LECTURE MARCH 16: SPLITTING FIELDS

1. Some examples

Remember that $\operatorname{Aut} F$ is the group of automorphisms of a field F, and if E/F is an extension of fields, then $\operatorname{Aut}(E/F)$ is the group of automorphisms $\sigma\colon E \to E$ which fix all elements of F.

- $\operatorname{Aut} \mathbf{Q} = \{e\}$.
- $\operatorname{Aut} \mathbf{Q}(\sqrt{2}) \cong \mathbf{Z}/2\mathbf{Z}$.
- $\operatorname{Aut} \mathbf{Q}(2^{1/3}) = \{e\}$.
- $\operatorname{Aut} \mathbf{Q}(2^{1/3}, \omega) \cong S_3$, where $\omega = e^{2\pi i/3}$.
- $\operatorname{Aut} \mathbf{Q}(2^{1/3}, \omega)/\mathbf{Q}(\omega) \cong \mathbf{Z}/3\mathbf{Z}$.
- $\operatorname{Aut} \mathbf{Q}(\sqrt{2}, \sqrt{3}) \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.
- $\operatorname{Aut} \mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{(2+\sqrt{2})(3+\sqrt{3})}) = Q_8$, the quaternion group of order 8.
- $\operatorname{Aut} \mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \dots) \cong \prod_p \mathbf{Z}/2\mathbf{Z}$.
- $\operatorname{Aut} \overline{\mathbf{Q}}$ is a large, rich, interesting, uncountable group.

If F is a field, and E is the splitting field of an irreducible polynomial of degree n, then

$$n \leqslant [E : F] \leqslant n!.$$

2. Splitting fields

Let F be a field. Let $\{f_i(x)\}$ be a collection of polynomials in $F[x]$. Then the *splitting field* of $\{f_i(x)\}$ is the smallest algebraic extension of F, such that all the $f_i(x)$ factor into linear factors. (To create the splitting field, adjoin *all* roots of each $f_i(x)$.)

Example: the splitting field of $x^2 - 2$ over $\mathbf{Q}$ is $\mathbf{Q}(\sqrt{2}, -\sqrt{2}) = \mathbf{Q}(\sqrt{2})$.

Example: the splitting field of $x^3 - 2$ over $\mathbf{Q}$ is $\mathbf{Q}(2^{1/3}, \omega 2^{1/3}, \omega^2 2^{1/3}) = \mathbf{Q}(2^{1/3}, \omega)$. This has degree $6 = 3!$ over $\mathbf{Q}$.

An algebraic extension E/F is a *splitting field* if it is the splitting field of some collection of polynomials.

For instance, $\mathbf{Q}(2^{1/3})$ is not a splitting field over $\mathbf{Q}$.

Theorem 2.1. *Let F be a field, and let $\overline{F}$ be an algebraic closure of F. Let $E \subset \overline{F}$ be an extension of F. Let $\psi\colon E \to \overline{F}$ be a homomorphism of fields, which fixes all elements of F. Then there exists an automorphism $\sigma\colon \overline{F} \to \overline{F}$, such that $\sigma(\alpha) = \psi(\alpha)$ for all $\alpha \in E$.*

Remark: when I say that ψ "fixes all elements of F", it means $\psi(\alpha) = \alpha$ for all $\alpha \in F$.

$$
\begin{array}{ccc}
\overline{F} & \xrightarrow{\sigma} & \overline{F} \\
\uparrow & & \uparrow \\
E & \xrightarrow[\psi]{} & \psi(E) \\
\uparrow & & \uparrow \\
F & \xrightarrow[=]{} & F
\end{array}
$$

Example: Let $F = \mathbf{Q}$, and let $E = \mathbf{Q}(2^{1/3})$. Let $\psi = \psi_{2^{1/3},\omega 2^{1/3}} \colon E \to \overline{\mathbf{Q}}$ send $2^{1/3}$ to $\omega 2^{1/3}$. The theorem says that there exists $\sigma \in \operatorname{Aut} \overline{\mathbf{Q}}$, such that $\sigma(2^{1/3}) = \omega 2^{1/3}$.

