Last hw posted

12/05/2018
We

36.1

Last time Defined the characteristic of a ring.
Proved that for an integral domain R, $\operatorname{char} R = 0$ or a prime.
Proved that if E is a finite field, then $|E| = (\operatorname{char} E)^n$ for some $n \in \mathbb{N}$.
Proved if $f \in F[x]$ is irreducible (and F is a field) then
$F \subseteq E := F[x]/\langle f \rangle$ and f has a root in E.

One thing we should have done awhile back: if F is a field then any $f \in F[x]$ is a product of irreducibles and that the factorization into irreducibles is unique (up to order and multiplication by units).

Definition An integral domain R is a unique factorization domain (a UFD) iff (i) $\forall r \in R$, $r \neq 0$, r not a unit is a product of irreducibles

(ii) if $u p_1 \cdots p_m = v q_1 \cdots q_n$ where u, v are units, p_i's, q_i's irreducible, then $n = m$ and $\exists\, \sigma \in S_n$ s.t. p_i and $q_{\sigma(i)}$ are associates (i.e. $p_i = \text{unit} \cdot q_{\sigma(i)}$)

Ex $R = \mathbb{Z}$ is a UFD.

Goal We'll prove: any PID is a UFD

Corollary Since for any field F, $F[x]$ is a PID
$F[x]$ is a UFD.

Note $\mathbb{Z}[\sqrt{-5}]$ is not a UFD:
$$2 \cdot 3 = 6 = (1+\sqrt{-5})\cdot(1-\sqrt{-5})$$

Definition Let R be a commutative ring. A collection of ideals is an <u>ascending chain</u> if $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \subseteq I_n \subseteq I_{n+1} \subseteq \cdots$

$R = \mathbb{Z}$

<u>Ex</u> $\underline{\langle 52\rangle \subseteq \langle 26 \rangle \subseteq \langle 13\rangle} \subseteq \langle 13\rangle \subseteq \cdots$

ie $I_1 = \langle 52\rangle$, $I_2 = \langle 26\rangle$, $I_3 = \langle 13\rangle$, $I_4 = \langle 13\rangle$, ... $I_k = \langle 13\rangle$ for $\forall k \geq$

is an ascending chain of ideals.

<u>Ex</u> Let R = functions from $\mathbb{R}$ to $\mathbb{R}$.

For any $X \subseteq \mathbb{R}$ $I_X = \{ f : \mathbb{R} \to \mathbb{R} \mid f(x) = 0 \ \forall x \in X\}$

is an ideal in R: $f, h \in I_X$, $x \in X \Rightarrow (f-h)(x) = f(x) - h(x) = 0$

$\forall g \in \mathbb{R} \to \mathbb{R}$, $\forall f \in I_X$ $(gf)(x) = g(x) \cdot f(x) = g(x) \cdot 0 = 0$.

Let $I_n = I_{[0, 1/n]} = \{ f : \mathbb{R} \to \mathbb{R} \mid f(x) = 0 \ \forall x \in [0, 1/n]\}$

Then $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \subseteq I_n \subseteq \cdots$

is an ascending of ideals.

<u>Lemma 36.1</u> Let R be a PID, $\{I_n\}_{n=1}^{\infty}$ an ascending chain of ideals: $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$

Then $\exists m \in \mathbb{N}$ s.t. $I_m = I_{m+1} = I_{m+2} \cdots = I_{m+k} = \cdots$ $\forall k \in \mathbb{N}$. (One says: "the chain stabilizes")

<u>Proof</u>

Consider $J = \bigcup_{i=1}^{\infty} I_i$. J is an ideal:

$\forall a, b \in J$, $\exists n, m \in \mathbb{N}$ s.t. $a \in I_n$, $b \in I_m$.

May assume $m \geq n$. Then $I_n \subseteq I_m \Rightarrow a \in I_m$.

Since I_m is an ideal, $a - b \in I_m \subseteq \bigcup I_i = J$.

Also, $\forall r \in R$, $ra \in I_m \subseteq \bigcup I_i = J$.

$\therefore$ J is an ideal.

