19.

PID and UFD

Fix a commutative integral domain R.

Def: $a \in R$ is irreducible if $a = bc \Rightarrow b \in R^*$ or $c \in R^*$ but not both.

$\langle a \rangle = \langle c \rangle$ or $\langle a \rangle = \langle b \rangle$

Lemma: $\langle p \rangle$ prime $\Rightarrow$ p irreducible.

Pf: $p = ab \Rightarrow a \in \langle p \rangle$ or $b \in \langle p \rangle$; say $a \in \langle p \rangle$.

Then $a = pc$, so $\underbrace{p = ab = pcb}$

$\Rightarrow cb = 1$ since R is entire. $\square$

Def: $a \mid b$ if $ac = b$ for some $c \in R$.

$b \in \langle a \rangle$

$d \in R \setminus \{0\}$ is a gcd of a and b if

- $d \mid a$ and $d \mid b$
- $c \mid a$ and $c \mid b \Rightarrow c \mid d$.

Def: R (a commutative integral domain) is a PID (principal ideal domain) if every ideal is principal.

Prop: In a PID, $\langle a, b \rangle = \langle d \rangle \Rightarrow d$ is a gcd of a and b.

Pf: Let $d = \alpha a + \beta b$ and suppose $a = ex$ and $b = ey$.

Then $d = \alpha e x + \beta e y$

$= e(\alpha x + \beta y) \Rightarrow e \mid d$.

But $d \mid a$ and $d \mid b$ because $a, b \in \langle d \rangle$. $\square$

Cor: $\langle p \rangle$ prime $\Leftarrow$ p irreducible if R is a PID.

Pf: $p \mid ab$ and $p \nmid a \Rightarrow \langle p, a \rangle = \langle d \rangle \supsetneq \langle p \rangle$

$\Rightarrow p = cd$ but $c \notin R^*$

$\Rightarrow d \in R^*$ since p is irreducible may as well take $d = 1$

$\Rightarrow 1 = xp + ya$

$\Rightarrow b = \underbrace{xpb}_{p \mid} + \underbrace{yab}_{p \mid}$

$\Rightarrow p \mid b$. $\square$

<u>Def</u>: R (a commutative integral domain) is <u>factorial</u> (or a <u>UFD</u>) unique factorization domain

if every $r \in R\setminus\{0\}$ <u>factors uniquely</u> into irreducible elements:

$$r = up_1\cdots p_k \quad \text{with } u \in R^* \text{ and}$$

$$r = vq_1\cdots q_\ell \quad \text{with } v \in R^* \Rightarrow k = \ell \text{ and } q_i = u_i p_i \text{ for some } u_i \in R^* \text{ after permuting the } q_i.$$

<u>Thm</u>: PID $\Rightarrow$ UFD.

<u>Pf</u>: <u>Claim</u>: Every $r \in R$ factors into irreducibles. no uniqueness yet

<u>Pf</u>: Let $S = \{\langle r\rangle \subseteq R \mid r \text{ doesn't factor into irreducibles}\}$.

Assume $S \neq \varnothing$. Then S has a maximal element $\langle r\rangle$ because

- every chain $\langle r_1\rangle \subseteq \langle r_2\rangle \subseteq \cdots$ yields an ideal $\langle b\rangle = \langle r_1\rangle \cup \langle r_2\rangle \cup \cdots$
- $b \in \langle r_n\rangle$ for some $n \Rightarrow \langle b\rangle \subseteq \langle r_n\rangle \subseteq \langle b\rangle$

$\Rightarrow \langle b\rangle = \langle r_n\rangle \in S$ is an upper bound.

Note: r is reducible since $r \in S$, so $r = cd$ with $c, d \notin R^*$.

But then $\langle r\rangle \subsetneq \langle c\rangle$ and $\langle r\rangle \subsetneq \langle c\rangle$, so

c and d have factorizations. Hence r does, too. $\divideontimes$

Thus $S = \varnothing$. $\square$

$$r = up_1\cdots p_k = vq_1\cdots q_\ell \Rightarrow p_k \text{ prime by Cor}$$
$$\Rightarrow p_k \mid q_i \text{ for some } i\text{; assume } i = \ell \text{ by permutation}$$
$$\Rightarrow p_k = u_k q_\ell \text{ with } u_k \in R^* \text{ since } q_\ell \text{ is irreducible}$$
$$\Rightarrow up_1\cdots p_{k-1} = vu_k q_1\cdots q_{\ell-1} \text{ because } R \text{ is entire.}$$

Done by induction. $\square$

<u>E.g.</u>
- $R = \mathbb{Z}$
- $R = \Bbbk[x]$

PID by Euclidean algorithm next week

- Thm: R factorial $\Rightarrow$ $R[x]$ is, too $\Rightarrow$ $\mathbb{Z}[x_1,\dots,x_n]$, $\Bbbk[x_1,\dots,x_n]$ UFD
- $\Bbbk[[x]]$ formal power series is UFD; one variable $\Rightarrow$ PID
- $\Bbbk[x^2, x^3]$ <u>not</u> UFD
- $\mathbb{Z}[\sqrt{-5}]$ <u>not</u> UFD