Field and Galois Theory

Lectures by Uzi Vishne
Summary by Ari Feiglin (ari.feiglin@gmail.com)

Contents

1 Field Extensions and Minimal Polynomials

1.1 Dimensions of Field Extensions

1.1.1 Definition

Suppose F and K are fields such that $F \subseteq K$. Then the pair is called a **field extension** and is denoted K/F.

Notice that if K/F is a field extension, then K can be viewed as a F-linear space, and thus has a dimension. We denote this dimension $[K : F] := \dim_F K$, this is unsurprisingly called the *dimension* (or *degree* of the extension. An extension is called *finite* if its dimension is finite. Immediately we can prove a useful theorem about dimensions of extensions:

1.1.2 Theorem

Suppose K/F is a field extension and V a K-vector space. Then by viewing V as an F-linear space:

$$\dim_F V = \dim_K V \cdot [K : F]$$

Proof: let B_1 be a basis for V relative to K and B_2 be a basis for K relative to F. Then define $B = \{\alpha v \mid \alpha \in B_2, v \in B_1\} \subseteq V$, which we claim is a basis for V relative to F. Firstly, it is linearly independent: suppose $\alpha_1 v_1, \ldots, \alpha_n v_n$ are in B and $\beta_1, \ldots, \beta_n$ are in F such that

$$\beta_1\alpha_1 v_1 + \cdots + \beta_n\alpha_n v_n = 0$$

Since B_1 is a basis for V, then $\beta_i\alpha_i = 0$ for all i, and since B_2 is a basis it has no zeroes, so $\beta_i = 0$ for all i, meaning B is linearly independent.

B spans V since if $v \in B$ then $v = \sum_{i=1}^{n} \alpha_i v_i$ for $v_i \in B_1$ and $\alpha_i \in K$, and so each α_i can be written as the linear combination of elements in B_2. So all in all v can be written as the linear combination of elements in B. And so B is a basis of V, and $(\alpha, v) \mapsto \alpha v$ is a bijection from $B_1 \times B_2$ to B: it obviously is surjective and if $\alpha_1 v_1 = \alpha_2 v_2$ then $\alpha_1 = \alpha_2$ and $v_1 = v_2$ since B_1 is linearly independent. Thus V is a basis of cardinality $|B_1 \times B_2| = \dim_K V \cdot [K : F]$ as required. ■

In particular if $E/K/F$ are field extensions then

$$[E : F] = [E : K] \cdot [K : F]$$

this is called the *multiplicity of dimension*.

1.2 Constructing Fields

Recall the following methods of constructing fields:

(**1**) If R is a commutative ring and $M \triangleleft R$ is a maximal ideal that R/M is a field. In particular if F is a field, $R = F[x]$, and p is an irreducible polynomial then (p) is maximal and so $F[x]/(p)$ is a field.

(**2**) If F is a field, so is the field of rational functions:

$$F \subseteq F(x) := \left\{ \frac{f(x)}{g(x)} \;\middle|\; f, g \in F[x], g \neq 0 \right\}$$

(**3**) If C is a chain of fields (meaning that for every $F, F' \in C$ either $F \subseteq F'$ or $F' \subseteq F$), then $\bigcup_{F \in C} F$ is also a field (the theory of fields is *inductive*). So for example $F(\lambda_1, \lambda_2, \ldots)$ is a field, the union of the chain $F_n = F(\lambda_1, \ldots, \lambda_n)$, the field of rational functions over F_{n-1}.

(**4**) If C is a chain of fields, then $\bigcap_{F \in C} F$ is also a field.

1.2.1 Definition

Let K/F be a field extension and $a \in K$, then denote $F(a)$ the smallest subfield of K containing both F and a.

It is not hard to see that

$$F(a) = \left\{ \frac{f(a)}{g(a)} \;\middle|\; f, g \in F[x], g(a) \neq 0 \right\}$$

Though we can actually get a simpler structure for $F(a)$.

