M622 notes, 02.13

Proposition 0.1 Eisenstein's Criterion: *Suppose R is an integral domain with a prime ideal P, and $b(x) = x^m + b_{m-1}x^{m-1} + \ldots + b_0$ is a monic polynomial with coefficients in R satisfying $\{b_0, \ldots, b_{m-1}\} \subseteq P$ and $b_0 \notin P^2$. Then $b(x)$ is irreducible.*

(Recall that prime ideals are, by definition, proper ideals.)

Proof. Contradiction. Suppose $b(x) = c(x)e(x)$, a non-trivial factorization of $b(x)$. Since $b(x)$ is monic, neither $c(x)$ nor $e(x)$ can be constants (i.e., degree 0): for example, if $c(x) = c$ is constant, then its productis awith the leading coefficient of $e(x)$ would be 1 (since $b(x)$ is monic). But $c(x) = c$ is a unit of R and of $R[x]$, and the factorization $b(x) = c(x)e(x)$ is a trivial factorization.

$deg(b(x)) > \max(deg(c(x), deg(e(x)))$. Let $c(x) = c_k x^k + \ldots + c_0$ and let $e(x) = e_j x^j + \ldots + e_0$. So $c_0 e_0 = b_0 \in P - P^2$. That P is a prime ideal implies that exactly one of $\{c_0, e_0\}$ is in P. Without loss of generality, assume $c_0 \in P$ so $e_0 \notin P$. Now consider $b_1 = c_0 e_1 + e_0 c_1$. Since $b_1 \in P$ and $c_0 \in P$, it follows that $e_0 c_1 \in P$. But $e_0 \notin P$ and that P is prime implies that $c_1 \in P$.

The claim is that for $i = 0, \ldots, k-1$, c_i is in P, a claim proved by induction. The base step is proven—in fact both c_0 and c_1 are in P. Suppose that there exists a positive integer j such that for all i such that $j > i$, $c_i \in P$. To complete the induction proof, it must be shown that $c_j \in P$. We have $b_j = c_0 e_j + c_1 e_{j-1} + \ldots c_j e_0 (= \sum_{n=0}^{n=j} c_n e_{j-n})$. By the induction hypothesis, and using that P is an ideal and that $b_j \in P$, it follows that $c_j e_0 \in P$. Since $e_0 \notin P$ (see above) and P is prime, we have $c_j \in P$. This completes the proof of the claim.

But now $c_k \in P$, and $b_m = c_k e_{m-k}$ implies that $b_m \in P$. However, $b(x)$ is monic, so $b_m = 1$, and we have $1 \in P$. Of course $1 \in P$ implies $P = R$, and P is not proper, a contradiction. This completes the proof. $\square$

The following comes out of the proof above.

Lemma 0.2 Eisenstein's Criterion 2 *If R is a PID, P is a prime ideal of R, $b(x) = b_m x^m + \ldots + b_0 \in R[x]$ with $\{b_0, \ldots, b_{m-1}\} \subseteq P$, $b_0 \notin P^2$, and $gcd(b_0, \ldots, b_m\} = 1$, then $b(x)$ is irreducible over R.*

Proof. In the notation of the proof by contradiction above, with $b(x) = c(x)e(x)$, again show that the coefficients of $c(x)$ are all contained in P, and therefore that coefficients of $b(x)$ are all contained in P. Since R is a PID, any finitely generated ideal $I = (r_1, \ldots, r_k)$ is equal to (d), for some $d \in R$ with $d = \gcd(r_1, \ldots, r_k)$. Returning to $b(x)$, $1 = \gcd(b_0, \ldots, b_m)$, $(1) = (b_0, \ldots, b_m) \subseteq P$, contradicting that P is proper. $\square$