2-3-1994

Principal ideal domains are unique factorization domains.

Definition. Let R be an integral domain.

(a) If $x, y \in R$, then x **divides** y if $xz = y$ for some $z \in R$. $x \mid y$ means x divides y.

(b) x and y are **associates** if $xu = y$, where u is a unit. (Recall that a **unit** in a ring is an element with a multiplicative inverse.)

(c) An nonzero element $x \in R$ is **irreducible** if x is not a unit, and if $x = yz$ implies either y is a unit or z is a unit.

(d) An element $x \in R$ is **prime** if $x \neq 0$, x is not a unit, and $x \mid yz$ implies $x \mid y$ or $x \mid z$.

Lemma. In a domain, primes are irreducible.

Proof. Let x be prime. I must show x is irreducible. Suppose $x = yz$. I must show either y or z is a unit.

$x = yz$, so obviously $x \mid yz$. Thus, $x \mid y$ or $x \mid z$. Without loss of generality, suppose $x \mid y$.

Write $xw = y$. Then $x = yz = xwz$, and since $x \neq 0$ (primes are nonzero) and we're in a domain, $1 = wz$. Therefore, z is a unit, and x is irreducible. □

Remark. The converse is true in a PID. □

Definition. Let R be a domain, and let $x, y \in R$. $d \in R$ is a **greatest common divisor** of x and y if:

1. $d \mid x$ and $d \mid y$.
2. If $d' \mid x$ and $d' \mid y$, then $d' \mid d$.

The definition say "a" greatest common divisor, rather than "the" greatest common divisor, because greatest common divisors are only unique up to multiplication by units.

Lemma. Let R be a PID, and let $x, y \in R$. Then x and y have a greatest common divisor d, and $\langle x, y\rangle = \langle d\rangle$.

Proof. Let $x, y \in R$, and consider the ideal $\langle x, y\rangle$. Since R is a PID, there is an element d such that $\langle x, y\rangle = \langle d\rangle$. Since $x \in \langle d\rangle$, $x = da$ for some $a \in R$, so $d \mid x$; likewise, $d \mid y$. It follows that d is a common divisor of x and y.

Suppose that $d' \mid x$ and $d' \mid y$. Since $d \in \langle x, y\rangle$, it follows that $d = px + qy$ for some $p, q \in R$. Then $d' \mid px + qy = d$. Hence, d is a greatest common divisor of x and y. □

The proof of the lemma shows that the following result (which is true in the integers) holds in a PID.

Corollary. Let R be a PID, and let $x, y \in R$. If (x, y) is a greatest common divisor of x and y, then

$$(x, y) = ax + by, \quad \text{for some} \quad a, b \in R. \ \square$$

Example. Consider the polynomial ring $\mathbb{Q}[x]$. $\mathbb{Q}[x]$ is a PID, since it's a Euclidean domain under the degree function. $x - 2$ is a greatest common divisor of $x^2 - 4$ and $x^2 - x - 2$:

$$x^2 - 4 = 1 \cdot (x^2 - x - 2) + (x - 2)$$

$$x^2 - x - 2 = (x + 1)(x - 2) + 0$$

Notice that the proof of the preceding result identifies $x - 2$ as the generator of $\langle x^2 - 4, x^2 - x - 2\rangle$: $\langle x^2 - 4, x^2 - x - 2\rangle = \langle x - 2\rangle$.

Finally, observe that any nonzero constant multiple of $x-2$ is also a greatest common divisor of x^2-4 and x^2-x-2: for example, $\frac{1}{100}(x-2)$ works. This makes sense, because the units in $\mathbb{Q}[x]$ are the nonzero elements of $\mathbb{Q}$. $\square$

Definition. Let R be a domain, and let $x, y \in R$. x and y are **relatively prime** if their only common divisors are units.

Clearly, if R is a PID and x and y are relatively prime, then $\langle x, y\rangle = R$.

Example. In the polynomial ring $\mathbb{Q}[x]$, x^2-4 and x^3+1 are relatively prime.

$$x^3+1 = x\cdot(x^2-4) + (4x+1)$$

$$x^2-4 = \left(\frac{1}{4}x - \frac{1}{16}\right)(4x+1) - \frac{63}{16}$$

$$4x+1 = -\frac{63}{16}\left(-\frac{64}{63}x - \frac{16}{63}\right) + 0$$

By unwinding this computation, you can express the greatest common divisor as a linear combination of x^2-4 and x^3+1:

$$-\frac{63}{16} = -(x^2-4) + \left(\frac{1}{4}x - \frac{1}{16}\right)(4x+1) = -(x^2-4) + \left(\frac{1}{4}x - \frac{1}{16}\right)\left((x^3+1) - x\cdot(x^2-4)\right) =$$

$$\left(-\frac{1}{4}x^2 + \frac{1}{16}x - 1\right)(x^2-4) + \left(\frac{1}{4}x - \frac{1}{16}\right)(x^3+1).$$

Notice that $-\dfrac{63}{16}$ is a unit in $\mathbb{Q}[x]$, so $\langle -\dfrac{63}{16}\rangle = \mathbb{Q}[x]$. Thus,

$$\langle x^2-4, x^3+1\rangle = \langle -\frac{63}{16}\rangle = \mathbb{Q}[x]. \ \square$$

Corollary. Let R be a PID, $x \in R$. If x is irreducible, then x is prime.

Proof. Suppose x is irreducible, and $x \mid yz$. Suppose $x \not\mid y$. I need to show that $x \mid z$.