1.2.2 Definition

Let K/F be a field extension with $a \in K$, then define the **evaluation homomorphism** at a to be the homomorphism $\psi_a \colon F[x] \longrightarrow K$ defined by $\psi_a(s) = s$ for $s \in F$ and $\psi_a(x) = a$. This uniquely defines

$$\psi_a\left(\sum \alpha_i x^i\right) = \sum \alpha_i a^i$$

1.2.3 Definition

Let K/F be a field extension, then $a \in K$ is **transcendental** if the kernel of the evaluation homomorphism is trivial: $\ker \psi_a = 1$. Otherwise a is **algebraic**.

If a is transcendental then $\ker \psi_a = 1$ and so by the isomorphism theorem

$$\mathrm{Im}\psi_a = \{f(a) \mid f \in F[x]\} = F[a] \cong {F[x]}\Big/{\ker \psi_a} \cong F[x]$$

In fact we can extend ψ_a to a homomorphism $F(x) \longrightarrow F(a)$, and we similarly get an isomorphism $F(x) \cong F(a)$. Thus in the case that a is transcendental, we get

$$\begin{array}{ccccccc} F & \subseteq & F[a] & \subseteq & F(a) & \subseteq & K \\ & & \cong & & \cong & & \\ & & F[x] & & F(x) & & \end{array}$$

Otherwise, suppose a is algebraic. Since $F[x]$ is a Euclidean domain, it is a PID, and therefore every ideal is a prime ideal. In particular $\ker \psi_a$ must be generated by some polynomial h_a. This means that $\ker \psi_a = (h_a) = h \cdot F[x]$, and so $h_a(a) = 0$ and if $f(a) = 0$ as well then h_a divides f. h_a is therefore called the *minimal polynomial* of a.

Now if $n = \deg h$ then $F[a] = \mathrm{span}\{1, a, \ldots, a^{n-1}\}$ since if $f \in F[x]$ then $f = h_a q + r$ for $\deg r < n$ by Euclidean division, and so $f(a) = r(a)$. And $r(x)$ is in $\mathrm{span}\{1, \ldots, a^{n-1}\}$ due to its dimension being at most $n-1$. Thus $\{1, \ldots, a^{n-1}\}$ spans $F[a]$, and it is a basis since any linear combination cannot be zero as $h_a(x)$ is minimal and has degree n. Therefore $F[a]$ is a F-linear space of dimension n.

Notice that

$${F[x]}\Big/{(h_a)} = {F[x]}\Big/{\ker \psi_a} \cong \mathrm{Im}\psi_a = \{f(a) \mid f \in F[x]\} = F[a] = \mathrm{span}\{1, \ldots, a^{n-1}\} \subseteq K$$

Since K is an integral domain, so is $F[a]$. Therefore (h_a) is a prime ideal, since a quotient ring is an integral domain iff the ideal is prime. Since $F[x]$ is a PID, prime and maximal ideals are the same, so (h_a) is maximal and therefore $F[a]$ is a field.

So we have proven

1.2.4 Proposition

Let K/F be a field extension and $a \in K$ algebraic in F. Let h_a be a's minimal polynomial over F, then

(**1**) h_a is irreducible,

(**2**) $F[a]$ is a field,

(**3**) $[F[a] : F] = n = \deg h_a$ and has a basis $\{1, a, \ldots, a^{n-1}\}$.

In particular we have shown that when a is algebraic, $F(a) = F[a]$.

1.2.5 Proposition

Suppose $F \subseteq K$ where F is a field and K is an integral domain. Further suppose $[K : F]$ is finite. Then every element of K is algebraic and K is a field.

