Queen Mary
University of London

MAS 305 — Algebraic Structures II

Notes 12 — **Autumn 2006**

Factorization in integral domains

Lemma If a, b, c are elements of an integral domain R and $ab = ac$ then either $a = 0_R$ or $b = c$.

Proof $ab = ac \Rightarrow a(b-c) = 0_R \Rightarrow a = 0_R$ or $b - c = 0_R$ because R has no zero-divisors. $\square$

Definition Let a and b be elements of an integral domain R. Then a is an *associate* of b if there is a unit u in R with $au = b$.

Lemma In an integral domain R, "is an associate of" is an equivalence relation.

Proof
(a) R has an identity 1_R, which is a unit, and $a1_R = a$ for all a in R. So the relation is reflexive.

(b) If u is a unit then there is v in R with $uv = 1_R$, so v is also a unit. If $au = b$ then $bv = auv = a$. So the relation is symmetric.

(c) Suppose that $au = b$ and $bw = c$, where u and w are units. Then uw is also a unit, and $a(uw) = bw = c$. So the relation is transitive. $\square$

Definition Let R be an integral domain and let r be in R. Then r is *irreducible* if $r \neq 0_R$ and r is not a unit and if whenever $r = ab$ then either a or b is a unit (so the other is an associate of r).

Example In $\mathbb{Z}$, n is irreducible if $\pm n$ is prime.

Definition An integral domain R is a *unique factorization domain* (UFD) if

(a) every element other than 0_R and units can be written as a product of a finite number of irreducibles, and

(b) if $r_1 r_2 \ldots r_n = s_1 s_2 \ldots s_m$ with $r_1, \ldots, r_n, s_1, \ldots, s_m$ all irreducible then $n = m$ and there is a permutation π of $\{1, \ldots, n\}$ such that r_i and $s_{i\pi}$ are associates for $i = 1, \ldots, n$.

Example $\mathbb{Z}$ is a UFD.

Definition Let R be a commutative ring.

(a) If r, s are in R, then r *divides* s if $s = rx$ for some x in R.

(b) If r, s are in R, then the element t in R is a *highest common factor* (hcf) or *greatest common divisor* (gcd) of r and s if

  (i) t divides r and t divides s

  (ii) if $x \in R$ and x divides t and x divides s then x divides t.

Theorem Let R be an integral domain. Let r and s be in R.

(a) If r divides s and s divides r then r and s are associates.

(b) If d and e are both hcfs of r and s then d and e are associates. (Note: r and s may not have any hcfs.)

Proof (a) Suppose that $s = rx$ and $r = sy$, for some x, y in R. Then $r = rxy$, so $r(1_R - xy) = 0_R$. If $r = 0_R$ then $s = 0_R x = 0_R$ so r and s are associates. If $r \neq 0_R$ then $1_R - xy = 0_R$, so $xy = 1_R$, so x and y are units and therefore r and s are associates.

(b) If d and e are hcfs of r and s then d divides e and e divides d, so, by part (a), d and e are associates. $\square$

Theorem If R is a unique factorization domain and r, s are in R then r and s have a highest common factor.

Proof If $r = 0_R$ then s is a hcf of 0_R and s, because all elements divide 0_R.

If r is a unit then there is some u with $ru = 1_R$. If $xy = r$ then $xyu = yxu = 1_R$ so x and y are both units. Thus the only elements dividing r are units, so 1_R is a hcf of r and s.

Suppose that r and s are neither zero nor units. Let $r = r_1 \ldots r_n$ where the r_i are irreducibles. Suppose that $r = ab$ where a, b are neither zero nor units. Let $a = a_1 \ldots a_m$ and $b = b_1 \ldots b_t$, where the a_j and b_k are irreducibles. Then

$$r = r_1 \ldots r_n = a_1 \ldots a_m b_1 \ldots b_t$$

so $m + t = n$ and we can reorder $r_1, \ldots, r_n$ so that

$$\begin{aligned} r_i &\text{ is an associate of } \quad a_i \quad \text{for } i = 1, \ldots, m \\ r_{m+j} &\text{ is an associate of } \quad b_j \quad \text{for } j = 1, \ldots, n. \end{aligned}$$

For irreducibles z in R, let $\phi_r(z)$ be the number of $r_1, \ldots, r_n$ which are associates of z; that is,

$$\phi_r(z) = |\{i : 1 \leqslant i \leqslant n,\ r_i \text{ is an associate of } z\}|\,.$$

This is well defined because R is a UFD. We have shown that a divides r if and only if $\phi_a(z) \leqslant \phi_r(z)$ for all irreducibles z. (Note: we need to check this only for $z = a_1, \ldots, a_m$, which is a finite number of cases.)

Put $\psi(z) = \min\{\phi_r(z), \phi_s(z)\}$ for the finite number of irreducibles $r_1, \ldots, r_n$. Then

$$\prod_{\text{such } z} z^{\psi(z)}$$

is a highest common factor of r and s. (Note that the product is over only finitely many irreducibles, and is defined to be 1_R if $\psi(z) = 0$ for $z = r_1, \ldots, r_n$. □

Definition A *principal ideal domain* (PID) is an integral domain in which every ideal is principal.

Example $\mathbb{Z}$ is a PID.

Theorem Let R be a PID, and let r, s be in R. Then r and s have a highest common factor t, and there are x, y in R such that $t = rx + sy$.

Proof Let $I = \langle\{r, s\}\rangle$, the smallest ideal containing r and s. Then

$$I = \{rx + sy : x, y \in R\}\,.$$

(R has an identity, so r and s are in I; the distributive law shows that I is a subgroup under $+$; and the associativity and commutativity of multiplication show that iz and zi are in I when $i \in I$ and $z \in R$.)

