Math 250A Lecture 22 Notes

Daniel Raban

November 14, 2017

1 Examples in Galois Theory and Primitive Elements

1.1 Galois group of an irreducible degree 3 polynomial

Consider an irreducible polynomial $x^3 + ax^2 + bx + c = 0$. The Galois group $G \subseteq S_3$, the permutations of the roots. 3 divides the order of the Galois group, so $G = \mathbb{Z}/3\mathbb{Z}$, so $\mathbb{Z} = S_3$.

Example 1.1. Take $x^3 - 2$ over $\mathbb{Q}$. The Galois group is S_3.

Example 1.2. Take $x^3 + x + 1$ over F_2. The Galois group is $\mathbb{Z}/3\mathbb{Z}$.

We look at $\Delta = (\alpha - \beta)(\beta - \gamma)(\gamma - \alpha)$, where α, β, and γ are the roots of the polynomial. Δ is fixed by $\mathbb{Z}/3\mathbb{Z}$, but changes sign under odd permutations of α, β, γ. If the Galois group is $\mathbb{Z}/3\mathbb{Z}$, Δ must be in the base field. If the Galois group is S_3, $\Delta \mapsto -\Delta$ must be an automorphism. We must find if

$$\Delta^2 = (\alpha - \beta)^2(\beta - \gamma)^2(\gamma - \alpha)^2$$

has a square root in the base field. This is a symmetric function of α, β, γ, and we can compute this as

$$\Delta^2 = -4b^3 - 27c^2$$

if $a = 0$.

Example 1.3. Take $x^3 - 3x - 1$ over $\mathbb{Q}$. $\Delta^2 = 81$, which is a square in $\mathbb{Q}$. So the Galois group is $\mathbb{Z}/3\mathbb{Z}$.

1.2 Algebraic closure of $\mathbb{C}$

We have enough tools to provide a mostly algebraic proof of the fundamental theorem of algebra: that $\mathbb{C}$ is algebraically closed.

Theorem 1.1. *$\mathbb{C}$ is algebraically closed.*

Proof. We will use the following facts about $\mathbb{R}, \mathbb{C}$:

1. $\mathbb{R}$ has characteristic 0.
2. Any polynomial of odd degree over $\mathbb{R}$ has a real root (follows from intermediate value theorem).
3. $[\mathbb{C} : \mathbb{R}] = 2$, and every element of $\mathbb{C}$ has a square root in $\mathbb{C}$.

Let L be a finite extension of $\mathbb{C}$; we want to show that $L = \mathbb{C}$. We may as well extend L to a Galois extension ($\mathrm{char}(\mathbb{C}) = 0$, so L is automatically separable). So we have $R \subseteq \mathbb{C} \subseteq L$. Let $G = \mathrm{Gal}(L/\mathbb{R})$. We want to show that G has order 2. Fact 2 above gives us that G has no subgroups of odd index > 1 as $\mathbb{R}$ has no extensions of odd degree. Let H be a subgroup of $\mathbb{C}$, so H has index 2 in G. Fact 3 gives us that H has no subgroups of index 2 (since $\mathbb{C}$ has no extensions of index 2).

Let S be a 2-Sylow subgroup of G. S has odd index, so $S = 6$ by fact 2. So $G = S$ has order 2^n for some n. So H has order 2^{n-1}. If $n - 1 > 0$, H has subgroups of index 2, which would contradict fact 3, so $|H| = 1$, and $|G| = 2$. So $\mathbb{C}$ is algebraically closed. □

1.3 Primitive elements of separable extensions

Lemma 1.1. *Suppose V is a vector space over an infinite field K. Then V is not a union of finitely many proper subspaces.*

Proof. By induction. Let $V_1, \ldots, V_n$ be proper subspaces. Choose v no in $V_1, \ldots, V_{n-1}$ by induction. Choose $w \notin V_n$. Look at $v + kq$ for $k \in K$. There is at most 1 value of k for which this is in V_i for any given i. Since K is infinite, we can choose k so that $v + kq$ is not in any V_j. □

