答疑

1. 纠错：$\mathbb{Z}[\sqrt{-3}]$是不满足分解唯一性，不是一个UFD

课上说：$A=\{a+b\sqrt{-3}\mid a,b\text{同奇.同偶}\}$是UFD.

这个集合写法有误. 应该是

$$A=\left\{\frac{1}{2}(a+b\sqrt{-3})\,\middle|\,a,b\text{同奇偶}\right\}=\left\{x+y\cdot\frac{1+\sqrt{-3}}{2}\,\middle|\,x,y\in\mathbb{Z}\right\}$$

我们后面将展示它是欧氏环，因而是UFD.

2. 设R是一个整区，如下条件：

$\forall a\in R$，$a\neq 0$，a非单位，则a可以写成有限个不可约元

乘积

$\Updownarrow$

设$(a_1)\subseteq(a_2)\subseteq\cdots\subseteq(a_k)\subseteq\cdots$是一个升链，$a_1,\cdots,a_k,\cdots\in R$

则$\exists n\in\mathbb{N}$，$(a_n)=(a_{n+1})=\cdots$ 这称为主理想升链条件

(ACCP)

因为若$a=a_1a_1'$，则$(a)\subseteq(a_1)$　$a_1=a_2a_2'$，则$(a_1)\subseteq(a_2)$

…

有些整区不满足这个条件，例 $\mathbb{Z}+x\mathbb{Q}[x]=\{f(x)\mid f(x)\in\mathbb{Q}[x]$，$f(x)$的常数项为整数$\}$　$(x)\subset(\frac{x}{2})$ 但 $(\frac{x}{2})\not\subseteq(x)$

有 $(x) \subset (\frac{x}{2}) \subset (\frac{x}{4}) \subset \cdots$

$$x = 2\cdot\frac{x}{2} = 2\cdot 2\cdot\frac{x}{4} = 2\cdot 2\cdot 2\cdot\frac{x}{8} = \cdots$$

3. 有同学问：在UFD讨论中只涉及乘法和消去律，能否直接在幺半群（含消去律）上讨论唯一分解性. 这是可以的.

即设 M 是一个幺半群有消去律，则 M 是一个唯一分解半群 $\Leftrightarrow$ $\forall x\in M$, $x\neq 0$, x 不可逆, $x = a_1a_2\cdots a_r = b_1\cdots b_s$, 则存在分解 $a_1 = c_1\cdots c_i$, $a_2 = c_{i+1}\cdots c_j$, $\cdots$, $b_1 = d_1\cdots d_k$, $b_2 = d_{k+1}\cdots d_p$, $\cdots$, 使得 $c_n = d_n \ \forall n$.

一个整区 R 是唯一分解整环 $\Leftrightarrow$ $R^* = R\setminus\{0\}$ 是唯一分解半群.

Ref. R.E. Johnson, Proceedings of the American Math. Society Vol.28, No.2. Page 397–404.

4. 有同学问：$\dfrac{\mathbb{Q}[x,y]}{(x^2+y^2-1)}$ 是否UFD？

我不太确定这个环
否UFD，这里x可能
是不可约的，哪位
学能给出肯定或否
的答案？大家忽略
个解答-4.

它不是UFD，因为 $\bar{x}^2 = (\overline{1-y})(\overline{1+y})$

但是 $\dfrac{\mathbb{C}[x,y]}{(x^2+y^2-1)}$ 是UFD.

因为令 ~~x~~ $u=x+iy$，$v=x-iy$.

$$\frac{\mathbb{C}[x,y]}{(x^2+y^2-1)}=\frac{\mathbb{C}[u,v]}{(uv-1)}=\mathbb{C}[u,\tfrac{1}{u}]$$ 这是 $\mathbb{C}[u]$ 的

局部化（在 $u=0$），也是UFD.

一般地，多项式环的商环的唯一分解性可能依赖于域是否代数闭域，很难判断是否UFD.

5. 最大公因子和最小公倍式

设 R 整区，$a,b\in R$

$\forall r\neq 0\in R$，$g.c.d(ra,rb)$ 存在

$l.c.m(a,b)$ 存在 $\Longleftrightarrow$

证明："$\Rightarrow$" 设 $lcm(a,b)=m$，$a|ab$，$b|ab \Rightarrow m|ab$，令 $ab=mx$

$x=\dfrac{ab}{m}$　$a=x\cdot\dfrac{m}{b}$　$b=x\cdot\dfrac{m}{a}\Rightarrow x|a,\ x|b$

~~$\Rightarrow x|gcd$~~ $\forall e\in R$ 且 $e|a$，$e|b$ 则 $eb|ab$，$ea|ab$，

$lcm(ea,eb)=e\cdot lcm(a,b)\Rightarrow em|ab\Rightarrow e|x$ 因此

$x=gcd(a,b)$ 反之"$\Leftarrow$" 设 $gcd(a,b)=d$，$d|a$，$d|b\Rightarrow$

$rd|ra,rb\Rightarrow rd|gcd(ra,rb)$　$\forall s\in R$，$s|ra$，$s|rb$ 则 $sb|rab$

$sa|rab$，~~lcm~~ $lcm(a,b)=\dfrac{ab}{gcd(a,b)}$（省略一些细节）