10/30/2022
Mon

Last time
- Defined PIDs, irreducibles and primes
- Defined Euclidean domains
- Proved that $\mathbb{Z}[i] = \{a+ib \mid a,b \in \mathbb{Z}\}$ is a Euclidean domain
- Proved that Euclidean domains are PID's.
- Proved that in an integral domain primes are irreducible.

Lemma 28.1 In $\mathbb{Z}[\sqrt{-5}] = \{a + \sqrt{5}ib \in \mathbb{C} \mid a,b \in \mathbb{Z}\}$, 2 is irreducible but not prime (note $\mathbb{Z}[\sqrt{-5}] \subseteq \mathbb{C}$, hence an integral domain).

Proof Consider $N: \mathbb{Z}[\sqrt{-5}] \to \mathbb{N}$, $N(a+\sqrt{-5}b) = |a+\sqrt{-5}b| = a^2+5b^2$.
Then $\forall\, u,v \in \mathbb{Z}[\sqrt{-5}]$, $N(uv) = |uv|^2 = |u|^2|v|^2 = N(u)N(v)$.

Observe also:
1) $N(a+\sqrt{-5}b) = 0 \Leftrightarrow a^2+5b^2 = 0 \Leftrightarrow a=0, b=0$, ie $a+\sqrt{-5}b = 0$.
2) $N(a+\sqrt{-5}b) = 1 \Leftrightarrow a^2+5b^2 = 1 \Leftrightarrow a = \pm 1$ and $b=0$

Hence: u,v are units in $\mathbb{Z}[\sqrt{-5}] \Leftrightarrow uv = 1$
$\Leftrightarrow N(u)\cdot N(v) = N(1) = 1$
$\Leftrightarrow N(u) = N(v) = 1$
$\Leftrightarrow u = \pm 1,\ v = \pm 1$

In other words $(\mathbb{Z}[\sqrt{-5}])^\times = \{\pm 1\}$.

Observation: The smallest values of N are $0 = N(0)$, $1 = N(\pm 1)$, $4 = N(2)$ and $5 = N(\pm\sqrt{-5})$.

Now suppose $2 = \alpha\beta$ for some $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$. Then
$$4 = N(2) = N(\alpha\beta) = N(\alpha)N(\beta)$$
$\therefore\ a^2 + 5b^2 = 2$ has no integer solutions.
Hence either $N(\alpha) = 4$ and $N(\beta) = 1$ or $N(\alpha) = 1$, & $N(\beta) = 4$.
If $N(\beta) = 1$, β is a unit. If $N(\alpha) = 1$, α is a unit.
$\therefore$ 2 is irreducible in $\mathbb{Z}[\sqrt{-5}]$

We now argue that 2 is <u>not</u> prime in $\mathbb{Z}[\sqrt{-5}]$:
$$2\cdot 3 = 6 = 1+5 = (1+\sqrt{-5})(1-\sqrt{-5})$$
If 2 is prime, 2 has to divide either $1+\sqrt{-5}$ or $1-\sqrt{-5}$.

If $2 \mid 1+\sqrt{-5}$, $\exists q \in \mathbb{Z}[\sqrt{-5}]$ s.t. $2q = 1+\sqrt{-5}$

But then $6 = N(1+\sqrt{-5}) = N(2q) = N(2)N(q) = 4N(q)$

This is impossible since in $\mathbb{Z}$, $4 \nmid 6$.

Similarly $2 \nmid 1-\sqrt{-5}$.

$\therefore$ 2 is not prime in $\mathbb{Z}[\sqrt{-5}]$.

Lemma 28.2 Let R be a PID, $x \in R$ irreducible. Then $\langle x \rangle$ is maximal (hence $\langle x \rangle$ is prime, hence x is prime)

Proof Suppose I is an ideal in R with $\langle x \rangle \subseteq I \subseteq R$.

Since R is a PID, $I = \langle c \rangle$ for some $c \in R$.

Recall: $\langle x \rangle \subseteq \langle c \rangle \Rightarrow x = qc$ for some $q \in R$ $(\langle x \rangle \subseteq \langle c \rangle \Rightarrow x \in \langle c \rangle)$

Since x is irreducible, q is a unit or c is a unit.

If q is a unit, $c = q^{-1}x \Rightarrow c \in \langle x \rangle \Rightarrow \langle c \rangle \subseteq \langle x \rangle$, hence $\langle x \rangle = \langle c \rangle$

If c is a unit $\langle c \rangle = R$.

$\therefore$ $\langle x \rangle$ is maximal and we are done. $\square$

Remarks

1) In a PID, the ~~set of~~ all irreducibles = the set of all (nonzero!) primes.

2) If R is a PID and x is irreducible then $R/\langle x \rangle$ is a field.