Theorem 1.2. *If L/K is a finite separable extension, L is generated by 1 element; i.e. there exists some $\alpha \in L$ such that $L = K(\alpha)$.*

Proof. There are only finitely many extensions between K and L. Let M be a Galois extension containing L. Then there ares only finitely many extensions of K in M, as these correspond to subgroups of the Galois group. Each extension is a vector space over K. Suppose K is infinite. Then the vector space L is not a union of a finite number of subspaces, so some element $\alpha \in L$ is not in any smaller extension of K. So $L = K(\alpha)$. If K is finite, then L is finite, so L^* is cyclic. □

Example 1.4. Let $F_p(t^p, u^p) \subseteq F_p(t, u)$. This has degree p^2 because

$$[F_p(t, u) : F_p(t, u^p)] = [F_p(t, u^p) : F_p(t^p, u^p)] = (p)(p) = p^2.$$

Every element a of $F_p(t, u)$ generates an extension of degree p or 1. In fact, $a^p \in F_p(t^p, u^p)$ for t or u since $(x + y)^p = x^p + y^p$ and $(xy)^p = x^p y^p$. So this is true for all polynomials in t, u. So $F_p(t, u)$ is not generated by 1 element, and there are infinitely many extensions between $F_p(t^p, u^p)$ and $F_p(t, u)$.

This is an example of a *purely inseparable* extension. These tend to be very weird and break your intuition. [Jacobson: in some cases subfields iff subalgebras of Lie algebra]

1.4 Primitive elements of extensions with Galois group $\mathbb{Z}/p\mathbb{Z}$

Suppose L/K is a Galois extension with Galois group $\mathbb{Z}/p\mathbb{Z}$ (cyclic). What can we say about L? Suppose $K = \mathbb{Q}(\zeta)$, where ζ is a primitive p-th root of unity. $L = K(\sqrt[p]{a})$ for some $a \in K$. This is a root of $x^p - a$. The other roots are $\sqrt[p]{a}$, $\sqrt[p]{a}\zeta$, $\sqrt[p]{a}\zeta^2, \ldots$. Any element of the Galois group takes $\sqrt[p]{a}$ to $\sqrt[p]{a}\zeta^i$ for some i. So the Galois groups is a subgroup of $\mathbb{Z}/p\mathbb{Z}$, making it 1 or $\mathbb{Z}/p\mathbb{Z}$ itself.

Suppose K contains all p-th roots of unity and K has characteristic $\neq p$. We want to show that $L = K(\sqrt[p]{a})$ for some a. How do we find this element? Let σ be a generator of the Galois group $\mathbb{Z}/p\mathbb{Z}$, so $\sigma^p = 1$. The key idea is to look at the action of σ on the vector space L over K (forget that L is a field). σ is a linear transformation, so we can look at its eigenvalues and eigenvectors. We hope to diagonalize σ.

$\sigma^p = 1$, so its eigenvalues are the roots of $x^p = 1$, which are contained in K. Now let's find eigenvectors. Pick any $v \in L$. Look at $v + \sigma v + \sigma^2 v + \cdots + \sigma^{p-1} v$, which has eigenvalue 1. Similarly, $v + \zeta\sigma v + \zeta^2\sigma^2 v + \cdots + \zeta^{p-1}\sigma^{p-1} v$ has eigenvalue ζ^{-1}. We then get $v + \zeta^{-1}\sigma v + \zeta^{-2}\sigma^2 v + \cdots + \zeta^{-(p-1)}\sigma^{p-1} v$ is an eigenvector with eigenvalue $\zeta = \zeta^{1-p}$. Note that v is the average of these, since $v = 1 + \zeta + \zeta^2 + \cdots + \zeta^{p-1} = 0$. So L is a direct sum of p 1 dimensional subspaces, on which σ acts as $1, \zeta, \zeta^2, \zeta^3, \ldots$.

