Math 510B Notes

Peter Kagey

January 15, 2019

Corollary. If R is a principal ideal domain (PID) then R is also a unique factorization domain (UFD).

Proof. It is sufficient to show that a PID satisfies the hypotheses of the previous theorem.
Proof of (a). Assume that $\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \ldots$ is a chain of (principal) ideals. Then define the ideal $I = \bigcup_{i \geq 1} \langle a_i \rangle$. Since R is a PID, $I = \langle b \rangle$ for some b. Since there exists some m such that $b \in \langle a_m \rangle$, $I = \langle a_m \rangle$, so the chain is constant after $\langle a_m \rangle$.

Proof of (b) (similar to argument for $\mathbb{Z}$). Assume that p is irreducible, and $p \mid ab$. If $p \mid a$, then we're done, so assume $p \nmid a$. Since p is irreducible, $\gcd(p, a) = 1$, so there exist $x, y \in R$ such that $xp + ya = 1$ and thus $xpb + yab = b$ since $p \mid ab$, p can be factored from the left-hand side, and thus $p \mid b$, and p is prime. ☐

Note. Euclidean domains (e.g. $\mathbb{Z}[i]$) are PIDs and PIDs are UFDs.

Theorem. If D is a UFD then so it $D[x]$.

Corollary. Let k be a field. Then the ring $k[x_1, x_2, \ldots, x_n]$ is a UFD.

Lemmas.

1. If D is an integral domain then so is $D[x]$.
2. If D is a UFD then greatest common divisors exist.

Proof.

1. Assume that $p(x) \cdot q(x) = 0$. For the sake of contradiction, assume we can write each polynomial as

$$\underbrace{(a_n x^n + \ldots + a_0)}_{p(x)}\underbrace{(b_m x^m + \ldots + b_0)}_{q(x)} = a_n b_m x^{n+m} + \ldots + a_0 b_0$$

   with a_n and b_m nonzero. Then since D is an integral domain, $a_n b_m \neq 0$ so $p(x) \cdot q(x)$ has degree $n+m$, and so is nonzero. Thus if $p(x) \cdot q(x) = 0$ either $p(x)$ or $q(x)$ is zero.

2. Given $a, b \neq 0$ look at irreducible factorizations of both, and then $\gcd(a, b)$ is the product of the factors which are the same up to unit.
   (Note: cannot use $\langle a \rangle + \langle b \rangle = \langle d \rangle$ because $\langle a \rangle + \langle b \rangle$ might not be principal.)

☐

Example. The ring $\mathbb{Z}[x]$ is a UFD but not a PID. In particular, the ideal $I = \langle 2, x \rangle$ is not principal. If $\langle 2, x \rangle = \langle f(x) \rangle$ then $2 \in \langle f(x) \rangle$ so $f(x) \in \mathbb{Z}$, but then $x \notin \langle f(x) \rangle$.

Example. The ring $F[x, y]$ with F a UFD is itself a UFD by a previous theorem. Notice that x and y are primes since $R/\langle x \rangle \simeq F[y]$ is a domain, so $\langle x \rangle$ is a prime ideal and thus x is a prime element.

Definitions. Let D be a UFD and let $R = D[x]$.

1. The content $C(f)$ is the gcd of the coefficients of f in D.
   (e.g. If $f(x) = 4x^2 + 6x + 8 \in \mathbb{Z}[x]$, then $C(f) = 2$)

2. The polynomial $f(x)$ is called primitive if $C(f) = 1$.

Note. Any polynomial can be factored as $f(x) = C(f)f_1(x)$ where $f_1(x)$ is primitive.

Lemma. (Gauss's Lemma)
If $f, g \in D[x]$ are both primitive then their product fg is primitive.

Proof. By contrapositive, assume fg is not primitive, that is $C(fg) \neq 1$. Then there exists a prime $p \in D$ such that $p \mid C(fg)$. Consider the homomorphism $\phi\colon D[x] \to D/\langle p \rangle[x]$ which maps all coefficients modulo p. Since p is chosen to be a prime, $D/\langle p \rangle$ is a domain, so $\phi(fg) = \overline{0} = \phi(f)\phi(g)$ implies that $p \mid C(f)$ or $p \mid C(g)$, a contradiction. $\square$

Corollary. The content of a product is the product of the content up to unit. That is, $C(fg) \approx C(f)C(g)$ where $\approx$ means "up to unit".

Fact. Any integral domain D has a field of fractions $K = S/\sim$ where is the set of pairs $S = D \times D$, and $(a, b) \sim (c, d)$ if $ad = bc$.