Proof: let $a \in K$, then

$$[K : F] = [K : F[a]] \cdot [F[a] : F]$$

meaning $[F[a] : F]$ must be finite and so a must be algebraic (as otherwise $F[a] \cong F[x]$ which has infinite degree). Since $F[a]$ is a field, it must have a multiplicative inverse for a, meaning K is a field. ■

Notice that $[F[a, b] : F[a]] \leq [F[b] : F]$, since the minimal polynomial of b relative to F, h_b, is also a zeroing a polynomial of b over $F[a]$. And so $[F[a, b] : F[a]] \leq \deg h_b = [F[b] : F]$. Thus we have that by multiplicity

$$[F[a, b] : F] = [F[a, b] : F[a]] \cdot [F[a] : F] \leq [F[b] : F] \cdot [F[a] : F]$$

And inductively we can show

1.2.6 Proposition

Suppose K/F is a field extension and $a_1, \ldots, a_n$ then

$$\big[F[a_1, \ldots, a_n] : F\big] \leq \prod_{i=1}^{n} \big[F[a_i] : F\big]$$

1.2.7 Definition

Call a field extension K/F **algebraic** if every $a \in K$ is algebraic over F.

1.2.8 Lemma

Suppose $F_3/F_2/F_1$ are field extensions such that F_2/F_1 is algebraic and $a \in F_3$ is algebraic over F_2. Then it is also algebraic over F_1.

Proof: there exists an $f \in F_2[x]$ such that $f(a) = 0$. Suppose $f = \sum b_i x^i$, then a is algebraic over $F_1[b_0, \ldots, b_n]$. Then

$$[F_1[b_0, \ldots, b_n, a] : F_1] = [F_1[b_0, \ldots, b_n, a] : F_1[b_0, \ldots, b_n]] \cdot [F_1[b_0, \ldots, b_n] : F_1]$$

and since a is algebraic over $F_1[b_0, \ldots, b_n]$ and $b_i \in F_2$ are algebraic over F_1, the right-hand side is finite. Thus a is algebraic over F_1 by the left-hand side, as required. ■

1.2.9 Theorem

Let K/F be a field extension, then

$$\mathrm{Alg}_F(K) := \{a \in K \mid a \text{ is algebraic over } F\}$$

is a field. Furthermore, every element in $K \setminus \mathrm{Alg}_F(K)$ is transcendental over $\mathrm{Alg}_F(K)$.

Proof: notice that $F[a \cdot b], F[a+b] \subseteq F[a,b]$ and $[F[a,b]:F] \leq [F[a]:F] \cdot [F[b]:F] < \infty$ for $a, b \in \mathrm{Alg}_F(K)$. So $\mathrm{Alg}_F(K)$ is closed under addition and multiplication. It is also obviously closed under additive inverses since $F[-a] = F[a]$. And since $F[a]$ is a field, $a^{-1} \in F[a]$ so $F[a^{-1}] \subseteq F[a]$ and thus $[F[a^{-1}]:F] \leq [F[a]:F] < \infty$, so a^{-1} is algebraic over F. So $\mathrm{Alg}_F(K)$ is indeed a field.

Now suppose $a \in K \setminus \mathrm{Alg}_F(K)$ is algebraic over $\mathrm{Alg}_F(K)$. Then by the above lemma, it is algebraic over F since $\mathrm{Alg}_F(K)/F$ is trivially algebraic. But then $a \in \mathrm{Alg}_F(K)$ by definition, in contradiction. ■

1.3 Splitting Fields

1.3.1 Proposition

Let F be a field and $f \in F[x]$ be an irreducible polynomial. Then there exists a field extension K/F such that f has a root in K and $[K:F] = \deg f$.

Proof: since f is irreducible, (f) is maximal (since $F[x]$ is a PID so prime ideals are maximal). Thus $K = {F[x]}/{(f)}$ is a field. The dimension of K is $\deg f$ since it has a basis $\{1, x, \ldots, x^{\deg f - 1}\}$.

By the second isomorphism theorem,

$$ {F}/{F \cap (f)} \cong {F + (f)}/{(f)} \subseteq {F[x]}/{(f)} = K $$

But $F \cap (f) = 0$, and so ${F}/{F \cap (f)} = {F}/{0} \cong F$. Thus we can embed F into K, so we can view K/F as a field extension.

