Math 250A Lecture 20 Notes

Daniel Raban

November 7, 2017

1 Normal, Separable and Galois Extensions

1.1 Normal extensions

Recall that the splitting field L of a polynomial p over K is a field such that all roots of p are in L, and L is generated by the roots.

Proposition 1.1. *L is the splitting field of some family of polynomials (over K) iff any irreducible $p \in K[x]$ splits into linear factors in L.*

Proof. Suppose p is irreducible in $K[x]$ and has a root $\alpha \in L$. Look at M, the algebraic closure of L. Any homomorphism $\varphi : K[\alpha] \to M$ extends to a homomorphism $\psi : L \to M$ as M is algebraically closed. But $\operatorname{im}(\psi)$ must be L as L is the splitting field of some family of polynomials; the splitting field is a uniquely determined subfield of M, as it is a subfield generated by a family. So α is already in L. $\square$

Example 1.1. Reducible polynomials need not split into linear factors in L. Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt[3]{2})$. $x^3 - 2$ has a root in L, but it does not split into linear factors.

Definition 1.1. A finite extension L/K is called *normal* if existence of 1 root of an irreducible polynomial p implies that p factors into linear factors.

So L/K is normal iff it its the splitting field of some family of polynomials.

Proposition 1.2. *Any degree 2 extension L/K is normal.*

Proof. Suppose α is a root of (say) $a^2 + ax + b = (a - \alpha)(a - \beta)$. We have that $\alpha + \beta = -a$, so $\beta = -a - \alpha$. So β is already in the field $K[\alpha]$. $\square$

Example 1.2. $\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$ is not normal. $x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + (\sqrt[3]{2})^2)$.

Example 1.3. Normal extensions of normal extensions need not be normal over the base field. $\mathbb{Q}[\sqrt[4]{2}]/\mathbb{Q}$ is not normal, but $\mathbb{Q}[\sqrt[4]{2}]/\mathbb{Q}[\sqrt{2}]$ and $\mathbb{Q}[\sqrt{2}]/\mathbb{Q}$ are.

1.2 Separable extensions

Definition 1.2. A polynomial p is called *separable* if it has no multiple roots, i.e. if p, p' are coprime.

Definition 1.3. If L/K is an extension, $\alpha \in L$ is called *separable* if its irreducible polynomial is separable.

Definition 1.4. A field extension L/K is called *separable* if all its elements are separable.

Theorem 1.1. *L/K is separable if K has characteristic 0.*

Proof. α is a root of an irreducible p. We have that $\deg(p') < \deg(p)$, so p, p' have no common factors since p is irreducible. So p and p' are coprime. $\square$

Remark 1.1. Why does this only work for characteristic 0? The statement that p, p' have no common factors does not hold if $p' = 0$; in algebra, this does not imply that p is constant if the characteristic of K is not 0.

Corollary 1.1. *Any extension F_q/F_p of finite fields is separable.*

Proof. Any element is a root of $x^q - x$. This has derivative -1, so $(f, f') = 1$. $\square$

Example 1.4. Here is a non separable extension. Look at $F_p(t)$¡ the rational functions with coefficients in F_p (contains $F_p(t^p)$). $F_p(t^p) \subseteq F_p(t)$, so t is a root of $x^p - t^p$. This factors as $(x-t)^p$ because $(a+b)^p = a^p + b^p$, so all roots are the same. So t cannot be the root of any separable polynomial in $F_p(t^p)[x]$.

1.3 Galois extensions

1.3.1 Galois extensions and Galois groups

Definition 1.5. An extension is called *Galois* if it is separable and normal.

Definition 1.6. The *Galois group* $\mathrm{Gal}(L, K)$ of L/K is the group of automorphisms of L fixing all elements of K.

In a sense, the main point of Galois theory is that $\mathrm{Gal}(L, K)$ controls the extension L/K. So we can reduce facts about fields to facts about groups.

Lemma 1.1. *Suppose L/K is an extension of degree n and M/K is any extension. Then there are at most n ways to define a map $L \to M$ that acts as the identity on K.*

Proof. Suppose L is generated by α, so $L = K[\alpha]$. Then α is a root of a polynomial of degree $\leq n$. And $f(\alpha)$ is the root of a polynomial in M. This also have $\neq n$ roots in M, so there are $\leq n$ possibilities for $f(\alpha)$. So there are $\leq n$ possibilities for f.

