elements have order dividing $n_r < n$

i.e. $\forall g \in G,\ g^{n_r} = 1$

But then the polynomial $x^{n_r} - 1$ has n distinct zeros. A contradiction!

Optional: Structure of $(\mathbb{Z}/n\mathbb{Z})^\times$

Step 1: Say n factors as $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$

Then Chinese remainder theorem $\Rightarrow \mathbb{Z}/n\mathbb{Z} \simeq \left(\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}\right) \times \cdots \times \left(\mathbb{Z}/p_r^{\alpha_r}\mathbb{Z}\right)$ as rings

Taking units $\Rightarrow \left(\mathbb{Z}/n\mathbb{Z}\right)^\times = \left(\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}\right)^\times \times \cdots \times \left(\mathbb{Z}/p_r^{\alpha_r}\mathbb{Z}\right)^\times$

(counting gives the formula $\varphi(n) = \varphi(p_1^{\alpha_1}) \cdots \varphi(p_r^{\alpha_r})$)

Step 2 Fix a prime p, p odd $\Rightarrow \left(\mathbb{Z}/p^\alpha\mathbb{Z}\right)^\times$ is cyclic of order $p^{\alpha-1}(p-1)$

$p=2 \Rightarrow \left(\mathbb{Z}/2\mathbb{Z}\right)^\times = \{1\}$

$\alpha > 1 \quad \left(\mathbb{Z}/2^\alpha\mathbb{Z}\right)^\times = \{\pm 1\} \times \left(1+4\mathbb{Z}/2^\alpha\mathbb{Z}\right)^\times = Z_2 \times Z_{2^{\alpha-2}}$

For p odd, $\left(1+p\mathbb{Z}/p^\alpha\mathbb{Z}\right)^\times$ is Sylow p-subgroup

Claim: $\left(1+p\mathbb{Z}/p^\alpha\mathbb{Z}\right)^\times \xrightarrow{\sim} Z_{p^{\alpha-1}}$

$1+px \longmapsto$ "$\frac{1}{p}\log(1+px) = \frac{1}{p}\left(px - \frac{(px)^2}{2} + \frac{(px)^3}{3} - \cdots\right)$"

$\exp(py) = 1+py+\frac{(py)^2}{2!}+\cdots \longmapsfrom y$

One can check that this gives a mutually inverse isomorphism

* Consider $\left(\mathbb{Z}/p^\alpha\mathbb{Z}\right)^\times \xrightarrow[\varphi]{\text{mod } p} \left(\mathbb{Z}/p\mathbb{Z}\right)^\times \simeq Z_{p-1}$

$\ker\varphi \simeq Z_{p^{\alpha-1}}$

Write $\left(\mathbb{Z}/p^\alpha\mathbb{Z}\right)^\times = \ker\varphi \times \underbrace{G^{p}}_{\text{prime-to-}p\text{ part}} \xrightarrow{\varphi} Z_{p-1} \quad \Rightarrow \varphi|_{G^p} : G^p \xrightarrow{\sim} Z_{p-1}$

So $\left(\mathbb{Z}/p^\alpha\mathbb{Z}\right)^\times \cong \ker\varphi \times G^p \simeq Z_{p^{\alpha-1}} \times Z_{p-1} = Z_{(p-1)p^{\alpha-1}}$

When $p=2$, the only difference is that the Claim should be changed to

$$\left(1+4\mathbb{Z}/2^\alpha\mathbb{Z}, \cdot\right) \xrightarrow{\sim} \left(Z_{2^{\alpha-2}}, +\right)$$

$1+4x \longmapsto \frac{1}{4}\log(1+4x)$

$\exp(4y) = 1+4y+\frac{(4y)^2}{2}+\cdots \longmapsfrom y$

↑ need 4 instead of 2 to ensure "convergence".