Now, define $\alpha = x + (f)$, and suppose $f(x) = \sum_{i=0}^{n} a_i x^i$ for $a_i \in F$. Then

$$ f(\alpha) = \sum_{i=0}^{n} a_i \big(x + (f)\big)^i = \sum_{i=0}^{n} a_i (x^i + (f)) = \sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} a_i (f) = f + (f) = 0 $$

Thus α is a root of f in K. ■

1.3.2 Corollary

Let F be a field and $f \in F[x]$ a polynomial. Then there exists a field extension K/F such that f has a root in K and $[K:F] \leq \deg f$.

Proof: take an irreducible factorization of f and apply the above result to one of its factors. ■

1.3.3 Definition

Suppose F is a field and $f \in F[x]$. Then f **splits** in F if there exist $\alpha_1, \ldots, \alpha_n \in F$ such that $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$.

1.3.4 Proposition

Let $f \in F[x]$ then there exists a field extension K/F such that f splits in K and $[K:F] \leq (\deg f)!$.

Proof: by induction on $n = \deg f$. For $n = 1$, f is linear and thus has a root so we can take $K = F$. Now suppose $\deg f = n + 1$, then by corollary 1.3.2 there exists a field extension K_0/F such that f has a root in K_0 and $[K_0 : F] \leq n + 1$. Now suppose $\alpha \in K_0$ is a root of f, then there exists a $g(x) \in K_0[x]$ such that $(x - \alpha)g(x) = f(x)$ and so $\deg g \leq n$. Therefore inductively there is a field extension K/K_0 which splits $g(x)$ and thus $f(x)$ and

$$ [K:F] = [K:K_0] \cdot [K_0:F] \leq n! \cdot (n+1) = (n+1)! $$

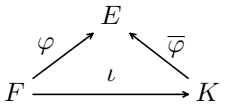
as required. ■

1.3.5 Definition

Suppose K/F is a field extension and $\varphi\colon F \hookrightarrow E$ is an embedding into some other field E. Then an **extension** of φ to K is an embedding $\overline{\varphi}\colon K \hookrightarrow E$ such that $\overline{\varphi}\big|_F = \varphi$ ($\overline{\varphi}$ is equal to φ on F). Let us then define

$$\eta^{\varphi}_{K/F} := \#\{\overline{\varphi} \mid \overline{\varphi} \text{ is an extension of } \varphi\}$$

In other words, an extension is an embedding $\overline{\varphi}$ such that the following diagram commutes:



Where $\iota\colon F \longrightarrow K$ is the inclusion embedding.

Suppose f, g are two field homomorphisms $F(a_1, \ldots, a_n) \longrightarrow K$ such that $f(x) = g(x)$ for all $x \in F$ and $f(a_i) = g(a_i)$ for $1 \leq i \leq n$. Then $f(x) = g(x)$ on all of $F(a_1, \ldots, a_n)$. This is since $\{r \in F(a_1, \ldots, a_n) \mid f(r) = g(r)\}$ is a field containing F and $a_1, \ldots, a_n$ and thus $F(a_1, \ldots, a_n)$.

In particular if $\varphi\colon F \hookrightarrow E$ is an embedding, then an extension $\overline{\varphi}\colon F(a_1, \ldots, a_n) \longrightarrow E$ is defined entirely by its image on $a_1, \ldots, a_n$.

1.3.6 Proposition

Suppose $K = F[\alpha]$, then $\eta^{\varphi}_{K/F}$ is equal to the number of distinct roots the minimal polynomial of α has in E. Formally, if $h(x) = \sum_{i=0}^{n} a_i x^i$ then define $\hat{h}(x) = \sum_{i=0}^{n} \varphi(a_i) x^i$, and $\eta^{\varphi}_{K/F}$ is equal to the number of roots $\hat{h}(x)$ has in E.

