I.E. Multiple roots

Let K be a field. Given an irreducible polynomial $f \in K[x]$, there exists a splitting field extension L/K (cf. I.C.5). So we can write

$$f(x) = \prod_i (x - r_i)^{k_i}$$

in $L[x]$, with the $r_i \in L$ *distinct*. If $k_i = 1$, then r_i is a **simple root**; otherwise, r_i is a **multiple root**.

When we vary the choice of splitting field extension, the multiplicities k_i do not change, since any two such extensions are isomorphic over K (cf. I.C.20). So the property of having simple roots, or of possessing a multiple root, may be regarded as a well-defined attribute of $f \in K[x]$, without reference to a splitting field.

Given distinct monic irreducible polynomials $f, g \in K[x]$, we have $\gcd(f, g) \sim 1$ hence $Ff + Gg = 1$ for some $F, G \in K[x]$. Since $0 \neq 1$, f and g can have no common root in a splitting field for fg; and we arrive at the

I.E.1. PROPOSITION. *Given a finite collection of distinct monic irreducible polynomials, each with simple roots, their product has simple roots.*

But this still begs the question of when an irreducible polynomial has multiple roots!

The standard derivation.

One way to detect these is by taking derivatives. For any polynomial $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in K[x]$, set

$$f' \text{ (or } Df) := a_1 + 2a_2 x + \cdots + n a_n x^{n-1},$$

thereby obtaining a K-linear map $D\colon K[x] \to K[x]$.

I.E.2. PROPOSITION. *We have*

$$f(x+h) \underset{(h^2)}{\equiv} f(x) + f'(x)h$$

in $K[x][h]/(h^2)$.

PROOF. By K-linearity, it suffices to check this on a monomial: $(x+h)^n = \sum_{j=0}^{n} \binom{n}{j} x^j h^{n-j} \underset{(h^2)}{\equiv} x^n + nx^{n-1}h$. $\square$

From this it follows that

$$\begin{aligned}(fg)(x+h) = f(x+h)g(x+h) &\underset{(h^2)}{\equiv} (f+f'h)(g+g'h) \\ &= fg + (f'g+g'f)h,\end{aligned}$$

whence $(fg)' = f'g + g'f$.

I.E.3. THEOREM. *Suppose $f \in K[x] \setminus \{0\}$, with splitting field L/K. Then the following are equivalent:*

(i) *f has a multiple root (in L).*
(ii) *$\exists\, \alpha \in L$ such that $f(\alpha) = f'(\alpha) = 0$.*
(iii) *$\exists\, g \in K[x]$ of positive degree, with $g \mid f, f'$.*
(iv) $\gcd(f, f') \nsim 1$.

PROOF. Clearly (iii) and (iv) are equivalent.

<u>(i) $\implies$ (ii)</u>: If $f = (x-\alpha)^k F$ with $k > 1$, then $f' = k(x-\alpha)^{k-1}F + (x-\alpha)^k F'$.

<u>(ii) $\implies$ (iii)</u>: The minimal polynomial m_α over K divides f, f'.

<u>(iii) $\implies$ (i)</u>: Since $g \mid f$ and f splits over L, so does g. That is, g has a root $\alpha \in L$; and writing $f = (x-\alpha)q$ in $L[x]$, we get $f' = q + (x-\alpha)q'$. Together with $(x-\alpha) \mid g \mid f'$, this gives $(x-\alpha) \mid q$ hence $(x-\alpha)^2 \mid f$. $\square$

I.E.4. DEFINITION. (i) An irreducible polynomial $f \in K[x]$ is **separable** over K if f has no multiple roots. (Equivalently: f has $\deg(f)$ distinct roots in a splitting field; or $\gcd(f, f') \sim 1$.)
(ii) An arbitrary polynomial $f \in K[x]$ is **separable** over K if each of its irreducible factors is.
(iii) K is **perfect** if every polynomial $f \in K[x]$ is separable over K.