Theorem 2.2. *Let F be a field, $\overline{F}$ an algebraic closure, and let $F \subset E \subset \overline{F}$ be a subfield. Then E/F is a splitting field if and only if for all $\sigma \in \operatorname{Aut}(\overline{F}/F)$, we have $\sigma(E) = E$.*

Remark: $\sigma(E) = E$ means that for all $\alpha \in E$, $\sigma(\alpha) \in E$. It does not mean that $\sigma(\alpha) = \alpha$.

Example: $E = \mathbf{Q}(2^{1/3})$ must not be a splitting field over $\mathbf{Q}$, since we just observed that there exists a $\sigma \in \operatorname{Aut} \overline{\mathbf{Q}}$, such that $\sigma(2^{1/3}) = \omega 2^{1/3}$, and therefore $\sigma(E) \neq E$.

Splitting fields are important in Galois theory: if you want this important equality to hold:

$$\# \operatorname{Aut}(E/F) = [E : F],$$

then you need (a) E/F to be a splitting field, and (b) E/F to be *separable*.

Proof. Assume that E/F is the splitting field of $\{f_i(x)\}$, where $f_i(x) \in F[x]$. Let $\sigma \in \operatorname{Aut}(\overline{F}/F)$. I want to show that $\sigma(E) = E$.

WLOG all the $f_i(x)$ are irreducible. Let S be the set of all elements of $\overline{F}$ which are roots of one of the f_i. Then $E = F(S)$, essentially by definition of splitting field.

Let $\alpha \in S$, say α is a root of $f_i(x)$. Then $\sigma(\alpha)$ is also a root of $f_i(x)$. (This is because $f_i(x)$ has coefficients in F, and σ fixes F.) Therefore $\sigma(\alpha) \in S$, and therefore $\sigma(\alpha) \in E$. We have shown that $\sigma(E) = E$.

In the other direction, assume that E/F has this property. I want to show that E/F is a splitting field. Let $f(x)$ be an irreducible polynomial in $F[x]$ having a root $\alpha \in E$. Let $\beta \in \overline{F}$ be another root of $f(x)$. There exists an isomorphism $\psi_{\alpha,\beta} \colon F(\alpha) \to F(\beta)$, which sends α to β. By the isomorphism extension theorem, there exists an automorphism $\sigma \in \operatorname{Aut}(\overline{F}/F)$, such that $\sigma(\alpha) = \beta$.

By hypothesis, $\sigma(E) = E$. Therefore $\sigma(\alpha) = \beta \in E$. This means that E is a splitting field, namely, it is the splitting field of the set of all irreducible polynomials in $F[x]$ with at least one root in E. □

3. Finite Galois extensions

Working definition of a Galois extension:

Let E/F be a finite extensions of fields. I define E/F to be *Galois* if

$$[E : F] = \# \operatorname{Aut}(E/F).$$

Lots of nice properties follow from this. For instance, there is a bijection between fields K intermediate between E and F, and subgroups of $\operatorname{Aut}(E/F)$.

Example 3.1. $\mathbf{C}/\mathbf{R}$, $\mathbf{Q}(\sqrt{2})/\mathbf{Q}$, $\mathbf{Q}(\sqrt[3]{2}, \omega)/\mathbf{Q}$ *are all Galois extensions.* $\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}$ *is not.*

Another example: If $F/\mathbf{Z}_p$ *is a finite extension of degree* n*, then* $F = \mathbf{Z}_p(\alpha)$ *for some element* α *of degree* n *over* $\mathbf{Z}_p$*. We have* $\operatorname{Aut}(F/\mathbf{Z}_p)$ *is the cyclic group of order* n *generated by the Frobenius element* σ*, where* $\sigma(\alpha) = \alpha^p$*. Thus* $F/\mathbf{Z}_p$ *is Galois.*

Sometimes we call the finite field of order p^n the *Galois field* $GF(p^n)$.