Since R is a PID, $J = \langle \alpha \rangle$ for some $\alpha \in R$.

Since $\alpha \in J$, $\alpha \in I_k$ for some $k \in \mathbb{N}$.

$\Rightarrow \langle \alpha \rangle \subseteq I_k \Rightarrow \forall m > k$, $\langle \alpha \rangle \subseteq I_k \subseteq I_m \subseteq J = \langle \alpha \rangle$

$\Rightarrow \forall\, m \geq k, \quad I_m = I_k.$ □

<u>Lemma 36.2</u> Let R be a PID. Then any $r \in R$, r not a unit, is an irreducible or a product of irreducibles: $\exists$ finitely many irreducibles $p_1 \cdots p_k$ s.t. $r = p_1 \cdots p_k$.

<u>Proof</u> Fix $r \in R$, r not a unit.

If r is an irreducible, we're done.

Otherwise $r = r_1 \cdot r_2$ for some $r_1, r_2 \notin R^\times$.

If r_1, r_2 are irreducible, we're done.

Otherwise r_1, r_2 (one or both) can be factored). Say

$$r_1 = r_{11} r_{12}, \quad r_{11}, r_{12} \notin R^\times, \quad r_2 \text{ irreducible.}$$

If r_{11}, r_{12} are irreducibles, we are done.

Otherwise one of r_{1i}'s can be factored. Say

$$r_{11} = r_{111} \cdot r_{112} \qquad r_{111}, r_{112} \notin R^\times$$

If the process <u>does not</u> terminate,

We get a chain of ideals $\langle r_1 \rangle \subsetneq \langle r_{11} \rangle \subsetneq \langle r_{111} \rangle \subsetneq \cdots$

By lemma 36.1, this is impossible in a PID.

$\therefore$ each $r \in R$, $r \notin R^\times$ is a product of finitely many irreducibles □

<u>Recall</u> if R is a PID and $p \in R$ is irreducible then $\langle p \rangle$ is maximal $\Rightarrow$ $R/\langle p \rangle$ is a field $\Rightarrow$ $R/\langle p \rangle$ is an integral domain $\Rightarrow$ $\langle p \rangle$ is prime $\Rightarrow$ p is prime: if $p \mid (ab)$ then $p \mid a$ or $p \mid b$

<u>Lemma 36.3</u> Let R be a PID

$$u \cdot p_1 \cdots p_m = v\, q_1 \cdots q_n \qquad u, v \in R^\times,$$

p_i's, q_j's irreducible. Then $m = n$ and $\exists\, \sigma \in S_n$

so that p_i, $q_{\sigma(i)}$ are associates for $i = 1, \ldots n$.

<u>Proof</u> (Induction on $\max(n, m)$)

- If $\max(n, m) = 1$, $n = m = 1 \Rightarrow u p_1 = v q_1 . \Rightarrow p_1 = u^{-1} v q_1$
  $\Rightarrow p_1, q_1$ are associates.

- (inductive step) Suppose $u p_1 \cdots p_m = v q_1 \cdots q_n$. Then
  - $v^{-1} u p_1 \cdots p_m = q_1 \cdots q_n$. Since $p_1 \mid (u p_1 \cdots p_m)$,
  $p_1 \mid (q_1 \cdots q_m)$. Since p_1 is irreducible, it's prime
  $\Rightarrow$ $p_1 \mid q_\ell$ for some ℓ. Reindex q_j's so that $p_1 \mid q_1$.
  $\Rightarrow q_1 = a p_1$ for some $a \in R$.

  q_1 is irreducible. $\Rightarrow$ a or p_1 is a unit. p_1 is <u>not</u> a unit.
  $\Rightarrow$ a is a unit. $\Rightarrow$ (1) p_1, q_1 are associates.
  (2) $v^{-1} u p_2 \cdots p_m = a q_2 \cdots q_n$
  $\max(m-1, n-1) < \max(n, m)$.

  Inductive assumption $\Rightarrow$ $n - 1 = m - 1$ (ie $n = m$)
  and (after reindexing q_i's)
  p_2 & q_2, p_3 & q_3, $\ldots$ p_m & q_m are associates.

$\square$