R is a PID, so I is a principal ideal, so there is an element t such that $I = \langle t \rangle = tR$. Moreover, $t \in I$, so there are elements x, y in R with $t = rx + sy$.

Now, $r \in I$ so t divides r, and $s \in I$ so t divides s. Suppose that a divides r and a divides s. Then $r = ab$ and $s = ac$ for some b, c in R. Thus $t = rx + sy = abx + acy = a(bx + cy)$ so a divides t. Hence t is an hcf of r and s. □

Definition A ring R is *Noetherian* if it satisfies the ascending chain condition (ACC), which says that if

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_j \subseteq I_{j+1} \subseteq \cdots$$

is an infinite ascending chin of ideals of R then there is some integer N such that $I_N = I_{N+1} = I_{N+2} = \cdots$, that is, $I_j = I_N$ whenever $j \geqslant N$.

Example The ideals of $\mathbb{Z}$ are $n\mathbb{Z}$ for n in $\mathbb{Z}$. If $n \neq 0$ then $n\mathbb{Z}$ is contained in only finitely many ideals of $\mathbb{Z}$, because $n\mathbb{Z} \subseteq m\mathbb{Z}$ if and only if m divides n. Hence $\mathbb{Z}$ is Noetherian.

Theorem If R is a PID then R is Noetherian.

Proof Suppose that

$$I_1 \subseteq I_2 \subseteq \cdots$$

are ideals of R. Put $I = \bigcup_{n=1}^{\infty} I_n$.

(a) $I_1 \subseteq I$, so I is not empty.

(b) Let r, s be in I. Then $r \in I_n$ and $s \in I_m$, for some n, m. We may suppose that $n \leqslant m$, so $r \in I_m$. Then $r - s \in I_m$, because I_m is an ideal, so $r - s \in I$.

(c) Let $r \in I$ and $t \in R$. Then $r \in I_n$, for some n, and $rt \in I_n \subseteq I$, since I_n is an ideal.

Hence I is an ideal of R.

However, R is a PID, so there is some x in R with $I = \langle x \rangle$. Then $x \in I$, so $x \in I_n$ for some n, so $\langle x \rangle \subseteq I_n$, so $I \subseteq I_n$. If $j \geqslant n$ then $I_j \subseteq I \subseteq I_n \subseteq I_j$, so $I_j = I_n$. □

Theorem Let R be a Noetherian integral domain. If $r \in R$ and r is neither zero nor a unit then r can be written as a product of a finite number of irreducibles.

Proof If r is irreducible, we are done.

If not, then $r = r_1 s_1$ with neither r_1 nor s_1 a unit or zero. If both r_1 and s_1 can be factorized as products of irreducibles, then so can r. If not, suppose that we chose the labels so that r_1 cannot be factorized. (We are writing "cannot be factorized" as a shorthand for "cannot be written as a product of a finite number of irreducibles".)

Similarly, $r_1 = r_2 s_2$ where neither r_2 nor s_2 is a unit or zero and r_2 cannot be factorized. Continuing in this way, we obtain elements $r_1, r_2, \ldots, r_n$, with $r_n = r_{n+1} s_{n+1}$ and neither r_{n+1} nor s_{n+1} a unit or zero. Then $r_n \in \langle r_{n+1} \rangle$ so $\langle r_n \rangle \subseteq \langle r_{n+1} \rangle$. If $\langle r_n \rangle = \langle r_{n+1} \rangle$ then $r_{n+1} \in \langle r_n \rangle$ so $r_{n+1} = r_n x$ for some x in R. Then $r_{n+1} = r_{n+1} s_{n+1} x$, so $1_R = s_{n+1} x$, because R is an integral domain and $r_{n+1} \neq 0$, so s_{n+1} is a unit, which is a contradiction.

So, for all n, we have $\langle r_n \rangle \subset \langle r_{n+1} \rangle$ but $\langle r_n \rangle \neq \langle r_{n+1} \rangle$. This contradicts ACC, so r must be factorizable. □

Theorem If R is a PID then it is a UFD.

Proof If R is a PID then R is Noetherian, so every element of R that is neither zero not a unit has a factorization into irreducibles.

Suppose that r is neither zero nor a unit and $r = r_1 \dots r_n = s_1 \dots s_m$ where all the r_i and s_j are irreducible. Since R is a PID, r_1 and s_1 have a hcf t. If t is not a unit then it is an associate of both r_1 and s_1, so r_1 and s_1 are associates. If t is a unit then 1_R is a hcf of r_1 and s_1, so $1_R = r_1 x + s_1 y$ for some x, y in R. Then

$$\begin{aligned} s_2 \dots s_m &= 1_R s_2 \dots s_m \\ &= r_1 x s_2 \dots s_m + s_1 y s_2 \dots s_m \\ &= r_1 x s_2 \dots s_m + y r_1 \dots r_n \\ &= r_1 (x s_2 \dots s_m + y r_2 \dots r_n), \end{aligned}$$

so r_1 divides $s_2 \dots s_m$.

Repeating the argument shows that there is some j such that r_1 is an associate of s_j (properly, this is induction on m). Renumber the s_i to make r_1 an associate of s_1, say $s_1 = r_1 u$ for some unit u. Then

$$r_1 r_2 \dots r_n = r_1 u s_2 \dots s_m$$

and $r_1 \neq 0$ so $r_2 \dots r_n = (u s_2) s_3 \dots s_m$ with $u s_2$ also irreducible.

Doing this for a finite number of steps (equivalently, using induction on n), shows that the s_j can be reordered so that r_i is an associate of s_i for $i = 1, \dots, n$, and hence $m = n$. $\square$