Here's a consequence. If E/F is finite Galois, I claim that E/F has to be a splitting field. I'm just going to examine the case that $E = F(\alpha)$. Observe that if $\sigma \in \operatorname{Aut}(E/F)$, then $\sigma(\alpha)$ must be F-conjugate to α. But also $\sigma(\alpha) \in E$. We now have a map

$$\operatorname{Aut}(E/F) \to \{F\text{-conjugates of } \alpha \text{ lying in } E\}$$

which is just $\sigma \mapsto \sigma(\alpha)$. This map has to be injective, for if $\sigma(\alpha) = \sigma'(\alpha)$, then $\sigma' = \sigma$ (reason: every element of E is a polynomial in α with coefficients in F). By assumption, $\# \operatorname{Aut}(E/F) = [E : F]$. But there can only be as many conjugates as the degree $[E : F]$, so that E must contain all F-conjugates of α. As a result, E must be a splitting field.

4. The nightmare example

Let $F = \mathbf{Z}_p(t)$. Thus F is the field of rational functions in an indeterminate t. The polynomial $x^p - t$ is irreducible in $F[t]$. We can use it to create an extension of F of degree p:

$$E = F[x]/(x^p - t).$$

Then $E = F(\alpha)$, where $\alpha \in E$ satisfies $\alpha^p = t$. Does every root of the polynomial $x^p - t$ belong to E? How does the polynomial $x^p - t$ factor in $E[x]$? (Certainly α is a root....) The polynomial $x^p - t$ factors this way:

$$x^p - t = (x - \alpha)^p$$

because $(x - \alpha)^p = x^p - \alpha^p = x^p - t$. So, E/F is a splitting field, because $x^p - t$ splits in to linear factors over E.

What is $\operatorname{Aut}(E/F)$? Let $\sigma \in \operatorname{Aut}(E/F)$. What could $\sigma(\alpha)$ be? Since $\sigma(\alpha)$ is F-conjugate to α, and the only element conjugate to α is α itself, we must have $\sigma(\alpha) = \alpha$. Therefore $\operatorname{Aut}(E/F) = \{e\}$. So E/F is a splitting field which is not Galois.

5. Separable extensions

Let E/F be an algebraic extension. Say that an element $\alpha \in E$ is *separable* over F if the irreducible polynomial $f(x)$ of α over F has α as a root with multiplicity

1. Call the whole extension E/F separable, if every element of E is separable over F.

If $f(x)$ has a root α of multiplicity greater than one, it means that $f(x)$ factors this way:

$$f(x) = (x-\alpha)^2 g(x).$$

It turns out that you can formally take the derivative of a polynomial in $F[x]$. The derivative is an F-linear map $D\colon F[x] \to F[x]$, sending x^n to nx^{n-1}. We need to do this definition because the usual definition in terms of limits may not be available for general fields F.

Exercise: $D\colon F[x] \to F[x]$ satisfies the properties:

- $D(fg) = fD(g) + gD(f)$ (the Leibniz rule),
- $D(f^n) = nf^{n-1}D(f)$.

If $f(x)$ has α as a root of multiplicity at least 2, then

$$Df(x) = 2(x-\alpha)g(x) + (x-\alpha)^2 D(g(x)).$$

so $f'(\alpha) = 0$.

Now assume that $f(x) \in F[x]$ is irreducible, and that E/F contains an element α, which is a root of $f(x)$ of multiplicity at least 2. Then $f'(\alpha) = 0$, and so α is also a root of $f'(x)$.

Easy to see that $\deg f'(x) < \deg f(x)$. Since $f(x)$ was the nonzero polynomial of minimal degree with α as a root, we must have that $f'(x)$ is identically 0!

