HW #13 posted

11/28/2

Last time:

- An integral domain R is a PID (principal ideal domain) if every ideal $I \subset R$ is principal: $\exists\, a \in R$ so that $I = \langle a \rangle$.

Ex $\mathbb{Z}$, $F[x]$ (F a field) are PID's.

Definition In an integral domain R two elements $a, b \in R$ are associates $\Leftrightarrow \exists$ a unit $u \in R$ so that $a = ub$
$\Leftrightarrow \exists$ a unit $v \in R$ so that $b = va$

Ex In $\mathbb{Z}$, n, m are associates $\Leftrightarrow n = \pm m \Leftrightarrow (n \mid m$ and $m \mid n$
This is because the units in $\mathbb{Z}$ are ± 1.

Remarks: $a, b \in R$ are associates $\Leftrightarrow \langle a \rangle = \langle b \rangle$ (prove that

Recall In an integral domain R, $0 \neq a \in R$ is irreducible if the only factorizations of a are "trivial":
$a = bc \Rightarrow$ b is a unit or c is a unit

Ex $x^2+1 \in \mathbb{R}[x]$ is irreducible. It has lots of trivial factorization: $x^2+1 = \sqrt{2}\left(\frac{1}{\sqrt{2}}(x^2+1)\right) = \frac{1}{\pi}\left(\pi(x^2+1)\right) = \cdots$

Note In our proof that $x^2+1 \in \mathbb{R}[x]$ is irreducible in $\mathbb{R}[x]$ we actually showed:
For any field F, for any $p(x) \in F[x]$ with $\deg p = 2$
p is irreducible $\Leftrightarrow$ p has no roots in F.

Ex (Abbreviate $[0], [1]$ in $\mathbb{Z}_2$ as 0 and 1, resp.)

Consider $p(x) = x^2 + x + 1$ $\quad p(0) = 0^2 + 0 + 1 = 1 \neq 0$

$p(1) = 1^2 + 1 + 1 = 1 \neq 0$

$\Rightarrow$ $p(x)$ is irreducible

$\rightarrow$ $F = \mathbb{Z}_2[x] / \langle x^2 + x + 1 \rangle$ is a field.

Claim F is a field with 4 elements.

Reason 1) we have a homomorphism $\varphi : \mathbb{Z}_2 \to F$, $\varphi(a) = a + \langle x^2 + x + 1 \rangle$

Note: $1 \notin \langle x^2 + x + 1 \rangle$ since $\deg 1 = 0$

and $\forall f(x) \in \langle x^2 + x + 1 \rangle$, $\deg f \geq 2$.

$\Rightarrow \varphi(1) \neq 0_{\mathbb{Z}_2} + \langle x^2 + x + 1 \rangle = 0_F$. $\Rightarrow \varphi$ is injective

Now write 0 for $\langle x^2 + x + 1 \rangle$, 1 for $1 + \langle x^2 + x + 1 \rangle$

and $\alpha = x + \langle x^2 + x + 1 \rangle$.

Note $\forall p(x) \in \mathbb{Z}_2[x]$, $\exists!\ q(x), r(x) \in \mathbb{Z}_2[x]$ s.t.

$p(x) = q(x) \cdot (x^2 + x + 1) + r(x)$ and $\deg r < 2$.

$\Rightarrow p(x) = q(x) \cdot (x^2 + x + 1) + a_0 + a_1 x$ for some $a_0, a_1 \in \mathbb{Z}_2$

$\Rightarrow p(x) + \langle x^2 + x + 1 \rangle = a_0 + a_1 x + \langle x^2 + x + 1 \rangle$

$= a_0 + a_1 \cdot (x + \langle x^2 + x + 1 \rangle)$

$= a_0 + a_1 \alpha$

$\Rightarrow F = \{ a_0 + a_1 \alpha \mid a_0, a_1 \in \mathbb{Z}_2 \}$

$= \{ 0, 1, \alpha, 1 + \alpha \}$. and $\alpha + \alpha = 0$ since $\alpha + x = (1+1)x = 0 \cdot x = 0$ in $\mathbb{Z}_2[x]$

Multiplication? ...