In particular $\eta^{\varphi}_{K/F}$ is independent of the choice of φ.

Proof: let $h(x) \in F[x]$ be the minimal polynomial of α, and $\overline{\varphi}$ be an extension of φ to K, then

$$\hat{h}(\overline{\varphi}(\alpha)) = \sum_{i=0}^{n} \varphi(a_i)\overline{\varphi}(\alpha)^i = \sum_{i=0}^{n} \overline{\varphi}(a_i)\overline{\varphi}(\alpha^i) = \overline{\varphi}\left(\sum_{i=0}^{n} a_i \alpha^i\right) = \overline{\varphi}(h(\alpha)) = \overline{\varphi}(0) = 0$$

Thus $\overline{\varphi}(\alpha)$ must be a root of $\hat{h}(x)$, and as explained above extensions of embeddings to $K = F[\alpha]$ are dependent only on their image of α. So there are at most as many extensions as there are distinct roots of $\hat{h}$.

Now suppose $\beta \in E$ is a root of $\hat{h}$, then we claim that there exists an extension with $\overline{\varphi}(\alpha) = \beta$. Indeed, $\alpha \notin F$ and β is not in the image of φ (as then $0 = \hat{h}(\varphi(a)) = \varphi(\hat{h}(a))$ so a is a root of $\hat{h}(x)$ but $\hat{h}$ is irreducible), so this is well-defined. ∎

1.3.7 Definition

A polynomial f which splits over E is called **separable** over E if its linear factors are all distinct (ie. it has $n = \deg f$ distinct roots in E).

When we have an embedding $\varphi\colon F \hookrightarrow E$ and a polynomial $f \in F[x]$ and we say that f has some property in E (eg. splits over E, separable over E), then we mean that its image under φ has that property. Meaning if $f(x) = \sum_{i=0}^{n} a_i x^i$ then $\sum_{i=0}^{n} \varphi(a_i) x^i$ has said property.

1.3.8 Theorem

Let K/F be a finite extension, and let $\varphi\colon F \hookrightarrow E$ be an embedding. Then

(1) $\eta^{E}_{K/F} \leq [K : F]$;

(2) if $K = F[\alpha_1, \ldots, \alpha_n]$ where α_i are roots of some $f \in F[x]$ which splits over E, then $1 \leq \eta^{\varphi}_{K/F}$.

Meaning there exists at least one extension of φ to K;

(**3**) if f is also separable over E, then $\eta^{\varphi}_{K/F} = [K : F]$.

Proof: since K/F is finite, we have that $K = F[\alpha_1, \ldots, \alpha_n]$ (we can take $\{\alpha_1, \ldots, \alpha_n\}$ to be a basis for K as a F-linear space).

(**1**) We proceed inductively on n. For $n = 1$, by the previous proposition $\eta^{\varphi}_{K/F}$ is equal to the number of roots h_{α_1} (the minimal polynomial of α_1) has in E.
For the inductive step, define $F_1 = F[\alpha_1]$, and so

$$\begin{aligned}\eta^{\varphi}_{K/F} &= \#\{\varphi'' \colon K \longrightarrow E \text{ is an extension of } \varphi\} \\ &= \#\bigcup\{\varphi'' \colon K \longrightarrow E \text{ is an extension of } \varphi' \mid \varphi' \colon F_1 \longrightarrow E \text{ is an extension of } \varphi\} \\ &= \sum_{\varphi'} \eta^{\varphi'}_{K/F_1}\end{aligned}$$

By our inductive hypothesis, $\eta^{\varphi'}_{K/F_1} \leq [K : F_1]$ and $\eta^{\varphi}_{F_1/F} \leq [F_1 : F]$ so

$$\leq \sum_{\varphi'} [K : F_1] = [F_1 : F] \cdot [K : F] = [K : F]$$

as required.