It is immediate from the definition that any algebraically closed field is perfect (why?). Slightly less obvious is the

I.E.5. COROLLARY. *Any field of characteristic zero is perfect.*

PROOF. Let $f \in K[x]$ be irreducible (hence of positive degree), with $\gcd(f, f') \not\sim 1$. Since f is irreducible, the only other possibility[15] is $\gcd(f, f') \sim f$, i.e. $f \mid f'$. Since $\deg(f') < \deg(f)$, this forces $f' = 0$.

But if $\mathrm{char}(K) = 0$, then $f' = 0 \implies f \in K$, a contradiction. $\square$

The argument shows more: if $f = \sum_{j=0}^{n} a_j x^j \in K[x]$ is irreducible, and $\mathrm{char}(K) = p > 0$, then

$$\begin{aligned} f \text{ is inseparable} \iff f' = 0 \iff ja_j = 0 \in K\ (\forall j) \\ \iff f(x) = b_0 + b_1 x^p + \cdots + b_m x^{mp} = g(x^p) \\ \text{(for some } g \in K[x]). \end{aligned} \tag{I.E.6}$$

We would like to see if we can prove "perfection" of any positive characteristic fields. To see what can go wrong, let us first show that

I.E.7. THEOREM. *$x^p - t$ is inseparable over $\mathbb{Z}_p(t)$.*

We will first require a

I.E.8. LEMMA. *Given $\alpha \in K$ and $\mathrm{char}(K) = p > 0$, the polynomial $x^p - \alpha$ is either irreducible or a p^{th} power in $K[x]$.*

PROOF. Say $f := x^p - \alpha$ is not irreducible, factoring as GH over K, with G monic of degree $e \neq 0, p$. Let $\beta \in L$ be a root of G in a splitting field of f. Then $\beta^p = \alpha \implies GH = x^p - \alpha = x^p - \beta^p = (x - \beta)^p \implies G = (x - \beta)^e$. Moreover, since $G \in K[x]$, we have $\beta^e \in K$. Now $\gcd(e, p) = 1 \implies ae + bp = 1$ (for some $a, b \in \mathbb{Z}$) $\implies \beta = (\beta^e)^a (\beta^p)^b \in K$. But then $x^p - \alpha = (x - \beta)^p$ works in $K[x]$, i.e. f is a p^{th} power. $\square$

PROOF OF I.E.7. Suppose $x^p - t$ is reducible in $\mathbb{Z}_p(t)[x]$. By the Lemma, it takes the form $(x - \beta)^p$ in $\mathbb{Z}_p(t)[x]$, thus has a root $\beta \in$

[15] Why? Write $f = gh$, $f' = gH$; then irreducibility of f means that g or h is a unit (i.e. constant). We've assumed g (i.e. $\gcd(f, f')$) nonconstant, so $h \in K^*$ and $g \sim f$.

$\mathbb{Z}_p(t)$. That is, $t = \beta^p = (\frac{F(t)}{G(t)})^p = (\frac{a_0+a_1t+\cdots+a_nt^n}{b_0+b_1t+\cdots+b_mt^m})^p$ for some $F, G \in \mathbb{Z}_p[t]$, $G \neq 0$. Then $tG^p = F^p$ reads

$$t(b_0^p + b_1^p t^p + \cdots + b_m^p t^{mp}) = a_0^p + a_1^p t^p + \cdots + a_n^p t^{np}$$

in $\mathbb{Z}_p[t]$, which forces every $b_i^p = 0$ hence every $b_i = 0$, which is absurd.

So $x^p - t$ is irreducible in $\mathbb{Z}_p(t)[x]$. But the Lemma *also* shows that it is a p^{th} power in a splitting field, hence has a multiple root. $\square$

The Frobenius map.

To prove any positive results about separability in positive characteristic, begin with the

I.E.9. PROPOSITION. *For K of characteristic $p > 0$, the* ***Frobenius map***

$$\phi\colon K \to K$$
$$\alpha \mapsto \alpha^p$$

is an injective homomorphism with fixed point set equal to the prime subfield: that is, $K^\phi = \imath(\mathbb{Z}_p)$.

