Abstract Algebra (H) Lect. 15

1. Thm : A PID is a UFD.

Proof : Let D be a PID. In D, irr $\Rightarrow$ prime. (prime condition of UFD)

only need $\forall a$ not inv. $a = p_1 \cdots p_s$, p_i irr (chain condition of UFD)

Take $a \in D \setminus \{0\}$. not inv. Sps a is not a finite product of irr. (反证法)

Then $a = a_1 b_1$ s.t. a_1 not irr $\longrightarrow a_1 = a_2 b_2 \longrightarrow \cdots$

Hence $(a) < (a_1) < \cdots < (a_i) < \cdots$, Let $I = (a) \cup (a_1) \cdots \cup (a_i) \cup \cdots$, I is an ideal of D.

Since D is PID. $I = (b)$ $\therefore b \in (a_i)$, thus $I = (b) \leq (a_i) < (a_{i+1}) < I$ ↯

($a = a_1 b_1 \longrightarrow (a) < (a_1)$ 构造 I, 由PID $I = (b)$ 导出矛盾)

2. ED (Euclidean Domain)

Recall: $\mathbb{Z}[\sqrt{-5}]$ isn't a UFD, as $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$. not uniquely factorized.

How about $\mathbb{Z}[\sqrt{-1}]$? It's even an ED, Let alone UFD :P

Defn: D be ID. A map $v: D \setminus \{0\} \longrightarrow \mathbb{Z}^+$ is called a valuation if

$\forall x, y \in D$. with $y \neq 0$, $\exists\, q, r \in D$. s.t. $x = qy + r$, $r = 0$ or $v(r) < v(y)$, then ED.

ED 即可以做带余除法的环. 译文: can apply Euclidean algorithm in D

Ex. $\mathbb{Q}[x]$ is ED, valuation : degree.

$\mathbb{Z}$ is ED. valuation : absolute value.

Thm. An ED is a PID. (So UFD)

Proof. ("You don't need a proof actually, just observation" — prof. Li).

Let D be ED, I be an ideal.

Take $b \in I$ .st. $v(b)$ is the smallest. Then $I = (b)$

Let's do the observation:

Let $a \in I$, then $a, b \in I$, $\exists\, q, r \in D$. s.t. $a = qb + r$, $r = 0$ or $v(r) < v(b) \Rightarrow$ smallest

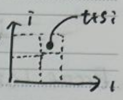
$\therefore r = 0$, $a = qb$. i.e. $a \in (b)$. $I = (b)$, thus D is a PID.

Claim : $J = \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$, $i = \sqrt{-1}$, J is ED.

Proof. Let $v(a+bi)=a^2+b^2$, we prove $v(\cdot)$ is a valuation.

Let $x,y\in D$ with $y\neq 0$, write $\frac{x}{y}=t+si$, $t,s\in\mathbb{Q}$

Let $q_1,q_2\in\mathbb{Z}$ be s.t. $|t-q_1|,|s-q_2|\leq\frac{1}{2}$ $\longrightarrow$ 在复平面上两个轴分别选靠近的点



Let $q=q_1+q_2 i$, we have $v(\frac{x}{y}-q)=v((t-q_1)+(s-q_2)i)=(t-q_1)^2+(s-q_2)^2\leq\frac{1}{2}$.

So $r:=x-qy$ is s.t. $v(r)=v(x-qy)=v(y(\frac{x}{y}-q))\leq v(y)v(\frac{x}{y}-q)\leq\frac{1}{2}v(y)<v(y)$

三角不等式

i.e. $x=qy+r$, $v(r)<v(y)$ thus $v(\cdot)$ a valuation. So J is ED.

3. Polynomial rings over UFD

Let R be a UFD, $f(x)\in R[x]$

Defn: ① The gcd of coefficients of $f(x)$ is called **capacity of f(x)**, denoted by $c(f)$.

② If $c(f)=1$, then $f(x)$ is **primitive**.

Lemma (Gauss) Let $f,g\in R[x]$, then $c(fg)=c(f)c(g)$. If f,g are primitive, then so is fg.

Proof. ("Have you proved this in high school?" — prof. Li)

Let $f(x)=a_0+a_1x+\cdots+a_nx^n$, $g(x)=b_0+b_1x+\cdots+b_mx^m$

$h(x)=f(x)g(x)=c_0+c_1x+\cdots+c_{m+n}x^{m+n}$

Then $c_{i+j}=a_ib_j+a_{i-1}b_{j+1}+\cdots+a_{i+1}b_{j-1}+\cdots$

Let p prime s.t. $c(f)_p=p^k$, $c(g)_p=p^l$, then $p^{k+l}\mid c(h)$, so $c(fg)\geq c(f)c(g)$.

(argument) Assume f,g prime. Sps $p\mid c(fg)$ (Let's prove it's impossible)

$\exists i,j$ s.t. • p divides $a_0,a_1,\cdots,a_{i-1}$, but $p\nmid a_i$

• p divides $b_0,b_1,\cdots,b_{j-1}$, but $p\nmid b_j$

Then $c_{i+j}=a_ib_j+a_{i-1}b_{j+1}+\cdots+a_{i+1}b_{j-1}+\cdots$, $p\nmid a_ib_j$ but divides all others.

so $p\nmid c_{i+j}$. ↯ so $c(fg)=c(f)c(g)$

we show if $c(f)=c(g)=1$, then $c(fg)=1$ in the upward discussion.

if $c(f)=a$, $c(g)=b$, $f=af'$, $g=bg'$. $c(fg)=c(abf'g')=ab\,c(f'g')=ab=c(f)\cdot c(g)$

number

Lemma. Let K be the fraction field of R. Then $f(x) \in R[x]$ irreducible iff $f(x)$ irr in $K[x]$.

Proof. Let $f(x)$ be irr in $R[x]$, Sps $f(x)$ reducible in $K[x]$, i.e. $f(x) = g(x)h(x)$, $g, h \in K[x]$

~~Then~~ $\exists r, s \in R$ s.t. $rg, sh \in R[x]$, so $rs f(x) = rg(x) \cdot sh(x)$ in $R[x]$

Let $a = c(rg(x))$, $b = c(sh(x))$. Then $rg(x) = a g_1(x)$, $sh(x) = b h_1(x)$. g_1, h_1 prim.

Thus $rs f(x) = rg(x) \cdot sh(x) = ab\, g_1(x) h_1(x)$

How can we get $f(x)$ primitive from irr. ?

in the prior stage, take r = lcm of coeffeient of g. s = lcm of coeffeient of h

$c(rs f(x)) = ab$, $f(x)$ primitive, thus $rs = uab$, u inv.

$f(x) = (u g_1(x)) h_1(x)$ in $R[x]$ ↯. so $f(x)$ irr in $K[x]$

Thought. $\mathbb{Z}[x] \xrightarrow[\text{trivial}]{} \mathbb{Q}[x] \longrightarrow \mathbb{R}[x]$

$\hookrightarrow x^2 - 2$ irr in $\mathbb{Q}[x]$. reducible in $\mathbb{R}[x]$

Thm. R is UFD, then $R[x]$ UFD.

Proof. Let $f \in R[x]$ of deg n. Then f is a product of finitely many polynomials.

Thus, we only need to prove irr $\equiv$ prime.

Sps f irr, and $f \mid gh$. Then $f(x) q(x) = g(x) h(x)$.

If $\deg f = 0$, then $f(x) = a \mid c(g) c(h)$. As R is UFD, $a \mid g(x)$ or $a \mid h(x)$, i.e.

$f(x) = a$ is a prime

("I've tried hard but we still can't finish it" — prof. Li).