7. Euclidean and principal ideal domains

Maximal Ideals

Proposition: (Krull) Every ideal in a ring with unity is contained in a maximal ideal.

Ring factorization theorem

Let R be a commutative ring with unity.

Proposition: Let $I_1, \ldots, I_k$ are ideals of R, then there is a ring homomorphism

$$R \to R/I_1 \times \cdots \times R/I_k.$$

Its kernel is the intersection $\bigcap_{i=1}^k I_i$. If, for every pair, $I_j + I_k = R$, the map is surjective and its kernel is $I_1 \cdots I_k$.

A first look at unique factorization: Euclidean domains and PID

Let R be an integral domain.

Definition: Let $\mathbb{N}$ be the natural numbers *starting at zero.* A function $N : R \to \mathbb{N}$ with $N(0) = 0$ is called a norm. If $N(a) = 0 \implies a = 0$ then N is calledf a positive norm.

Definition: R is called a *Euclidean domain* if there is a norm on R such that, given $a, b \in R$, with $b \neq 0$, there are elements q and r in R such that

$$a = qb + r$$

and either $N(r) = 0$ or $N(r) < N(b)$.

Euclidean domains have a euclidean algorithm.

Key Examples: $F[x]$ when F is a field; Z; $Z[i]$; $Z[\sqrt{-2}]$.

Proposition: Every ideal in a Euclidean Domain R is principal. More precisely, if I is a nonzero ideal in R, then $I = aI = (a)$ where a is any nonzero element of I of minimal norm.

Divisibility and ideals

Definition: Let R be a commutative ring, with $a, b \in R$ and $b \neq 0$. - We say a divides b ($a|b$) if there is $x \in R$ with $b = ax$. - A greatest common divisor of a and b is an element $d \in R$ with $d|a$ and $d|b$, and such that, if $x|a$ and $x|b$ then $x|d$. (In general the gcd need not be unique)

Translations. - $a|b$ if and only if $bR \subset aR = (a)$. (*to contain is to divide*) - Let I be the ideal of R generated by a and b: $I = (a, b) = aR + bR$. Then $d = \gcd(a, b)$ if and only if $I \subset dR$ and if aR is any principal ideal containing I then $dR \subset aR$.

Proposition: Let the ideal $I = (a, b)$. If $I = dR$ (so that I is principal) then d is the greatest common divisor of a and b.

Proposition: Two principal ideals aR and bR are equal if and only if $a = bu$ for some unit $u \in R$.

In a Euclidean domain, the ideal $I = (a, b)$ is principal and generated by the "last remainder" obtained from Euclid's algorithm.

Principal Ideal domains

Definition: An integral domain in which every ideal is principal is called a Principal Ideal Domain.

Principal ideal domains satisfy the conclusions of the Euclidean algorithm (but maybe without the algorithm).

That is, given $a, b \in R$ if R is a PID, then the ideal $(a, b) = (d)$ where d is a greatest common divisor of R, and there are x and y in R such that $ax + by = d$. The gcd d is unique up to multiplication by a unit.

Proposition: In a principal ideal domain, every nonzero prime ideal is maximal.

Proof: Suppose (p) is a prime ideal and (m) is an ideal with $(p) \subset (m)$. Then $p = mx$ for some $x \in R$. Since (p) is prime, either $m \in P$ or $x \in P$. If $m \in P$, then $(m) = (p)$. If $x \in P$, then $x = pr$ and so $p = mpr$ or $p(1 - mr) = 0$, meaning $mr = 1$ and so m is a unit. Then $(m) = R$. So the only ideals of R containing (p) are (p) and R, and (p) is maximal. (Note: this is the ideal theoretic version of the statement that, if $p|xm$, then either $p|x$ or $p|m$.)

Proposition: A Euclidean ring is a PID. (DF p. 281 contains a strengthening of this result, proving that an integral domain R is a PID if and only if it has a "Dedekind-Hasse" norm, which is a slightly more general type of norm that isn't necessarily positive)

Unique factorization

Key Terminology: Let R be an integral domain.

1. A non-unit element $x \in R$ is called irreducible if whenever $x = ab$ in R, either a or b is a unit.
2. A non-unit element $x \in R$ is called prime if, whenever p divides ab, either p divides a or p divides b. Equivalently, p is prime if the ideal pR is a prime ideal.
3. Two elements a and b are called associates in R if there is a unit in R such that $a = bu$.

Lemma: If R is an integral domain, then every prime is irreducible. If R is a principal ideal domain, then the converse is true.

Definition: A unique factorization domain (UFD) is an integral domain such that every nonzero element $r \in R$ which is not a unit is a product

$$r = p_1 p_2 \cdots p_n$$

where the p_i are (not necessarily distinct) irreducible elements of R and, if $r = q_1 q_2 \cdots q_k$ is another such factorization, then there is a rearrangement of the q_i so that q_i and p_i are associates.

Lemma: in a UFD, p is prime if and only if it is irreducible.

Lemma: A UFD has greatest common divisors (computed using the factorization into primes as in $\mathbb{Z}$).

Theorem: A principal ideal domain is a UFD.