Math 254A. An Overly Long Proof of Eisenstein's Criterion

This handout gives a proof of Eisenstein's criterion from the point of view of valued fields.

We start with a lemma.

Lemma. *Let $K = (K, |\cdot|)$ be a non-archimedean valued field, and let*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

be a polynomial in $K[x]$ with $a_n \neq 0$ and $a_0 \neq 0$. Assume that, for all $i = 1, \dots, n-1$, the point $(i, -\log|a_i|)$ lies above or on the line passing through $(0, -\log|a_0|)$ and $(n, -\log|a_n|)$, where we use the convention that $-\log 0 = +\infty$. Then all roots α of f in $\overline{K}$ have absolute value

$$|\alpha| = \sqrt[n]{\frac{|a_0|}{|a_n|}}\,.$$

Proof. Let $R = \sqrt[n]{|a_0|/|a_n|}$.

The line mentioned above has slope $(-\log|a_n| + \log|a_0|)/n$, so the absolute values of the coefficients satisfy

$$-\log|a_i| + \log|a_0| \ge \frac{i}{n}(-\log|a_n| + \log|a_0|)\,;$$
$$-\log|a_i| \ge -\frac{i}{n}\log|a_n| - \frac{n-i}{n}\log|a_0|\,;$$

hence

$$-\log\frac{|a_i|}{|a_n|} \ge -\frac{n-i}{n}\log\frac{|a_0|}{|a_n|} \qquad \text{and} \qquad -\log\frac{|a_i|}{|a_0|} \ge -\frac{i}{n}\log\frac{|a_n|}{|a_0|}\,.$$

Now we claim that $|\alpha| \le R$. Indeed, suppose $|\alpha| > R$. Then

$$\frac{|a_i\alpha^i|}{|a_n\alpha^n|} \le \left|\frac{a_0}{a_n}\right|^{(n-i)/n} = \left(\frac{R}{\alpha}\right)^{n-i} < 1$$

for all $i < n$, so

$$|a_{n-1}\alpha^{n-1} + \cdots + a_0| < |a_n\alpha^n|\,,$$

contradicting the fact that $f(\alpha) = 0$.

Similarly, $|\alpha| \ge R$, because if $|\alpha < R$ then

$$\frac{a_i\alpha^i}{a_0} \le \left|\frac{a_n}{a_0}\right|^{i/n}|\alpha|^i = \left(\frac{\alpha}{R}\right)^i < 1$$

for all $i > 0$, so

$$|a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha| < |a_0|\,,$$

and again this contradicts $f(\alpha) = 0$. □

(This is part of the standard theory of Newton polygons. So far, it says nothing about f being irreducible. In fact, K could be algebraically closed.)

Now let A be a factorial ring, and let K be its fraction field. Let $p \in A$ be an irreducible element. Then (p) is a prime ideal, and the corresponding local ring $A_{(p)}$ is a dvr, hence is Dedekind. Let $v\colon K \twoheadrightarrow \mathbb{Z} \cup \{\infty\}$ be the corresponding valuation. Let $f \in A[x]$ be a polynomial that satisfies the hypotheses of Eisenstein's criterion for p. Write $f(x) = a_n x^n + \cdots + a_0$ as in the lemma; we then have that $v(a_n) = 0$, $v(a_i) > 0$ for all $i < n$, and $v(a_0) = 1$.

Let $\widehat{K}$ be the completion of K relative to v; this is a cdvf. Let α be a root of f in an algebraic closure of $\widehat{K}$. As 1 is the minimum positive value of v, f satisfies the hypotheses of the lemma, so $v(\alpha) = 1/n$. Let $\widehat{L} = \widehat{K}(\alpha)$, and let $\mathfrak{p}$ and $\mathfrak{q}$ be the valuation ideals of $\widehat{K}$ and $\widehat{L}$, respectively. Then, since $v(\alpha) = 1/n$, the ramification index $e = e_{\mathfrak{q}/\mathfrak{p}}$ of $\widehat{L}/\widehat{K}$ satisfies $e \ge n$, and therefore

$$n \ge [\widehat{L} : \widehat{K}] = e_{\mathfrak{q}/\mathfrak{p}} f_{\mathfrak{q}/\mathfrak{p}} \ge e_{\mathfrak{q}/\mathfrak{p}} \ge n\ .$$

Therefore equality must hold at every step, so in particular $[\widehat{L} : \widehat{K}] = n$, which implies that f is irreducible over $\widehat{K}$. It is therefore also irreducible over K, and we are done.

Admittedly, this is quite a bit longer than the usual proof of Eisenstein's criterion. However, there are some proofs that provide insights into why something is true, and there are other proofs that tell you that the theorem is true (and nothing more). This proof falls into the former category, because it shows that Eisenstein polynomials are associated to totally ramified extensions.