1.4 Divisibility and Factorization

Let A be a ring and $x \in A$.

Call x **irreducible** if x is not a unit and

$(\forall y, z \in A)$

$$x = yz \implies y \text{ or } z \text{ is a unit.}$$

Call x **prime** if $x \neq 0$, x is not a unit and

$(\forall y, z \in A)$

$$x \mid yz \implies x \mid y \text{ or } x \mid z \, .$$

Easy to check, for nonzero x :

x is prime iff xA is a prime ideal.

Example:

If $A = \mathbb{Z}$ then irreducibles and primes coincide and are just the usual prime numbers.

Exercise:

Prove that in an integral domain every prime is irreducible.

However there are integral domains in which not all irreducibles are primes.

Exercise: Let

$$A \;=\; \mathbb{Z}[\sqrt{-5}] \;=\; \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\} \,,$$

which, being a subring of $\mathbb{C}$, is an integral domain.

Recall that the map : $\mathbb{C} \longrightarrow \mathbb{R}^+ \cup \{0\}$ defined by

$$z \;\mapsto\; |z|^2$$

is multiplicative.

(1) Deduce that the units of A are precisely ± 1 .

(2) Observe that

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

in A . Prove that

$$2\,,\;\; 3\,,\;\; 1+\sqrt{-5}\,,\;\; 1-\sqrt{-5}$$

are irreducibles but not primes.

Call an integral domain A a **unique factorization domain (UFD)** if

(i) every nonzero nonunit of A can be expressed as a product of irreducibles; and

(ii) the factorization is unique up to order and multiplication by units.

e.g. $A = \mathbb{Z}$ is a UFD and (noting the units are ± 1):

$$30 = 2 \cdot 3 \cdot 5 = 3 \cdot 2 \cdot 5 = -3 \cdot -5 \cdot 2 \, .$$

Exercise:

Prove that in a UFD every irreducible is prime.

Thus in a UFD the notions of irreducible and prime coincide.

Gauss' Theorem:

If A is a UFD then the polynomial ring $A[x]$ is also a UFD.

The proof is deferred until later.

Note that vacuously

$$\boxed{\text{all fields are UFD's.}}$$

Examples:

(1) Let $A = F[x_1, \ldots, x_n]$, the polynomial ring in n commuting indeterminates over a field F .

Clearly, by iterating Gauss' Theorem, A is a UFD.

If $p = p(x_1, \ldots, x_n)$ is any irreducible polynomial over F then p is prime (by a previous exercise), so the principal ideal

$$\boxed{pA \text{ is a prime ideal of } A\,.}$$

(2) Let $A = \mathbb{Z}$ or $A = F[x]$ where F is a field.

It is straightforward to show, using the Division algorithm, that

$$\boxed{\text{every ideal of } A \text{ is principal.}}$$

In the case $A = \mathbb{Z}$ the prime ideals are precisely those generated by 0 or a prime number.

In the case $A = F[x]$ the prime ideals are precisely those generated by the zero polynomial or an irreducible polynomial.

In both cases, because of the Observation below,

all nonzero prime ideals are also maximal.

Observation:

Let A be a **principal ideal domain (PID)**, that is, an integral domain in which all ideals are principal.

Then every nonzero prime ideal is maximal.

Proof: Let I be a nonzero prime ideal, and suppose

$$I \subset J \triangleleft A .$$

Then, for some $x, y, z \in A$,

$$I = xA \; , \quad J = yA \; , \quad x = yz \; .$$

But I is prime and $yz \in I$, so

$$y \in I \qquad \text{or} \qquad z \in I \; .$$

If $y \in I$ then $J \subseteq I \subset J$, impossible.

Hence $y \notin I$, and so $z \in I$.

Thus $z = xt$ for some $t \in A$,

and so

$$x = yz = yxt = xyt ,$$

so

$$0 = xyt - x = x(yt - 1) .$$

But $I \neq \{0\}$, so $x \neq 0$.

Hence, since A is an integral domain, $yt-1 = 0$, so y is a unit, and $J = A$.

This shows I is maximal, and the proof is complete.

Examples (continued):

(3) Consider again $A = F[x_1, \ldots, x_n]$ where F is a field. Put

$$M = \{ p \in A \mid \text{the constant term of } p \text{ is } 0 \} .$$

Then $M = \ker \psi$ where $\psi : A \to F$ is the epimorphism

$$p(x_1, \ldots, x_n) \mapsto p(0, \ldots, 0) .$$

By the Fundamental Homomorphism Theorem, $A/M \cong F$.

This proves

$$\boxed{M \text{ is maximal.}}$$

However, if $n > 1$, then

$$\boxed{M \text{ is not principal,}}$$

because of the following

Exercise: Prove that M is generated by n elements, but not by fewer than n elements.