PROOF. Obviously $\phi(\alpha\beta) = \phi(\alpha)\phi(\beta)$ and $\phi(1) = 1$, while $\phi(\alpha + \beta) = \phi(\alpha) + \phi(\beta)$ works by the binomial formula/freshman's dream (p divides $\binom{p}{j}$ for $j = 1, \ldots, p-1$). It is injective because it is a field homomorphism. The fixed elements contain the prime subfield $\imath(\mathbb{Z}_p)$ by little Fermat. There can't be more fixed elements because $x^p - x$ can have at most p distinct roots. $\square$

I.E.10. COROLLARY. *If K is algebraic over $\mathbb{Z}_p$,*[16] *then $\phi \in \mathrm{Aut}(K)$.*

PROOF. This is I.A.23; the argument is so simple and important we will repeat it. Given $\alpha \in K$, with minimal polynomial $m_\alpha \in \mathbb{Z}_p[x]$, and r any root of m_α in K, we have $m_\alpha(\phi(r)) = \phi(m_\alpha(r)) = 0$. So ϕ permutes the roots of m_α; in particular, $\alpha \in \phi(K)$. $\square$

[16]Note that in this case $\mathrm{char}(K) = p$, since it contains $\mathbb{Z}_p$ and this is then its prime subfield.

I.E.11. PROPOSITION. *Given K of characteristic $p > 0$, let $f(x) = g(x^p) \in K[x]$, with $g(x) = \sum_{j=0}^{m} b_j x^j$. Then $f(x)$ is irreducible $\iff$ $g(x)$ is irreducible and not all $b_i \in \phi(K)$.*[17]

PROOF. ($\implies$): If $g = g_1 g_2$, then $f(x) = g_1(x^p) g_2(x^p)$. If $b_i = c_i^p$ $(\forall i)$, then $f = c_0^p + \cdots + c_m^p x^{mp} = (c_0 + c_1 x + \cdots + c_m x^m)^p$. So neither can happen when f is irreducible.

($\impliedby$): Suppose $f = f_1^{\ell_1} \cdots f_r^{\ell_r}$ as a product of relatively prime irreducibles, with $\ell_1 + \cdots + \ell_r > 1$. Note that $f(x) = g(x^p) \implies f' = 0$. We must show g is reducible or that all b_i are p^{th} powers.

Case 1: $r > 1$. Write $f = h_1 h_2$, with h_1, h_2 coprime. This yields $H_1 h_1 + H_2 h_2 = 1$ and $0 = f' = h_1' h_2 + h_2' h_1$ in $K[x]$, whence

$$H_1 h_1' h_1 - H_2 h_2' h_1 = H_1 h_1' h_1 + H_2 h_1' h_2 = h_1'(H_1 h_1 + H_2 h_2) = h_1',$$

which shows that $h_1 \mid h_1'$. Since $\deg(h_1) > \deg(h_1')$, we must have $h_1' = 0$; the same argument gives $h_2' = 0$. So $h_i(x) = g_i(x^p)$ for $i = 1, 2$ (and $g_i \in K[x]$), and $g = g_1 g_2$ is reducible.

Case 2: $r = 1$. Here $f = f_1^{\ell}$, with $\ell > 1$ and f_1 irreducible. If $p \mid \ell$, then the coefficients of $f = (f_1^{\ell/p})^p$ are p^{th} powers by the usual freshman's dream. So suppose $p \nmid \ell$, and reason that that $0 = f' = \ell f_1' f_1^{\ell - 1} \implies f_1' = 0 \implies f_1(x) = g_1(x^p)$ for some $g_1 \in K[x] \implies g(x^p) = f(x) = (g_1(x^p))^{\ell} \implies g = g_1^{\ell}$ is again reducible. $\square$

I.E.12. THEOREM. *If K is algebraic over $\mathbb{Z}_p$, then K is perfect.*

PROOF. Let $f \in K[x]$ be irreducible. If f is also inseparable, then by (I.E.6) we have $f(x) = g(x^p)$ for some $g \in K[x]$. By I.E.11, $g(x) = \sum_i b_i x^i$ is irreducible with not all $b_i \in \phi(K)$. This contradicts $\phi(K) = K$ (from I.E.10); so f cannot be inseparable. $\square$

I.E.13. COROLLARY. *Every finite field is perfect.*

[17] Alternatively, we could write K^p, since $\phi(K)$ comprises the p^{th} powers of elements in K.