Math 510B Notes

Peter Kagey

Wednesday, January 9, 2019

Definition. Let R be a commutative domain with unity. Then R is called Euclidean if it has a "division algorithm". This is, there exists $\phi\colon R - \{0\} \to \mathbb{N}$ satisfying

1. $\phi(a) \leq \phi(ab)$ if $ab \neq 0$, and
2. $a = qb + r$ with $\phi(r) < \phi(b)$ for some $q, r \in R$ if $a, b \neq 0$.

Examples.

1. If $R = \mathbb{Z}$, then $\phi(a) = |a|$.
2. If $R = k[x]$, then $\phi(f) = \deg(f)$

Lemma. If R is Euclidean then R is a PID.

Proof. Need to show any ideal $I \subset R$ is principal. First, if $I = \langle 0 \rangle$, we're done. Otherwise I contains a nonzero element. Pick such an element $b \neq 0$ such that $\phi(a)$ is minimal. If a is another nonzero element, then $a = qb + r$ where $\phi(r) < \phi(b)$, so $r = 0$. Thus $b = qa \in \langle a \rangle = I$. $\square$

Example. Let $F = \mathbb{Q}(\sqrt{m})$, and let $\mathcal{O}_F = \{a \in F : a \text{ is integral over } \mathbb{Z}\}$.

1. If $m \cong 2, 3 \mod 4$, then $\mathcal{O}_F = \mathbb{Z} \oplus \mathbb{Z}(\sqrt{m})$.
2. if $m \cong 1 \mod 4$, then $\mathcal{O}_F = \mathbb{Z} \oplus \mathbb{Z}(1/2 + \sqrt{m}/2)$.

Note. An element $a \in \mathbb{Q}(\sqrt{m})$ is integral over $\mathbb{Z}$ if there exists $\alpha_i \in \mathbb{Z}$ such that $a^k + \alpha_{k-1}a^{k-1} + \ldots + \alpha_0 = 0$

Note. A048981 gives the twenty one values of m such that $\mathcal{O}_F$ is Euclidean.

Lemma. Let R be a PID, then greatest common divisors exist, and given $a, b \neq 0$ and $d = \gcd(a, b)$ (...?)

Proof. Omitted. $\square$

Corollary If R is Euclidean is it a PID, so it has greatest common divisors as usual.

Theorem. Let R be an integral domain. Then R is a UFD if and only if

(a) R has an ascending chain condition on principal ideals. (That is, every chain $\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \ldots$ is eventually constant.)

(b) Irreducible elements are prime. (i.e. if $p | ab$ then $p | a$ or $p | b$.)

Proof.
($\Longrightarrow$) Assume R is a UFD.
Proof of (a). First note that for any $a, b \in R$, $\langle a \rangle \subseteq \langle b \rangle$ if and only if $b | a$. So suppose there is a chain of principal ideals $\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \ldots$; since $a_{i+1} | a_i$, we can write $a_{i+1} = p_1 \ldots p_n$ and write $a_i = up_{j_1} \ldots p_{j_k}$ where u is a unit and $k \leq n$. Therefore the number of prime factors of the generators weakly decreases, and so the chain must eventually stop or become constant.

Proof of (b). Assume a is irreducible, and assume $a|bc$ where $b = p_1 \cdots p_r$ and $c = q_1 \cdots q_s$; that is, there exists $x \in R$ such that $xa = bc = p_1 \cdots p_r q_1 \cdots q_s$. Since a is irreducible, $a = up_i$ or $a = uq_i$, so either $a|b$ or $a|c$.

($\Longleftarrow$) Assume (a) and (b).
Existence. Let $\mathcal{S} = \{a \in R : a \text{ is not the product of irreducible polynomials}\}$. Then assume for the sake of contradiction that $a \in \mathcal{S}$ is chosen so that $\langle a \rangle$ is maximal among the ideals $\langle b \rangle$, which can be done by (1). But since $a \in \mathcal{S}$, a is not irreducible (or else is could be written as the one-term product a) so it factors as $a = a_1 \cdots a_k$. But since $a \in \mathcal{S}$ was chosen so that $\langle a \rangle$ is maximal, and $\langle a \rangle \subset \langle a_i \rangle$, $a_i \notin \mathcal{S}$, and so can be written as a product of irreducible elements, and thus a can be written as a product of irreducible elements. Thus $a \notin \mathcal{S}$ so $\mathcal{S} = \emptyset$.

Uniqueness. Say $a = q_1 \ldots q_s = p_1 \ldots p_r$ where p_i and q_i are irreducible. By (2) this means p_i and q_i are prime, so since $p_1|a$, $p_1|q_1 \ldots q_s \ldots q_s$. In particular, after relabeling, $q_1 = u_1 p_1$. By the cancellation property, it follows that $q_2 \ldots q_s = u_1 p_2 \ldots p_r$. By induction, it follows that $s = r$ and $q_i = u_i p_i$ for all i with u_i unit. $\square$