MATH 416, Modern Algebra II

Volodymyr Nekrashevych

2020, April 7

A reminder

Theorem 1

Let $F \subset E \subset \overline{F}$ be fields. Then E is a splitting field over F if and only if every automorphism σ of $\overline{F}$ fixing every element of F satisfies $\sigma(E) = E$.

Let $F \subset E$. We say that a polynomial $f(x) \in F[x]$ *splits in E* if it factors over E into a product of linear polynomials.

Proposition 2

Let E be a splitting field over F. Then every irreducible polynomial $f(x) \in F[x]$ that has a root in E splits in E.

The proof is the same as the proof of the theorem. If α and β are roots of an irreducible polynomial $f(x) \in F[x]$ and $\alpha \in E$, then the isomorphism $F(\alpha) \to F(\beta)$ extends to an automorphism σ of $\overline{F}$ which satisfies $\sigma(E) = E$. But this means that $\sigma(\alpha) = \beta \in E$, so $f(x)$ splits in E.

Corollary 3

If $E \subseteq \overline{F}$ is a splitting field over F, then every isomorphism $\sigma : E \to \sigma(E) \subset \overline{F}$ fixing F is an automorphism of E. In particular, $\{E : F\} = |G(E/F)|$.

Proof: Every such a isomorphism σ can be extended to an automorphism of $\overline{F}$. Therefore, by Theorem 1, σ is an automorphism of E.

Our next aim is to understand when $\{E : F\} = [E : F]$. Let $f(x) \in F[x]$. An element $\alpha \in \overline{F}$ such that $f(\alpha) = 0$ is a root of *multiplicity* k if $(x - \alpha)^k$ divides $f(x)$, and k is the greatest integer with this property. We can define a formal derivative of a polynomial $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ as $f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1$. It is easy to check that this derivative satisfies all the usual properties: $(af(x) + bg(x))' = af'(x) + bg'(x)$ for $f, g \in F[x]$ and $a, b \in F$; $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$. It follows that if α is a root of $f(x)$ multiplicity k, then $f(x) = (x - \alpha)^k g(x)$, so $f'(x) = k(x-\alpha)^{k-1}g(x)+(x-\alpha)^k g'(x) = (x-\alpha)^{k-1}(kg(x)+(x-\alpha)g'(x))$. If the field is of characteristic 0, then we see that α is a root of $f'(x)$ of multiplicity $k - 1$. If characteristic of F is non-zero, then it may happen that $f'(x) = 0$ and this argument doesn't work.

Theorem 4

Let $f(x) \in F[x]$ be irreducible. Then all zeros of $f(x)$ in $\overline{F}$ have the same multiplicities.

Proof: For any two roots α, β of $f(x)$ there is an automorphism σ of $\overline{F}$ such that $\sigma(\alpha) = \beta$. □

It follows that an irreducible polynomial $f(x) \in F[x]$ factors as $a \prod_i (x - \alpha_i)^k$ for some $k \in \mathbb{N}$ and $a \in F \setminus \{0\}$.

Note that an irreducible polynomial $f(x)$ over a field of characteristic 0 can not have multiple roots, since otherwise $f(x)$ and $f'(x)$ have a non-trivial common divisor.

Example

Consider the field $\mathbb{Z}_p(t)$ of rational functions in t over $\mathbb{Z}_p$. Denote $y = t^p$ and consider $\mathbb{Z}_p(t)$. We have $\mathbb{Z}_p(y) \subset \mathbb{Z}_p(t)$. Then $\mathbb{Z}_p(t)$ is algebraic extension of $\mathbb{Z}_p(y)$, because t is a root of $x^p - y \in \mathbb{Z}_p(y)[x]$. Note that in $\mathbb{Z}_p(t)$ we have $y = t^p$ and $x^p - y = x^p - t^p = (x - t)^p$. The polynomial $x^p - y$ is irreducible, because any other factor of $x^p - y$ in $\mathbb{Z}_p(t)$ must be $(x - t)^k$ for some k, but then the value at 0 is $(-t)^k$, which belongs to $\mathbb{Z}_p(y)$ only when $k = 0$ or $k = p$. We see that $x^p - y$ is irreducible over $\mathbb{Z}_p(y)$ and factors as $(x - t)^p$ over $\mathbb{Z}_p(t)$.

