Math 210A Lecture 26 Notes

Daniel Raban

December 3, 2018

1 Ideals of Localizations, Hilbert's Basis Theorem, and UFDs

1.1 Ideals of localizations

Let R be a commutative ring, and let S be multiplicatively closed. We have a map S^{-1} sending ideals of R to ideals of $S^{-1}R$. This is onto; that is, every ideal of $S^{-1}R$ arises this way. Suppose S has no 0-divisors. Then

$$I \mapsto S^{-1}I \iff I \in S^{-1}I \iff 1 = a/s, a \in I, s \in S \iff I \cap S = \varnothing.$$

Example 1.1. Let $S = S_p$ for p prime. Then $S_p \cap I = \varnothing \iff I \subseteq p$. This is because Rp is ocal; that is, pRp is the unique maximal ideal.

Example 1.2. Let $R = \mathbb{Z}$, and let $p \in \mathbb{Z}$ be prime. Then $\mathbb{Z}_{(p)} = \{a/b : a, b \in \mathbb{Z}, p \nmid b\} \subseteq \mathbb{Q}$. This has ideals $p^n\mathbb{Z}_{(p)}$, where $n \geq 0$.

1.2 Hilbert's basis theorem

Theorem 1.1 (Hilbert's basis theorem)**.** *Let R be a commutative noetherian ring. Then $R[x]$ is noetherian.*

Proof. Let $I \subseteq R[x]$ be an ideal. Let L be the set of leading coefficients of polynomials in I. We claim that L is an ideal of R. If $a \in L$, then a is the leading coefficient of $f \in I$. Then for $r \in R$, then $rf \in I$ has leading coefficient ra or $ra = 0 \in L$. If $a, b \in L$, then $f, g \in I$ with $f(x) = ax^n + \cdots$ and $g(x) = bx^m + \cdots$; without loss of generality, $n \geq m$, so $f + x^{n-m}g = (a + b)x^n + \cdots \in I$. So $a + b \in L$.

Since R is noetherian, $L = (a_1, \dots, a_k)$, where $a_i \in R$. Let $f_i \in I$ have leading coefficients a_i and degree n_i, and let $n = \max\{n_i\}$. Let $L_m \subseteq R$ be the ideal of leading coefficients of polynomials of degree m and 0. Then $L_m = (b_{1,m}, \dots, b_{\ell_m,m})$, since R is noetherian. Let $g_{i,m} \in I$ have degree m and leading coefficient $b_{i,m}$. Now let $J = (f_1, \dots, f_k, g_{1,1} \cdots g_{\ell_0,0}, \dots, g_{1,n}, \dots, g_{\ell_n})$.

We claim that $J = I$. Let $h \in I$ have leading coefficient c. Write $c = \sum_{i=1}^k r_i a_i$ with $r_i \in R$. If $m = \deg(h) > n$, then set $h' = \sum_{i=1}^k r_i x^{m-n_i} f_i$. This has degree m, leading coefficient c, so $\deg(h-h') < m$. Repeat, so we can assume $\deg(h) \le n$. Then there exist $s_1, \dots, s_{\ell_m} \in R$ such that $c = \sum_{i=1}^{\ell_m} s_i b_{i,m}$. So $h - \sum_{i=1}^{\ell_m} s_i g_{i,m}$ has degree $< m$. Repeat until we get degree zero. $\square$

Corollary 1.1. *If R is noetherian, then $R[x_1, \dots, x_n]$ is noetherian.*

Definition 1.1. Let R be a ring. The **center** of R is $Z(R) = \{r \in R : rs = sr\ \forall s \in R\}$.

Definition 1.2. An **algebra** A over a commutative ring R is a ring A and a nonzero homomorphism of rings $R \to Z(A)$.

If R is a field, the homomorphism $R \to Z(A)$ is injective, and A is an R-vector space.

Example 1.3. $F[x_1, \dots, x_n]$ is an algebra over R.

Example 1.4. The quaternions, $\mathbb{H} = \{a + bi + c_j + dl : a, b, c, d \in \mathbb{R}\}$ is an $\mathbb{R}$ algebra. This is not a $\mathbb{C}$-algebra, but it contains $\mathbb{C}$.

Example 1.5. A finitely generated commutative algebra over a field is isomorphic to $F[x_1, \dots, x_n]/I$, where I is an ideal.

Corollary 1.2. *Any finitely generated algebra over a field (which is noetherian) is noetherian (as a ring).*

$F[(x_i)_{i \in I}]$ is the free object on I in the category of commutative F-algebras.

1.3 Unique factorization domains

Example 1.6. $\mathbb{Z}[\sqrt{-5}]$ is not a UFD. $6 = 23 = (1 + \sqrt{-5})(1 - \sqrt{5})$. The only units in $\mathbb{Z}[\sqrt{-5}]$ are ± 1, so these factorizations really are different.

Definition 1.3. Let R be a UFD. An element $d \in R$ is a **gcd** of $a_1, \dots, a_r \in R$ if $d \mid a_i$ for all i and if $d' \mid a_i$ for all i, ten $d' \mid d$.

Lemma 1.1. *Let R be a UFD. Then $a_1, \dots, a_r$ have a gcd.*

Proof. Take $\pi \mid a_1, \dots, a_r$, and consider $a_1 \pi_1^{-1}, \dots, a_r \pi_1^{-1}$. Repeat until there does not exist a $\pi_k \mid a_i \pi_1^{-1} \cdots \pi_{k-1}^{-1}$ for all i. Then $\pi_1 \cdots \pi_{k-1}$ is a gcd. $\square$

Lemma 1.2. *Let R be a UFD. If $a \in R \setminus \{0\}$. Then (a) is maximal iff (a) is prime iff (a) is irreducible.*

Proof. Let $a \notin R^x$. Then the existence of $b, c \notin R^\times$ such that $a = bc$ is equivalent to $(b) \supsetneq (a)$ for some $b \in R \setminus R^\times$. This is equivalent to $(a) \subsetneq I \subsetneq R$, which is equivalent to (a) not being maximal.

The rest is an exercise. $\square$

Theorem 1.2. *A PID is a UFD.*