Now suppose that L is generated by $\alpha, \beta, \gamma, \ldots$. Look at

$$K \subseteq K[\alpha] \subseteq K[\alpha, \beta] \subseteq \cdots$$

There are at most $[K[\alpha, \beta], K[\alpha]$ ways to extend a map from $K_[\alpha]$ to $K[\alpha, \beta]$. So there are $\leq [K[\alpha] : K][K[\alpha, \beta], K[\alpha]][K[\alpha, \beta, \gamma], K[\alpha, \beta]] \cdots$ ways to extend a map from K to L. But this is just $[L : K]$. $\square$

So if L/K is an extension of degree n, there are at most N automorphisms of L fixing all elements of K.

Theorem 1.2. *For a finite extension L/K, the following are equivalent:*

1. *L is the splitting field of a separable polynomial.*
2. *L is Galois.*
3. *$[L : K] = |G|$, where G is the Galois group of L/K.*
4. *$K = L^G$ (the set of elements of L fixed by G).*

Proof. (1) $\implies$ (2): A splitting field is normal.

(2) $\implies$ (3): Look at $K \subseteq L \subseteq M$, where M is the algebraic closure of K. Look at maps $l \to M$ extending the identity map of K. Since L/K is separable, there are n such extensions ($n = [L : K]$). Why? Suppose L is generated by α of degree n (root of p). We can map α to any root of p in M, and p has n roots as it is separable. We leave the case where L is not generated by 1 element as an exercise.

L/K is normal, so the image of any map $L \to M$ lies in L. So there are $\geq n$ maps from L to L fixing K. From our lemma, we have that there are always $\leq [L : K]$ maps L to L, so $|g| = [L : K]$.

(3) $\implies$ (4): Look at $K \subseteq L^G \subseteq L$. There are $\geq n$ maps L to L extending L^G. So $[L : L^G] \geq n$. But $[L : K] = n$¡ so $K = L^G$.

(4) $\implies$ (1): Let $\alpha \in L$, Look at all conjugates of α under $G = \mathrm{Gal}(L/K)$. Look at $(x - \alpha)(x - \beta)(x - \gamma) \cdots$. This is in $K[x]$ as all coefficients are invaraiant under G, since $K = L^G$. So α is a root of a separabble polynomial as $\alpha, \beta, \gamma, \ldots$ are distinct. The polynomial splits into linear facts, which gives us normality. $\square$

By our lemma, the third statement means that L is "as symmetric as possible."

Example 1.5. Take $x^3 - 2$ over $\mathbb{Q}$. This has 3 roots, $\sqrt[3]{2}$, $\sqrt[3]{2}w$, and $\sqrt[3]{2}w^2$, where w is a cube root of 1.

Let L be the splitting field. Then $[L : \mathbb{Q}] = 6$ because $[L : \mathbb{Q}[\sqrt[3]{2}]] = 2$, and $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = 3$. So $G = \mathrm{Gal}(L, \mathbb{Q})$ has order $6 = [L : \mathbb{Q}]$. It acts as permutations of α, β, γ, so it is the symmetric group S_3.

Example 1.6. Consider $\mathbb{C}/\mathbb{R}$. The Galois group has order 2, and is generated by complex conjugation $x + iy \mapsto x - iy$, which permutes the roots of $z^2 + 1 = 0$.

Example 1.7. Consider F_{16}/F_2. This is the splitting field of $x^{16} - x$, so it is Galois. So the galois grou[has order $4 = [F_{16} : F_2]$. What is it?

One element is the Frobenius element[1] φ, which takes $a \mapsto a^2$. Then $\varphi(ab) = \varphi(a)\varphi(b)$, and $\varphi(a + b) = \varphi(a) + \varphi(b)$ since $(a + b)^2 = a^2 + b^2$ in F_2. If a is fiixed by φ, then $a^2 = a$, so $a = 1$ or 0. So $a \in F_3$. So φ generates the Galois group, and $\varphi^4 = \text{id}$. $\varphi 4(a) = (((a^2)^2)^2)^2 = a^{16} = a$. So the Galois group is $\mathbb{Z}/4\mathbb{Z}$.