2a) For example in $\mathbb{Z}$ any prime $p \neq 0$ is irreducible $\Rightarrow \mathbb{Z}/p\mathbb{Z}$ is a field

2b) Consider $x^2+1 \in \mathbb{R}[x]$. If x^2+1 is not irreducible,

$x^2+1 = p(x)q(x)$ with $\deg p = \deg q = 1$

$p(x) = a_0 + a_1 x$ for some $a_0, a_1 \in \mathbb{R}$

$\alpha = -a_0/a_1$ is a root of $p(x)$

$\Rightarrow$ x^2+1 has a root in $\mathbb{R}$, which is impossible since $\forall \alpha \in \mathbb{R}$, $\alpha^2 \geq 0$, hence $\alpha^2+1 > 0$.

$\Rightarrow$ x^2+1 is irreducible and $\mathbb{R}[x]/\langle x^2+1 \rangle$ is a field.

3) In $\mathbb{Z}[\sqrt{-5}]$ 2 is irreducible and not prime.
$\Rightarrow$ $\mathbb{Z}[\sqrt{-5}]$ is not a PID.

Definition Let R be a commutative ring. $x, y \in R$ are associates if $\exists$ a unit $u \in R$ s.t. $x = uy$ (and $y = u^{-1}x$)

Ex $n, m \in \mathbb{Z}$ are associates $\Leftrightarrow$ $x = \pm 1$.
$p(x), q(x) \in \mathbb{R}[x]$ are associate $\Leftrightarrow$ $\exists \lambda \in \mathbb{R}, \lambda \neq 0$ s.t. $p(x) = \lambda q(x)$.

Lemma 28.3 Let R be an integral domain, $x, y \in R$, $x, y \neq 0$. Then
$x | y$ and $y | x$ $\Leftrightarrow$ x & y are associates ($\Leftrightarrow$ $\langle x \rangle = \langle y \rangle$)

Proof ($\Leftarrow$) easy.
($\Rightarrow$) Suppose $x | y$ and $y | x$. Then $\exists u, v \in R$ s.t. $y = ux$, $x = vy$
$\Rightarrow$ $x = v(ux)$. Since R is an integral domain, $1 = uv$
$\Rightarrow$ u, v are units $\square$

Definition An integral domain is a Unique Factorization Domain (UFD) iff
1) Every $r \in R$, $r \neq 0$, $r \neq$ unit is a product of irreducibles
2) If $u p_1 \cdots p_m = v q_1 \cdots q_n$, u, v units, $p_1 \cdots p_m$, $q_1 \cdots q_n$ irreducible Then $n = m$ and $\exists \sigma \in S_n$ st p_i and $q_{\sigma(i)}$ are associates

Ex $\mathbb{Z}$ is a UFD. $\mathbb{Z}[\sqrt{-5}]$ is not a UFD since
$$2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$$
and $2, 3, 1 \pm \sqrt{5}$ are all irreducibles

We proved: Euclidean domains $\subseteq$ PID's.
We'll prove: PID's $\subseteq$ UFDs
It turns out
$$\text{Euclidean domains} \subsetneq \text{PID's} \subsetneq \text{UFD's}.$$

To prove that PID's are UFD's we need

Definition A collection of ideals $\{I_j\}_{j=1}^{\infty}$ in a ring R is an *ascending chain* if $I_j \subseteq I_{j+1}$ for all j.

Ex $R = \mathcal{F}(\mathbb{R},\mathbb{R}) = \mathbb{R}^{\mathbb{R}}$, the set of all functions from $\mathbb{R}$ to $\mathbb{R}$.

Recall $\forall Y \subseteq \mathbb{R}$, $I_Y = \{ f \in \mathcal{F}(\mathbb{R},\mathbb{R}) \mid f|_Y = 0 \}$ is an ideal.

Note: if $Y_1 \subseteq Y_2$ and $f|_{Y_2} = 0$ then $f|_{Y_1} = 0$

$\Rightarrow$ $I_{Y_1} \supseteq I_{Y_2}$.

So let $Y_n = [0, 1/n]$, $I_n := I_{[0,1/n]}$

Then $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots \subseteq I_n \subseteq \dots$ is an ascending chain of ideals. <stopped here>.

Lemma 28.4 Let $\{I_j\}_{j=1}^{\infty}$ be an ascending chain of ideals in a ring R. Then $J = \bigcup_{j=1}^{\infty} I_j$ is an ideal in R.

Proof 1) Since each $I_j \neq \emptyset$, $J \neq 0$.

2) If $a, b \in J$ then $\exists\, i_1, i_2$ st $a \in I_{i_1}$, $b \in I_{i_2}$. May assume $i_1 \leq i_2$.
Then $a \in I_{i_1} \subseteq I_{i_2}$ $\Rightarrow$ $a - b \in I_{i_2} \subseteq \bigcup I_j = J$.

3) $\forall r \in R$ $\forall x \in J$ $\exists j$ st $x \in I_j$. Since I_j is an ideal
$rx, xr \in I_j$ $\Rightarrow$ $rx, xr \in \bigcup I_j = J$.

Theorem 28.5 Let R be a PID and $\{I_j\}_{j=1}^{\infty}$ an ascending chain.
Then $\exists\, m \in \mathbb{N}$ st $I_m = I_{m+1} = \dots = I_{m+j} = \dots$
and $\bigcup_{k=1}^{\infty} I_k = I_m$.

<Proof next time.>