(**2**) Again, we proceed inductively on n. For $n = 1$, $K = F[\alpha]$ and $\eta^{\varphi}_{K/F}$ is equal to the number of roots h_α has in E. But since $f(\alpha) = 0$ and h_α is minimal, h_α must divide f and therefore split in E, meaning it has at least one root in E. So $1 \leq \eta^{\varphi}_{K/F}$ as required.

Inductively, set $F_1 = F[\alpha_1]$ and so there exists an extension of φ to $\varphi' \colon F_1 \hookrightarrow E$ by our base case. And there then exists an extension of φ' to $\varphi'' \colon K \hookrightarrow E$, so there exists at least one extension as required.

(**3**) If we review the proof of (2), for the base case we must have that f is separable and splits in E, which means that h_α does as well. Then h_α has precisely $\deg h_\alpha$ distinct roots in E, so $\eta^{\varphi}_{K/F} = \deg h_\alpha = [K : F]$ as required. The rest of the proof proceeds similarly. ■

1.3.9 Definition

Let $f \in F[x]$ be any polynomial over F. Then a field $F \subseteq K$ is called a **splitting field** if f splits over K and it contains no other field over which f splits (meaning it is the smallest field which splits f).

Notice that if K is a splitting field of $f \in F[x]$, then K is of the form $K = F[\alpha_1, \ldots, \alpha_n]$ where α_i are roots of f in K. Then

$$[K : F] \leq \prod_{i=1}^{n} [F[\alpha_i] : F] < \infty$$

so K/F is a finite extension. And such a finite field exists: we know there exists a field extension F_1 such that f has a root α_1 in F_1, so there must be an extension F_2/F_1 such that $f/(x - \alpha)$ has a root α_2 in F_2, and we continue inductively. This gives us a field F_n with roots $\alpha_1, \ldots, \alpha_n$ and so defining $K = F[\alpha_1, \ldots, \alpha_n]$ gives us a splitting field.

1.3.10 Theorem

Any two splitting fields of a polynomial $f \in F[x]$ are isomorphic.

Proof: let K be a splitting field of f, and suppose f splits in E, where $F \subseteq E$. By the above theorem, there must exist an extension of the inclusion embedding $F \hookrightarrow E$ to an embedding $K \hookrightarrow E$. This embedding gives rise to an embedding of F-linear spaces, meaning $[K : F] \leq [E : F]$. In particular, if E is another splitting field of f then $[E : F] \leq [K : F]$ as well, so that K and E are isomorphic F-linear spaces, and thus are isomorphic as fields. ■

1.3.11 Definition

Let $f(x) = \sum_{k=0}^{n} a_k x^k \in F[x]$ be a polynomial. We define its **formal derivative** to be the polynomial

$$f'(x) = \sum_{k=1}^{n} k a_k x^{k-1}$$

It is not hard to prove that $(f+g)' = f' + g'$ and $(f \cdot g)' = f'g + fg'$.

1.3.12 Lemma

Let $f, g \in F[x]$ and define $r(x) = \gcd(f, g)$. Then $r(x)$ is the gcd of f and g over *every* field extension K/F.

Proof: let $r_K(x)$ be the gcd of f, g over K. Since $r(x)$ still divides f, g we have that $r(x) | r_K(x)$. And by Euclid's algorithm there exist $a(x), b(x) \in F[x]$ such that

$$r(x) = a(x)f(x) + b(x)g(x)$$

But $r_K(x)$ divides f, g so it divides $r(x)$. Thus $r_K(x) = r(x)$ as required. ■

1.3.13 Theorem

Let $f \in F[x]$ be a polynomial, then f is separable if and only if $\gcd(f, f') = 1$.

