Current Topic: "Some Algebra."

Review:

Any ring, $p \in R$ called prime iff $pR \subseteq R$ is prime ideal, i.e., iff $p \nmid a$ & $p \nmid b \implies p \nmid ab$.

[Equivalently, $p | ab \implies p | a$ or $p | b$.]

Observe: $0 | a \iff a \in 0R$
$\iff a = 0$.

Consequence: $0 \in R$ is a prime element iff R is a domain.

Now let R be domain. Then

$aR = bR \iff a = ub$ for some unit $u \in R$.

Notation: "$a \sim b$" = "a, b similar / associated"

We say $m \in R$ is irreducible if

$d \mid m \implies d \sim m$ or $d \sim 1$.

Equivalently, $mR \subseteq R$ is maximal among principal ideals, i.e,

$$mR \subseteq dR \subseteq R \implies \underset{d \sim m}{mR = dR} \text{ or } \underset{d \sim 1}{dR = R}.$$

If R is a <u>PID</u> then

$$\underset{\text{irreducible}}{m \in R} \iff \underset{\text{maximal}}{mR \subseteq R}.$$

[Are units irreducible? They are iff $1R \subseteq R$ is maximal.

Conventionally: $1R \subseteq R$ is not maximal, hence units not irreducible.

Following this if

$$R/I \text{ field} \iff I \text{ maximal},$$

then $0 \neq 1$ in a field.]

Observe that "primality" & "irreducibility" are both famous properties of "prime" integers.

Euclid's Lemma:

Irreducible $\Longleftrightarrow$ Prime in a PID.

[Technically, irreducible elements are the nonzero primes.]

Proof: Let $p \in R$ be prime, $p \neq 0$.
To show irreducibility, let $p = ab$.
Thus $a, b \mid p$ & $p \mid ab$.

p prime $\Rightarrow p \mid a$ or $p \mid b$.

If $p \mid a$ then since $a \mid p$ we have $pR = aR$, i.e., $p \sim a$.

If $p \mid b$ then since $b \mid p$, have $b = up$ for some (unit) $u \in R$, hence

$$p = ab = aup \Rightarrow 1 = au \Rightarrow 1 \sim a.$$

Summary: $p = ab \Rightarrow p \sim a$ or $p \sim b$

$[a \mid p \Rightarrow p \sim a$ or $1 \sim a]$

Remark: prime $\Rightarrow$ irred in <u>any</u> domain.

Other direction, let $m \in R$ be irreducible. Then

$m \in R$ irreducible $\Leftrightarrow mR \subseteq R$ maximal

$\Leftrightarrow R/mR$ field

one way $\Rightarrow R/mR$ domain

$\Leftrightarrow mR \subseteq R$ prime

$\Leftrightarrow m \in R$ prime.

Q: which direction was easier?

Concept of "Euclidean ring" is awkward; mostly a convenient way to prove PIR. The size function

$\delta : R \setminus 0 \to \mathbb{N}$

is used for inductive proofs, but a PIR has its own intrinsic version of induction.

<u>PIR $\Rightarrow$ Noetherian</u>:

Any strictly ascending chain of ideals is finite.

<u>Proof</u>: Assume for contradiction $\exists$ infinite ascending chain:

$$a_1 R \subsetneq a_2 R \subsetneq a_3 R \subsetneq \cdots \subsetneq R.$$

Let $I = \bigcup_i a_i R$. Then $I \subseteq R$ is an ideal:

$\alpha, \beta \in I$, $r \in R$

$\alpha \in a_i R$

$\beta \in a_j R$

$\alpha, \beta \in a_k R$, $k = \max(i, j)$.

Then $\alpha + r\beta \in a_k R$

$\Rightarrow \alpha + r\beta \in I$.

Since R is PIR, $I = bR$ for some $b \in R$. Finally, since $b \in I$, $b \in a_i R$ some i, hence

$$bR \subseteq a_i R \subsetneq a_{i+1} R \subseteq I = bR.$$

$$bR \subsetneq bR.$$

Contradiction. ///

Combing Euclid's Lemma and "generalized induction," we obtain a version of unique prime factorization.

<u>PID $\Rightarrow$ UFD</u>: Let R be PID. For any $a \in R \setminus 0$ we have a factorization into primes

$$a \sim p_1 p_2 \cdots p_k.$$

Furthermore, if $a \sim q_1 q_2 \cdots q_\ell$ then $k = \ell$ & $p_i \sim q_i$ after relabeling.

In other words, <u>R is a UFD</u>.

<u>Proof</u>: Existence: If $a \in R \setminus 0$ cannot be factored into primes, then a itself is not prime & not a unit, hence a can be factored as

$$a = bc \quad \text{with } a \not\sim b \ \& \ a \not\sim c,$$

i.e. $aR \subsetneq bR$ & $aR \subsetneq cR$. If the process never stops then we will obtain some infinite increasing chain:

$$aR \subsetneq a_1R \subsetneq a_2R \subsetneq \cdots$$

Contradiction.

Uniqueness: Suppose we have two factorizations into primes:

$$p_1 p_2 \cdots p_k \sim q_1 q_2 \cdots q_l .$$

Since $p_1 \mid q_1 q_2 \cdots q_l$ and p_1 is prime, Euclid's Lemma says $p_1 \mid q_i$ for some i.

By relabeling the factors we can assume $p_1 \mid q_1$.

Then since q_1 is irreducible we have $p_1 \sim q_1$ or $p_1 \sim 1$.

But $p_1 \sim 1$ is not allowed for primes, hence $p_1 \sim q_1$. Finally, we cancel this factor from both sides:

$$p_2 \cdots p_k \sim q_2 \cdots q_l .$$

And the proof follows by induction. ///

Remark: This proof should motivate the definitions.

irred, prime, similar, etc.

We take this as the foundation for further definitions.