Pick w to be any eigenvector of σ with eigenvalue $\neq 1$ (so $q \notin K$, where K is an subspace with eigenvalue $= 1$). Then $\sigma w = \zeta w$, say, which gives $\sigma w^p = \zeta^p w^p = w^p$. So $w^p \in K$ as it is fixed by σ. Put $a = w^p \in K$. Then $L = K(\sqrt[p]{a})$. So we have shown that

Proposition 1.1. *If L/K is a Galois extension such that*

1. *$Gal(L/K) = \mathbb{Z}/p\mathbb{Z}$,*
2. *K contains roots of $1 + x + \cdots + x^{p-1} = 0$,*
3. *K has characteristic $\neq p$,*

then $L = K(\sqrt[p]{a})$ for some $a \in K$.

What if K has characteristic p? Assume that L/K is Galois, $[L : K] = p$. Again, let σ be a generator of the Galois group. L cannot be of the form $K(\sqrt[p]{a})$ because $x^p - a$ is inseparable (all roots are the same). So the splitting field is not Galois! Look at the eigenvalues and eigenvectors of σ on the vector space L. $\sigma^p = 1$, so $\sigma - 1)^p = 0$. So $\sigma - 1$ is nilpotent and not diagonalizable! The only eigenvalue is 1, and the eigenspace is K.

Nilpotent matrices look something like this:

$$M = \begin{bmatrix} 0 & * & * & * \\ & 0 & * & * \\ & & 0 & * \\ & & & 0 \end{bmatrix}$$

The eigenvectors of M are no use, but generalized eigenvectors, $(M-\lambda)^n = 0$, are useful. So try to find the easiest generalized eigenvector, $(\sigma-1)^2 v = 0$. This means that $(\sigma-1)v \in K$, as it is fixed by σ. So $\sigma v - v = a$ for some $a \in K$ and $v \in L$. Changing v to v/a, we get $\sigma v - v = 1$. This is the simplest substitute for an eigenvector. Instead of $\sigma v = \lambda v$, we have $\sigma v = \lambda v + 1$. So $\sigma v = v + 1$, and $\sigma v^p = v^p + 1$. Then $\sigma(v^p - v) = v^p - v$, so $v^p - v \in K$. So r is a root of $x^p - x - b = 0$ for some $b \in K$. This is called an *Artin-Schrier equation*, the analogue of $x^p - b$. So $L = K(v)$, where v is a root of an A-S polynomial.

Suppose v is a root of $x^p - x - b = 0$ in characteristic p. What are the other roots?

$$(v+1)^p - (v+1) - b = v^p + 1 - v - 1 - b = v^p - v - b = 0$$

So the other roots are $v, v+1, v+2, \ldots, v+(p-1)$. This is p distinct roots. So $K(v)$ is Galois because it is separable (distinct roots) and normal (given one root, we can find the others). The Galois group is a subgroup of $\mathbb{Z}/p\mathbb{Z}$.

Over characteristic p, there are 2 possibilities:

1. $x^p - x - b$ is irreducible, so it is a Galois extension with Galois group $\mathbb{Z}/p\mathbb{Z}$.

2. $x^p - x - b$ factors into linear factors (b is of the form $c^p - c$ for $c \in K$).

Example 1.5. We can apply this to the construction of finite fields. What was the issue with order p^2? $F_p(\sqrt[p]{a})$, a is not a square in F_p, but there is no neat way to write down a in general. We can choose a choice of irreducible polynomial. What about p^p? In this case, we can take a root of $x^p - x - 1$. Check that this has no roots over F_p. $x^p - x = 0$ for all $x \in F_p$.

Given a polynomial $x^n + a_{n-1}x^{n-1} + \cdots + a_n$, a classical problem is to find formulas for its roots. For example, $x^2 + bx + c$ has roots $x = \frac{-b \pm \sqrt{b^2-4c}}{2}$. There are no formulas for 5th degree polynomials; we will show this next time.