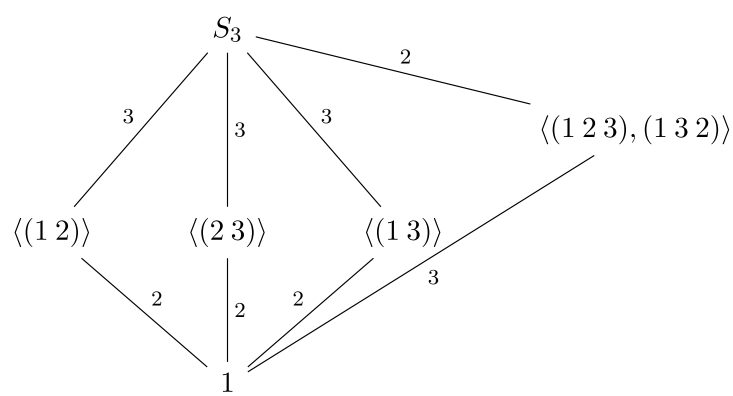
1.3.2 Galois groups and subextensions

Theorem 1.3. *Suppose M/K is a Galois extension with Galois group G. For any subextension L ($K \subseteq L \subseteq M$), $\mathrm{Gal}(M/L)$ is a subgroup of G. Conversely, any subgroup $H \subseteq G$ induces a subextension M^H, the elements fixed by H.*

In effect, we want to prove a bijection between subfields of M containing K and subgroups of G. We have a major problem: bigger subfields correspond to smaller subgroups.[2]

This can really be a source of confusion. Suppose that $K \subseteq L \subseteq M$, where L, M are Galois extensions of K. Then $\mathrm{Gal}(M, K)$ is bigger than $\mathrm{Gal}(L, K)$.

Example 1.8. Let's find all fields between $\mathbb{Q}$ and the splitting field of $x^3 - 2$. Look at the Galois group S_3. The subgroups of S_3 are:



[1]According to Professor Borcherds, the φ stands for Frobenius, even though Frobenius was German, not Greek. I can't tell if this was a joke or not.

[2]Professor Borcherds has been doing Galois theory for decades, but this still trips him up sometimes.

The subextensions of this splitting field are:

$$
\begin{tikzcd}
 & \mathbb{Q} \arrow[dl, dash, "3"'] \arrow[d, dash, "3"] \arrow[dr, dash, "3"] \arrow[drr, dash, "2"] & & \\
\mathbb{Q}(\sqrt[3]{2}w^2) \arrow[dr, dash, "2"'] & \mathbb{Q}(\sqrt[3]{2}) \arrow[d, dash, "2"] & \mathbb{Q}(\sqrt[3]{2}w) \arrow[dl, dash, "2"] & \mathbb{Q}(w) \arrow[dll, dash, "3"] \\
 & \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}w) & &
\end{tikzcd}
$$

The indices of the subgroups will correspond to the degrees of the subextensions.

Example 1.9. Let ζ be the a 7th root of unity in $\mathbb{C}$. Then $\zeta^7 = 1$, and $\zeta^6 + \zeta^5 + \zeta^4 + \zeta^3 + \zeta^2 + \zeta^+ 1 = 0$, where this polynomial is irreducible. This is $(x - \zeta)(x - \zeta^2) \cdots (z - \zeta^6)$. So $\mathbb{Q}[\zeta]$ is normal of degree 6.

The Galois group has order $6 = [\mathbb{Q}[\zeta] : \mathbb{Q}]$. What is it? Suppose that σ is in the Galois group. Then $\sigma(\zeta)$ is a root of $x^6 + x^5 + x^4 + x^3 + x^2 + x^+ 1$, so it is ζ^k for some $1 \leq k \leq 6$. Similarly, for τ, $\tau(\zeta) = \zeta^\ell$, so $\sigma\tau(\zeta) = \zeta^{k\ell}$. So the Galoid group is the group is $(\mathbb{Z}/7\mathbb{Z})^* \cong \mathbb{Z}/6\mathbb{Z}$, which is cyclic. There are 4 subgroups of orders 1, 2, 3, and 6, respectively (of index 6, 3, 2, and 1), so there are 4 extension of $\mathbb{Q}$ contained in $\mathbb{Q}[\zeta]$, of degrees 6, 3, 2, and 1.