Consider the ideal $\langle x, y\rangle$. R is a PID, so $\langle x, y\rangle = \langle w\rangle$ for some w. Since $x \in \langle x, y\rangle = \langle w\rangle$, it follows that $x = wa$ for some a. However, x is irreducible, so one of w, a is a unit.

Suppose a is a unit. Then $\langle w\rangle = \langle x\rangle$, so $\langle x, y\rangle = \langle x\rangle$. This means $y \in \langle x\rangle$, so $x \mid y$. $\times$

Hence, w is a unit. Therefore, $\langle w\rangle = R$, so $\langle x, y\rangle = R$. Write $1 = cx + dy$. Then

$$z = cxz + dyz.$$

Since x divides both terms on the right, x divides z. $\square$

Definition. A commutative ring R is **Noetherian** if it satisfies the **ascending chain condition** on ideals: If

$$I_1 \subset I_2 \subset \cdots$$

is a sequence of ideals, then for some $n \ge 1$

$$I_n = I_{n+1} = I_{n+2} = \cdots.$$

Remarks. Emmy Noether (1882 - 1935) was a German algebraist who worked in the United States during the last part of her life. She made many important contributions to algebra, for example in ring and ideal theory.

The **descending chain condition** on ideals is stated in the obvious way. A commutative ring satisfying the descending chain condition on ideals is said to be **Artinian**, after the German algebraist Emil Artin (1898 - 1962). $\square$

Lemma. PIDs are Noetherian.

Proof. Suppose R is a PID, and let

$$I_1 \subset I_2 \subset \cdots$$

be a sequence of ideals. Let

$$I = \bigcup_{n=1}^{\infty} I_n.$$

The ascending union of ideals is an ideal, so I is an ideal.

Since R is a PID, there exists $x \in R$ such that $\langle x \rangle = I$. Then $x \in I_n$ for some n, so $I = \langle x \rangle \subset I_n$. It follows that $I = I_n$, and clearly $I = I_{n+1} = I_{n+2} = \cdots$. Hence, R is Noetherian. $\square$

Definition. A **unique factorization domain** (UFD) is an integral domain R satisfying the following properties:

(a) If $x \in R$, $x \neq 0$, and x is not a unit, then x may be written as a finite product of irreducible elements of R.

(b) If $p_1 \cdots p_m$ and $q_1 \cdots q_n$ are two factorizations of a given element into irreducibles, then $m = n$. Moreover, the q's may be renumbered so that p_i and q_i are associates (that is, they differ by a unit).

The proof that every PID is a UFD will be broken into steps. First, I'll show that property (a) holds: Every element not zero or a unit can be factored into irreducibles.

Lemma. Let R be a domain, $x, y \in R$. x and y are associates if and only if $\langle x \rangle = \langle y \rangle$.

Proof. Assume $x, y \neq 0$, otherwise the result is trivial.

If x and y are associates, then $x = uy$, where u is a unit. Immediately, $x \in \langle y \rangle$. However, $u^{-1}x = y$ shows $y \in \langle x \rangle$. Therefore, $\langle x \rangle = \langle y \rangle$.

Conversely, suppose $\langle x \rangle = \langle y \rangle$. Since $x \in \langle y \rangle$, $x = ya$; likewise, $y \in \langle x \rangle$ implies $y = xb$. Therefore, $x = ya = xba$, so $1 = ab$, and a and b are units. Hence, x and y are associates. $\square$

Theorem. Let R be a PID, $x \in R$. If $x \neq 0$ and x is not a unit, then x can be written as a product of irreducible elements.

Proof. Suppose x is nonzero and a nonunit. If x is irreducible, I'm done. Otherwise, x can be written as $x = yz$, where neither y nor z is a unit. If y and z are irreducible, I'm done. If not, continue the process by factoring y and z. I only need to show that this process terminates.

Note that an equation $x = yz$ implies that $\langle x \rangle \subset \langle y \rangle$ and $\langle x \rangle \subset \langle z \rangle$. Moreover, the previous lemma shows that the inclusions are equalities if and only if x is an associate of one of the factors. Thus, if the factorization is proper — if neither y nor z is a unit — it doesn't hurt to assume these are strict inclusions.

Thus, if x factors indefinitely, there is a strictly ascending chain of ideals

$$I_1 \subset I_2 \subset \cdots.$$

This contradicts the fact that R, as a PID, is Noetherian. Hence, the factorization process must terminate, which can only happen when x has been factored into a product of irreducibles. $\square$

Theorem. Every PID is a UFD.

Proof. Every nonzero nonunit can be factored into a product of irreducibles. It remains to show that such a factorization is unique.

Let $p_1 \cdots p_m = q_1 \cdots q_n$ be two factorizations of a given element into irreducibles. Without loss of generality, say $n \geq m$.

Since p_1 is irreducible, it is prime. Since p_1 divides the product on the right, and easy induction shows it divides one of the factors. Again without loss of generality, suppose it divides q_1.

Now $q_1 = p_1 a_1$ implies a_1 is a unit, since q_1 is irreducible. Thus, p_1 and q_1 are associates. Replace q_1 with $p_1 a_1$ and cancel p_1 off both sides; then

$$p_2 \cdots p_m = a_1 q_2 \cdots q_n.$$

Continuing in this fashion exhausts the p's, at which point the equation is

$$1 = a_1 \cdots a_m q_{m+1} \cdots q_n.$$

It follows that $q_{m+1}, \ldots q_n$ are units, if they're really there. Since they're irreducible, they can't be units, so they're not there. This proves $m = n$, and the rearranging done during the proof proves the claim about associates. $\square$