Suppose that $f(x) \in F[x]$ is an irreducible polynomial with multiple roots. Let $\alpha \in \overline{F}$ be a root of f. Then any extension of the identity automorphism of F to $F(\alpha)$ is of the form $F(\alpha) \to F(\beta)$ mapping α to another root β of f. It follows that $\{F(\alpha) : F\}$ is equal to the number of **distinct roots** of $f(x)$, while $[F(\alpha) : F]$ is equal to the degree of f, i.e., to the **total** number of roots counted with multiplicities. We see that actually $[F(\alpha) : F] = k\{F(\alpha) : F\}$, where k is the multiplicity of α as a root of an irreducible polynomial.

Theorem 5

If E is a finite extension of F, then $\{E : F\}$ divides $[E : F]$.

Definition 1

A finite extension $F \subseteq E$ is *separable* if $\{E : F\} = [E : F]$. An element $\alpha \in \overline{F}$ is *separable over* F if $F \subseteq F(\alpha)$ is a separable extension. An irreducible polynomial $f(x) \in F[x]$ is *separable* if every its root is separable over F.

Theorem 6

If K is a finite extension of E and E is a finite extension of F, then K is separable over F if and only if K is separable over E and E is separable over F. A finite extension $F \subset E$ is separable if and only if every element of E is separable over F (i.e., is a simple root of an irreducible polynomial over F).

Perfect fields

A field F is called *perfect* if every finite extension $F \subset E$ is separable. We have seen that every field of characteristic zero is perfect. We have seen that the field $\mathbb{Z}_p(y)$ is not perfect.

We will need the following fact.

Lemma 7

Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \overline{F}[x]$. If $(f(x))^m \in F[x]$ and $m \cdot 1 \neq 0$ in F, then $f(x) \in F[x]$.

Proof: We prove by induction on r that $a_{n-r} \in F$. We have $(f(x))^m = x^{nm} + ma_{n-1}x^{nm-1} + \cdots$. Since $m \neq 0$ in F and $ma_{n-1} \in F$, we get that $a_{n-1} \in F$. Suppose that we know that $a_{n-i} \in F$ for all $i < r$. The coefficient at x^{mn-r} in $(f(x))^m$ is equal to the sum of products all possible products $a_{i_1}a_{i_2}\cdots a_{i_m}$ such that $i_1 + i_2 + \cdots + i_m = nm - r$. There are m such products of the form $a_na_n\cdots a_na_{n-r}$, which will contribute ma_{n-r} into the sum (since $a_n = 1$). In all the other products we will have $\min(i_1, i_2, \ldots, i_m) > n - r$. By the inductive hypothesis all such products $a_{i_1}a_{i_2}\cdots a_{i_m}$ belong to F. It follows that $ma_{n-r} \in F$, hence $a_{n-r} \in F$.

Theorem 8

Every finite field is perfect.

Proof. Let E be a finite extension of a finite field F. Let p be the characteristic of F. Let $\alpha \in E$. We want to show that α is separable over F. Let $f(x) \in F[x]$ be irreducible such that $f(\alpha) = 0$. Let k be the multiplicity of α. Then $f(x) = \prod_i (x - \alpha_i)^k = \left(\prod_i (x - \alpha_i)^{p^l}\right)^e$, where $k = p^l e$ and e is not divisible by p. Then by the lemma above $\prod (x - \alpha_i)^{p^l} \in F[x]$. Since f is irreducible, this means that $e = 1$, i.e., k is a power of p.

We have $f(x) = \prod_i \left(x^{p^l} - \alpha_i^{p^l}\right)$. Denote $g(x) = \prod_i \left(x - \alpha_i^{p_l}\right)$. Then all the roots of $g(x)$ are distinct, i.e., $g(x)$ is separable over F, so $F \subseteq F(\alpha^{p^l})$ is a separable extension. The map $x \mapsto x^p$ is a field isomorphism and is injective. The field $F(\alpha^{p^l})$ is finite, so the map $x \mapsto x^p$ must be an automorphism (since it is an injective map from a finite set to itself). Apply it l times to get the automorphism $x \mapsto x^{p^l}$. Since it is a bijection, it is also onto. We have $\alpha \mapsto \alpha^{p^l}$. Since α^{p^l} was separable, α is also separable.