Roots of Polynomials.

12/03/06 Radford

Throughout R is a commutative ring with unity.

1 Fractional Roots and the Eisenstein Criterion

Suppose that $p, q \in R$ and the ideals $(p) = Rp, (q) = Rq$ are comaximal. Then $R = Rp + Rq$ which means that $1 = ap + bq$ for some $a, b \in R$. Thus if $c \in R$ and $p|qc$ then $p|c$ as $c = 1c = apc + bqc$. When R is a Principal Ideal Domain to say that (p) and (q) are comaximal is the same as saying that 1 is a greatest common divisor of p and q.

Lemma 1 *Let R be an integral domain, let F be its field of quotients, and let $f(X) = a_nX^n + \cdots + a_0 \in R[X]$. Suppose $p, q \in R$, where $q \neq 0$ and $(p), (q)$ are comaximal, and $r = p/q$ is a root of $f(X)$ in F. Then $p|a_0$ and $q|a_n$.*

PROOF: Multiplying both sides of the equation

$$a_n(p/q)^n + \cdots + a_0 = 0$$

by q^n yields the equation $a_np^n + a_{n-1}p^{n-1}q + \cdots + a_0q^n = 0$ in R. Therefore

$$p(a_np^{n-1} + a_{n-1}p^{n-2}q + \cdots + a_1q^{n-1}) = -a_0q^n$$

and

$$a_np^n = -(a_{n-1}p^{n-1} + \cdots + a_0q^{n-1})q$$

which means $p|a_0q^n$ and $q|a_np^n$ from which $p|a_0$ and $q|a_n$ follow. $\Box$

Here is a version of the Eisenstein Criterion.

Lemma 2 *Let R be an integral domain and $f(X) = a_nX^n + \cdots + a_0 \in R[X]$ be primitive. Suppose that $p \in R$ is a prime such that:*

(1) *p does not divide a_n;*

(2) *p divides a_i for all $0 \leq i < n$; and*

(3) *p^2 does not divide a_0.*

Then $f(X)$ is irreducible.

PROOF: Consider a factorization $f(X) = q(X)r(X)$, where $q(X) = b_\ell X^\ell + \cdots + b_0$ and $r(X) = c_mX^m + \cdots + c_0$ are polynomials of degrees ℓ and m respectively. We need to show one of $q(X), r(X)$ is a unit.

Since $b_\ell c_m \neq 0$, we conclude $\ell + m = n$ and $a_n = b_\ell c_m$. In any event $a_0 = b_0c_0$. Note p does not divide b_ℓ, c_m by (1) and one of b_0, c_0 is not divisible by p by (3). Without loss of generality we may assume that p does not divide b_0.

Since p is prime Rp is a prime ideal of R. Therefore R/Rp is an integral domain. Consider the ring homomorphism $R[X] \longrightarrow (R/Rp)[X]$ defined by

$$d(X) = d_sX^s + \cdots + d_0 \mapsto (d_s + Rp)X^s + \cdots + (d_0 + Rp) = \overline{d_s}X^s + \cdots + \overline{d_0} = \overline{d(X)},$$

where $\overline{r} = r + Rp$ for all $r \in R$. Since the leading coefficient of $q(X)$ is not divisible by p we conclude that $\mathrm{Deg}\, q(X) = \mathrm{Deg}\, \overline{q(X)}$. Now

$$\overline{a_n}X^n = \overline{f(X)} = \overline{q(X)r(X)} = \overline{q(X)}\;\overline{r(X)}.$$

Therefore $\overline{q(X)}$ has one term since this is true when the polynomial is regarded as a polynomial over the field of quotients of R/Rp. Since p does not divide b_0 it follows that $\overline{q(X)}$ has a non-zero constant term. Therefore $0 = \mathrm{Deg}\, \overline{q(X)} = \mathrm{Deg}\, q(X)$ which means that $q(X)$ is a constant polynomial. Since $f(X)$ is primitive $g(X)$ is a unit. We have shown that $f(X)$ is irreducible. $\square$

2 A Ring Extension with a Root of $f(X)$

Let $f(X) = a_nX^n + \cdots + a_0$ and $g(X) = b_mX^m + \cdots + b_0$ be polynomials in $R[X]$ and suppose that $f(X)$ has degree n. Since $f(X)g(X) = a_nb_mX^{n+m} +$

$\cdots + a_0 b_0$ it follows that $\operatorname{Deg} f(X)g(X) = \operatorname{Deg} f(X) + \operatorname{Deg} g(X)$ for all $g(X) \in R[X]$ if and only if a_n is not a zero divisor. When $a_n = 1$ the division algorithm holds for $f(X)$.

Lemma 3 *Suppose that $f(X) = X^n + \cdots + a_0 \in R[X]$, where $n \geq 0$. Then for $g(X) \in R[X]$ there are $q(X), r(X) \in R[X]$ such that*

$$g(X) = q(X)f(X) + r(X),$$

where $r(X) = 0$ or $\operatorname{Deg} r(X) < \operatorname{Deg} f(X)$. Furthermore $q(X), r(X)$ are determined by these conditions.