But, it is possible that $f'(x)$ is identically 0, without $f(x)$ being constant. For instance, $f(x) = x^p - t \in F[x]$ from before, has derivative $f'(x) = px^{p-1} = 0$. However, if F has characteristic 0, and $f(x)$ has degree n, then $\deg f'(x) = \deg f(x) - 1$. Reason: if $f(x) = x^n + a_{n-1}x^{n-1} + \dots$, then $f'(x) = nx^{n-1} + (n-1)a_{n-1}x^{n-2} + \dots$, and since we're in characteristic 0, this really does have degree $n-1$.

Theorem 5.1. *Let F be a field of characteristic 0, and let E/F be an algebraic extension. Then E/F is separable.*

6. Perfect fields

We call a field F *perfect* if all algebraic extensions E/F are separable. Certainly, all fields of characteristic 0 are perfect.

From the above discussion, a field F is perfect if its irreducible polynomials $f(x)$ never have the property that $f'(x) = 0$ (identically).

What would it mean for $f'(x)$ to be zero identically, in a field of characteristic p? It would mean that each nonzero term $a_n x^n$ appearing in the polynomial satisfies $na_n = 0$ in F. This would mean that $p|n$.

Theorem 6.1. *A field F of characteristic p is perfect if and only if for every $\alpha \in F$, there exists $\beta \in F$, such that $\beta^p = \alpha$.*

Another way of saying this is that the Frobenius map $\sigma\colon F \to F$, which sends $\alpha \mapsto \alpha^p$, is an automorphism of F. (*A priori* it is only an injective homomorphism.)

Proof. Let F be a field of characteristic p.

Suppose $\alpha \in F$ is not a pth power in F. Consider the polynomial $f(x) = x^p - \alpha$. We claim that $f(x)$ is irrededucible in $F[x]$. Assume otherwise: $f(x) = g(x)h(x)$, where $g(x), h(x) \in F[x]$ are monic and $1 \leqslant \deg g \leqslant p-1$. Now in an algebraic closure $\overline{F}$, there exists a root β of $f(x)$, so that $\beta^p = \alpha$. Then $f(x)$ factors in $\overline{F}[x]$ this way:

$$f(x) = x^p - \alpha = (x-\beta)^p.$$

Since $g(x)$ is supposed to divide $f(x)$, it must be of the form $g(x) = (x-\beta)^a$, where $1 \leqslant a \leqslant p-1$. The coefficient of x^{a-1} in $g(x)$ is $-a\beta$. Since $g(x) \in F[x]$, this means $-a\beta \in F$. Since $a \neq 0$ in F (!), it must be a unit, and so by cancellation, $\beta \in F$. This contradicts the fact that α is not a pth power in F.

We have shown that if $\alpha \in F$ is not a pth power in F, then $f(x) = x^p - \alpha \in F[x]$ is irreducible. If such an α exists, then $f(x)$ is an irreducible polynomial with $f'(x) = 0$, and so F cannot be perfect.

Conversely, suppose every element of F is a pth power. Suppose $f(x) \in F[x]$ is a polynomial with $f'(x) = 0$. By our observation about derivatives above, this can only happen if every exponent appearing in $f(x)$ is divisible by p:

$$f(x) = \alpha_n x^{pn} + \alpha_{n-1} x^{p(n-1)} + \cdots + \alpha_1 x^{pn} + \alpha_0,$$

with $a_i \in F$. By hypothesis, there exists $\beta_i \in F$ with $\beta_i^p = \alpha_i$. Then

$$f(x) = \sum_i \alpha_n x^{pn} = \left(\sum_i \beta_n x^n\right)^p$$

cannot be irreducible in $F[x]$! □

Theorem 6.2. *Every finite field is perfect.*

Proof. Let F be a finite field of characteristic p. The Frobenius homomorphism $F \to F$ is injective automatically, since F is a field. Since F is finite, this is automatically surjective as well. □

An example of a nonperfect field is $\mathbf{Z}_p(t)$. There are examples of infinite perfect fields of characterist p. For instance, the field $\mathbf{Z}_p(t, t^{1/p}, t^{1/p^2}, \ldots)$ (with all pth power roots of t adjoined) is perfect.