$1 + \alpha + \alpha^2 = 1 + (x + \langle x^2 + x + 1 \rangle) + (x + \langle x^2 + x + 1 \rangle)^2$

$= (1 + x + x^2) + \langle x^2 + x + 1 \rangle = 0_F$

$\Rightarrow \alpha^2 = 1 + \alpha$ (remember: $1 = -1$ in $\mathbb{Z}_2$)

$\cdot$	α	$\alpha+1$
α	$1+\alpha$	1
$\alpha+1$	1	α

$\alpha \cdot (\alpha + 1) = \alpha^2 + \alpha = \alpha^2 + \alpha + 1 + 1$

$= 1$

$(\alpha + 1)(\alpha + 1) = \alpha^2 + \alpha + \alpha + 1 = \alpha$

Remark We'll show later: for any field F, for any $p(x) \in F[x]$ with $\deg p = n \geq 1$

$F[x]/\langle p \rangle$ is a vector space over F with a basis $\{1+\langle p\rangle, x+\langle p\rangle, \ldots x^{n-1}+\langle p\rangle\}$

Recall that we proved last time:

If R is an integral domain, $0 \neq p \in R$ Then

(1) $\langle p\rangle$ is maximal $\Rightarrow \langle p\rangle$ is prime $\Rightarrow p$ is prime $\Rightarrow p$ is irreduci

(2) If R is a PID, then

p irreducible $\Rightarrow \langle p\rangle$ is maximal

Hence in a PID irreducibles are primes.

There are integral domains where irreducibles are not prim

Example Consider $\mathbb{Z}[\sqrt{-5}] := \{a+b\sqrt{-5} \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$

$= \{a+ib\sqrt{5} \mid a, b \in \mathbb{Z}\}$

It's a subring of the field $\mathbb{C}$, hence is an integral domain. Also

$(1+\sqrt{-5})(1-\sqrt{-5}) = 1^2 - (\sqrt{-5})^2 = 1-(-5) = 6 = 2\cdot 3$

We will show: (i) $1 \pm \sqrt{-5}$, 2, 3 are irreducibles in $\mathbb{Z}[\sqrt{-5}]$

(ii) $2 \nmid (1 \pm \sqrt{-5})$.

(i) & (ii) $\Rightarrow$ 2 is irreducible and 2 is not prime

Now the details: Consider

$$N: \mathbb{Z}[\sqrt{-5}] \longrightarrow \mathbb{Z}$$

$$N(\alpha) = \alpha\bar{\alpha} = |\alpha|^2$$

[That is $N(a+b\sqrt{-5}) = (a+ib\sqrt{5})\overline{(a+ib\sqrt{5})}$

$= (a+ib\sqrt{5})(a-ib\sqrt{5}) = a^2+(b\sqrt{5})^2 = a^2+5$

Note: For any $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$,

$$\boxed{N(\alpha\beta) = \alpha\beta\,\overline{\alpha\beta} = \alpha\beta\,\bar{\alpha}\bar{\beta} = \alpha\bar{\alpha}\,\beta\bar{\beta} = N(\alpha)N(\beta)}$$

Since $N(a+b\sqrt{5}) = a^2+5b^2$,

The smallest values of N are $0 = N(0)$, $1 = N(\pm 1)$, $4 = N(\pm 2)$

$6 = N(\pm 1 \pm \sqrt{-5})$, $9 = N(\pm 3)$.

If $u, v \in \mathbb{Z}[\sqrt{-5}]$ are units with $1 = uv$, then $1 = N(1) = N(u)N(v)$

$\Rightarrow N(u) = N(v) = 1 \Rightarrow u, v = \pm 1$

If $2 = \alpha\beta$ for some $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$, then $4 = N(2) = N(\alpha)N(\beta)$

There is no $\alpha \in \mathbb{Z}[\sqrt{-5}]$ s.t. $N(\alpha) = 2$. $\Rightarrow N(\alpha)$ or $N(\beta)$ are 1

$\Rightarrow \alpha$ or β are units. $\therefore$ 2 is irreducible in $\mathbb{Z}[\sqrt{-5}]$.

If $2 \mid (1 \pm \sqrt{-5})$, $1 \pm \sqrt{-5} = 2\alpha_\pm$ for some $\alpha_\pm \in \mathbb{Z}[\sqrt{-5}]$

$\Rightarrow \quad 6 = N(1 \pm \sqrt{-5}) = N(2)N(\alpha_\pm) = 4\,\underbrace{N(\alpha_\pm)}_{\text{pos. integer}}$.

This is impossible, since $4 \nmid 6$.

$\Rightarrow 2 \nmid 1 \pm \sqrt{-5}$.

$\therefore$ $2 \in \mathbb{Z}[\sqrt{-5}]$ is an irreducible which is not a prime

($\Rightarrow$ $\mathbb{Z}[\sqrt{-5}]$ is not a PID).

Definition An integral domain R is a unique factorization domain (a UFD) iff

1) every $r \in R$ ($r \neq 0$, r not a unit) is a product of irreducibles

2) if $u p_1 \cdots p_m = v q_1 \cdots q_n$

(u, v units, $p_1 \cdots p_m$, $q_1 \cdots q_n$ irreducibles) then $n = m$ and $\forall i \in 1, \ldots, n$ $\exists \sigma \in S_n$ s.t. p_i and $q_{\sigma(i)}$ are associates.

Note $\mathbb{Z}[\sqrt{-5}]$ is not a UFD. $\mathbb{Z}$ is a UFD.