PROOF: Mimic the proof of the Division Algorithm when R is a field. $\Box$

The Division Algorithm holds when $a_n \in R^\times$ by an easy reduction to the monic case.

Suppose that $f(X) = X^n + \cdots + a_0 \in R[X]$, where $n \geq 1$, and let $I = (f(X))$. Then an element of I is either zero of has degree greater than or equal to n. Let

$$\mathcal{R} = R[X]/I$$

and

$$\mathcal{S} = \{r(X) \in R[X] \mid r(X) = 0 \text{ or } \operatorname{Deg} r(X) < n\}.$$

The map $j : \mathcal{S} \longrightarrow \mathcal{R}$ defined by $j(r(X)) = r(X) + I$ is bijective. It is surjective by Lemma 3. Suppose that $r(X), r'(X) \in \mathcal{S}$ and $j(r(X)) = j(r'(X))$. Then $r(X) + I = r'(X) + I$ or equivalently $r(X) - r'(X) \in I$. But the difference $r(X) - r'(X)$ is zero or has degree less than n. Since an element of I is zero or has degree greater than or equal to n, necessarily $r(X) - r'(X) = 0$. Therefore $r(X) = r'(X)$ which establishes the injectivity of j. Observe that the restriction $i = j|R$ is in fact an injection of rings.

We regard R as a subring of $\mathcal{R}$ via the identification of $r \in R$ with $j(r) = r + I$. Let $\alpha = X + I$ and $r(X) = b_{n-1}X^{n-1} + \cdots + b_0 \in \mathcal{S}$. Then

$$\begin{aligned} r(X) + I &= (b_{n-1}X^{n-1} + \cdots + b_0) + I \\ &= (b_{n-1} + I)(X + I)^{n-1} + \cdots + (b_0 + I) \\ &= b_{n-1}\alpha^{n-1} + \cdots + b_0 \\ &= r(\alpha). \end{aligned}$$

Observe that

$$f(\alpha) = \alpha^n + \cdots + a_0 = (X + I)^n + \cdots + (a_0 + I) = f(X) + I = I;$$

thus α is a root of $f(X)$ in $\mathcal{R}$.

Proposition 1 *Suppose that R is a commutative ring with unity and $f(X) = X^n + \cdots + a_0 \in R[X]$, where $n \geq 1$. Then there is a commutative ring with unity $\mathcal{R}$ which contains R as a subring, and an element $\alpha \in \mathcal{R}$, such that:*

(1) $f(\alpha) = 0$;

(2) *each element of $\mathcal{R}$ has a unique expression as $b_{n-1}\alpha^{n-1} + \cdots + b_0$, where $b_{n-1}, \ldots, b_0 \in R$; and*

(3) *if $f(X)$ is irreducible and R is a field then $\mathcal{R}$ is a field.*

PROOF: In light of the comments preceding the proposition, we need only establish part (3). Suppose that $f(X)$ is irreducible and R is a field. Since R is a subring of $\mathcal{R}$ there is a ring homomorphism $F : R[X] \longrightarrow \mathcal{R}$ determined by $F(r) = r$ for all $r \in R$ and $F(X) = \alpha$. Thus F is substitution of α for X. Observe that F is surjective. Since $F(f(X)) = f(\alpha) = 0$ it follows that $f(X) \in \operatorname{Ker} F$. Since $\operatorname{Ker} F$ is an ideal of $R[X]$ it follows that $(f(X)) \subseteq \operatorname{Ker} F$.

We will show that $(f(X)) = \operatorname{Ker} F$ by showing that $\operatorname{Ker} F \subseteq (f(X))$. Let $g(X) \in \operatorname{Ker} F$. By the Division Algorithm there are $q(X), r(X) \in R[X]$ such that $g(X) = q(X)f(X) + r(X)$, where $r(X) = 0$ or $\operatorname{Deg} r(X) < \operatorname{Deg} f(X) = n$. Now $r(X) = g(X) + (-q(X))f(X) \in \operatorname{Ker} F$. Writing $r(X) = b_{n-1}X^{n-1} + \cdots + b_0$ we have $b_{n-1}\alpha^{n-1} + \cdots + b_0 = F(r(X)) = 0$. By uniqueness of expression $b_{n-1} = \cdots = b_0 = 0$ from which we conclude $r(X) = 0$. Therefore $g(X) = q(X)f(X) \in \operatorname{Ker} F$.

By the First Isomorphism Theorem for rings $R[X]/(f(X)) \simeq \mathcal{R}$. Since $f(X)$ is irreducible and $R[X]$ is a Principal Ideal Domain $(f(X))$ is a maximal ideal of $R[X]$. Therefore the quotient $R[X]/(f(X)) = \mathcal{R}$ is a field. $\square$