Math 210A Lecture 27 Notes

Daniel Raban

December 5, 2018

1 Unique Factorization in PIDs and Polynomials, Gauss' Lemma, and Eisenstein's Criterion

1.1 Unique factorization in PIDs

Proposition 1.1. *In a PID, every irreducible element generates a prime ideal.*

Proof. If $a \in R^\times$ is irreducible, then $b \mid a \iff (a) \subsetneq (b) \subsetneq R$. Since R is a PID, a is maximal, and so it is prime. $\square$

Theorem 1.1. *If R is a PID, R is a UFD.*

Proof. Let $a \neq 0$ with $a \notin \mathbb{R}^\times$. If a is irreducible, we are done. Otherwise, write $a = bc$, where b, c are not units. If b, c are not irreducible, break them down into smaller pieces in the same way. Keep doing this until the process stops. Why must it stop? This is because R is noetherian.

For uniqueness of factorizations, suppose that $a = b_1 b_2, \dots b_r = c_1 c_2 \cdots c_s$, where b_i, c_j are irreducible. We want to show that $r = s$, and there exists a permutation $\sigma \in S_r$ such that $b_{\sigma(i)} = c_i u_i$ for some unit u_i for each i. We know that b_1 generates a prime ideal, so $b_1 \mid c_1 \cdots c_r$. So $b_1 \mid c_i$ for some i, and we get that $c_i = b_i v$, where $v \in R^\times$ (since b_1, c_i are irreducible). By induction on r, we are done. $\square$

Is every PID a UFD?

Example 1.1. Look at $k[x, y]$, where k is a field. This is a UFD, but it is not a PID. It is not a PID because the ideal (x, y) is not principal.

1.2 Gauss' lemma and unique factorization of polynomials over a UFD

Theorem 1.2. *If R is a UFD, then so is $R[x]$.*

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

The idea is this: Let $Q(R)$ be the quotient field of R. Then $Q(R)[x]$ is a PID and hence a UFD. We will try to factor the polynomial in $Q(R)[x]$ and bring that factorization back down to $R[x]$.

Definition 1.1. If $f \in R[x]$, the **content** of f is the ideal generated by the gcd of its coefficients.

Example 1.2. If $f = a_0 + a_1 x + \cdots + a_n x^n$, then $c(f) = (\gcd(a_1, \ldots, a_n))$.

Definition 1.2. f is **primitive** if $c(f) = R$.

Lemma 1.1. *If $f \in R[x]$, then $f(x) = cg(x)$, where $c \in R$ and $g(x)$ is primitive.*

Lemma 1.2 (Gauss)**.** *If $f(x), g(x) \in R[x]$ are primitive, so is $f(x)g(x)$.*

Proof. Take π irreducible such that $\pi \mid c(fg)$. Write $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ and $g(x) = b_0 + b_1 x + \cdots + b_m x^m$. Take r, s minimal such that $\pi \nmid b_r, c_s$. Then $f(x)g(x) = a_0 b_0 + \cdots + (a_0 b_{r+s} + a_1 b_{r+s-1} + \cdots + a_r b_s + \cdots + a_{r+s} b_0) x^{r+s} + \cdots$. Then π divides all these terms in the coefficient of x^{r+s} except $a_r b_s$. Then $\pi \mid a_r b_s$, which is a contradiction. $\square$

Proposition 1.2. *Let $f(x) = f(x)h(x)$ with $g, h \in Q(R)[x]$. Then $f(x) = f_1(x)h_1(x)$, where $g_1, h_1 \in R[x]$, $\deg(g_1) = \deg(g)$, and $\deg(h_1) = \deg(h)$.*

Proof. Take $r, s \in R$. Then $rg(x), sh(x) \in R[x]$. Then $rsf(x) = (rg(x))(sh(x))$. Let $g_0 = rg$ and $h - 0 = sh$. Then $f(x) = cf_2(x)$, $g_0(x) = dg_2(x)$, and $h_0(x) = eh_2(x)$, where f_2, g_2, h_2 are primitive. Then $f_2 = g_2 h_2$. $\square$

We can now prove the theorem.

Proof. If $g \in R[x] \subseteq Q(R)[x]$, factor $f(x) = g_1(x) \cdots g_r(x)$ where $g_1, \ldots, g_r \in R[x]$ are irreducible in $Q(R)[x]$. Then $f(x) = ch_1(x) \cdots h_r(x)$, where $c \in R$ and $h_1, \ldots, h_r$ are primitive. Since R is a UFD, $c = \pi_1 \cdots \pi_s$, where the π_1 are irreducibles.

To get uniqueness, let $\pi_1' \cdots \pi_s' h_1'(x) \cdots h_r'(x)$ be another factorization. If we look at the content, we get $(\pi_1 \cdots \pi_s) = (\pi_1' \cdots \pi_s')$. Since R is a sUFD, ss $= s'$. So $(\pi_i) = (\pi'_{\sigma(i)})$ for some σ. We can do the same for the h_i'. $\square$

1.3 Eisenstein's criterion

How can we tell if $f(x) \in k[x]$ is irreducible?

Theorem 1.3 (Eisenstein)**.** *Suppose $f \in R[x]$, and let $\mathfrak{p} \subseteq R$ be a prime ideal. Write $f(x) = a_0 + \cdots + a_n x^n$. Assume $a_0, \ldots, a_{n-1} \in \mathfrak{p}$ but $a_0 \notin \mathfrak{p}^2$ and $a_n \notin \mathfrak{p}$. Then f is irreducible.*

Proof. Let $\overline{f}(x) \in (R/\mathfrak{p})[x]$. Then $\overline{f}(x) = \overline{a}_n x^n$. If $g(x)h(x) = f(x)$, then $\overline{g}(x)\overline{h}(x) = \overline{f}(x) = \overline{a}_n x^n$. Then $\overline{g}(x) = \overline{b}_m x^m$ and $\overline{h}(x) = \overline{c}_k x^k$ with $m, k > 0$. This is a contradiction. □

Example 1.3. Look at the cyclotomic polynomial $\Phi_p = 1 + x + \cdots + x^{p-1} = (x^p - 1)/x - 1$. Then $\Phi_p(x+1) = (x^{p-1} + px^{p-2} + \cdots + p$, so it is irreducible.