Proof: let K be a splitting field of f. Suppose f is not separable, then it has the form $f(x) = (x-\alpha)^m g(x)$ for $g(x) \in K[x]$ and $m > 1$. But then $f'(x) = m(x-\alpha)^{m-1} g(x) + (x-\alpha)^m g'(x)$ and so $x - \alpha$ is a common factor of both f and f' so $\gcd(f, f') \neq 1$ in $K[x]$, but the gcd of f, f' in F is equal to its gcd in K by the above lemma. Alternatively if f is separable, then $f(x) = \prod_{i=1}^{n} (x - \alpha_i)$ and so

$$f'(x) = \sum_{j=1}^{n} \prod_{\substack{1 \leq i \leq n \\ i \neq j}} (x - \alpha_i)$$

But the irreducible factors of f, which are $x - \alpha_i$, do not divide $f'(x)$ since no two roots are equal. Thus $\gcd(f, f') = 1$. ■

Recall that for any ring R, there is a unique homomorphism $\varphi : \mathbb{Z} \longrightarrow R$. In particular if F is a field then $\mathbb{Z}/\ker\varphi \cong \mathrm{Im}\varphi \subseteq F$. Since F is a field, $\mathrm{Im}\varphi$ is an integral domain and so $\ker\varphi$ is a prime ideal of $\mathbb{Z}$, meaning $\ker\varphi = (p)$ for some prime p or 0. This is called the *characteristic* of F.
Since $\varphi(n) = 1 + \cdots + 1$, the characteristic of F is simply the prime p such that $\varphi(p) = 0$, ie. $1 + \cdots + 1 = 0$ (p times), or 0 if no such primes exist.

1.3.14 Definition

The **characteristic** of a field F is the unique positive generator of the kernel of $\varphi : \mathbb{Z} \longrightarrow F$. Equivalently it is the minimum number p such that $1 + \cdots + 1 = 0$ (p times), or 0 if no such p exists.

If F has characteristic 0, then φ is an embedding so we can view $\mathbb{Z}$ as a subfield of F. But then the field generated by $\mathbb{Z}$ must also be a subfield of (embeddable into) F, meaning $\mathbb{Q} \subseteq F$. Similarly for fields of characteristic $p > 0$, $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p \subseteq F$.

Notice that for fields of characteristic p, $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ is zero for $k \neq 0, p$. Thus:

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{n-k} = a^p + b^p$$

So $x \mapsto x^p$ is a homomorphism, called the *Frobenius homomorphism*. It can be viewed as a homomorphism to $F^p = \{x^p \mid x \in F\}$ (which is a field precisely because the Frobenius homomorphism is a homomorphism). The homomorphism has a trivial kernel, so $F \cong F^p$. In particular every element of F is of the form x^p.

1.3.15 Theorem

Let $f \in F[x]$ be an irreducible polynomial, then the following are equivalent:

(**1**) f is not separable (has a multiple root),

(**2**) F has a characteristic $p > 0$, and $f(x) = g(x^p)$ for some $g \in F[x]$,

(**3**) every root of f is a multiple root.

Proof: (1) $\implies$ (2): by theorem 1.3.13 we have that $\gcd(f, f') \neq 1$. But f is irreducible and thus has no nontrivial divisors, so $f' = 0$. But since f is nonconstant, we must have that F is of characteristic p (since in characteristic 0 a nonconstant polynomial cannot have a zero derivative).

Now, if $f(x) = \sum_{k=0}^{n} a_k x^k$ then $ka_k = 0$ for all k since $f'(x) = 0$. So for k not divisible by p, this means that $k \neq 0$ and so $a_k = 0$. Thus

$$f(x) = \sum_{p|k} a_k x^k = \sum_j a_{pj} x^{pj}$$

so define $g(x) = \sum_j a_{pj} x^j$ and we have the desired result.

(2) $\implies$ (3): take a splitting field of $g(x)$, then write $g(x) = a\prod_i (x - a_i)^{m_i}$. Then we have that $f(x) = a\prod_i (x^p - a_i)^{m_i}$. We can extend this to a field with p-roots of a_i (which are roots of $x^p - a_i$), α_i, and so over this field $f(x) = a\prod_i (x - \alpha_i)^{pm_i}$. So all the roots of f have a multiplicity greater than 1.

(3) $\implies$ (1) is trivial. ■