Lecture Notes in Galois Theory

Lectures by Dr Sheng-Chi Liu

Throughout these notes, □ signifies end proof, and ▲ signifies end of example.

Table of Contents

Notes by Jakob Streipel. Last updated December 6, 2019.

Lecture 1 Review of Group Theory

1.1 Groups

Definition 1.1.1 (Group)**.** A ***group*** $(G, *)$ is a set G with a binary operation $*$ satisfying

(*i*) associativity, or $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$;

(*ii*) identity, meaning there exists an element $e \in G$ such that $g * e = e * g = g$ for all $g \in G$; and

(*iii*) inverse, meaning that for all $g \in G$ there exists an element $g' \in G$ such that $g * g' = g' * g = e$.

If $g_1 * g_2 = g_2 * g_1$ for all $g_1, g_2 \in G$, then G is called ***abelian***.

Generally we will suppress the symbol $*$ for the binary operation and write simply $g_1 g_2$ in place of $g_1 * g_2$.

Definition 1.1.2 (Group homomorphism)**.** Let G and G be groups.

A function $f\colon G \to H$ is a ***homomorphism*** is $f(g_1 g_2) = f(g_1) f(g_2)$ for all $g_1, g_2 \in G$. Another way of saying this is that f preserves the structure or respects the binary operation of the group G.

Similarly f is an ***isomorphism*** if f is a homomorphism that is one-to-one and onto.

An important object related to a homomorphism (or indeed any map) is the ***kernel*** of f, denoted

$$\ker f \coloneqq \left\{ g \in G \;\middle|\; f(g) = e_H \right\}.$$

Proposition 1.1.3. *A homomorphism $f\colon G \to H$ of groups is one-to-one if and only if $\ker f = \left\{ e_G \right\}$ is trivial.*

Definition 1.1.4 (Cosets)**.** Let H be a subgroup of a group G, and let $g \in G$. A ***left coset*** of H is a set of the shape $gH \coloneqq \left\{ gh \;\middle|\; h \in h \right\}$ and a ***right coset*** of H is a set of the kind $Hg = \left\{ hg \;\middle|\; h \in H \right\}$.

Proposition 1.1.5. *Let G be a group and H a subgroup of G.*

(*i*) *Let $g_1, g_2 \in G$. Then $g_1 H = g_2 H$ if and only if $g_1^{-1} g_2 \in H$.*

(*ii*) *Similarly, for $g_1, g_2 \in G$, we have $H g_1 = H g_2$ if and only if $g_2 g_1^{-1} \in H$.*

(*iii*) *If moreover H is finite, then $|gH| = |H| = |Hg|$ for any $g \in G$.*

Definition 1.1.6 (Index)**.** Let H be a subgroup of a group G. The ***index*** of H in G, denoted $[G\colon H]$, is the number of distinct left (or right) cosets of H in G.

Remark 1.1.7. Since each coset of H in G is of the same size, in the event that G is finite we must therefore have $|G| = [G : H] \cdot |H|$.

An immediate corollary of this is

Date: August 20th, 2019.

Theorem 1.1.8 (Lagrange)**.** *Let G be a finite group, and let $H < G$ be a subgroup. Then $|H| \mid |G|$.*

The converse of this theorem is not generally true, however in the special case of finite abelian groups it is. This is a consequence of the fundamental theorem of finite abelian groups, which we will discuss shortly.

In general left and right cosets gH and Hg are *not* equal, and moreover $\{ H, g_1H, g_2H, \dots \}$ is *not* a group.

Definition 1.1.9 (Normal subgroup)**.** Let H be a subgroup of a group G. We say that H is ***normal*** if $gH = Hg$ for all $g \in G$ (as sets; we are not saying that $gh = hg$ for every $g \in G$ and $h \in H$).

Theorem 1.1.10. *If H is a normal subgroup of G, then $G/H = \{ gH \mid g \in G \}$ is a group under the (natural) binary operation*

$$(gH)(g_1H) = (gg_1)H.$$

Proposition 1.1.11 (First isomorphism theorem)**.** *Let $f\colon G \to H$ be a group homomorphism. Then*

(*a*) $\ker f$ *is a normal subgroup of G, and*

(*b*) $G/\ker f \cong \operatorname{im} f$.

1.2 Structure of cyclic groups

Definition 1.2.1 (Cyclic group)**.** A group G is ***cyclic*** if $G = \langle a \rangle = \{ a^n \mid n \in \mathbb{Z} \}$, i.e., G is generated by a.

Theorem 1.2.2. *Let $G = \langle a \rangle$ be a cyclic group.*

(*a*) *If $|G| = \infty$, then $G \cong (\mathbb{Z}, +)$.*

(*b*) *If $|G| = m < \infty$, then $G \cong (\mathbb{Z}_m, +)$.*

Remark 1.2.3. By $\mathbb{Z}_m$ we mean $\mathbb{Z}/m\mathbb{Z}$, the integers modulo m. We will have occasion to write this quite frequently, hence the shorthand.

Proposition 1.2.4. *If $m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, where $p_1, p_2, \dots, p_k$ are distinct primes, then*

$$\mathbb{Z}_m \cong \mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_2^{a_2}} \times \dots \times \mathbb{Z}_{p_k^{a_k}}.$$

This is a consequence of the fact that if $\gcd(m, n) = 1$, then $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$.

1.3 Permutation groups

We denote by S_n the group of all bijections $\sigma\colon \{ 1, 2, \dots, n \} \to \{ 1, 2, \dots, n \}$, called the ***symmetric group*** of n elements.

Example 1.3.1. For instance, in S_4, we write things like

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 4 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 4 \end{pmatrix},$$

where the first form is a notation indicating that 1 goes to 4, 2 goes to 1, and so on. The second expression is the same permutation written in cycle notation, read as a cycle where 1 goes to 4 goes to 3 goes to 2 and returns to 1. Finally we have factored the cycle into ***transpositions***.

As an other example showing that not everything has to be in the same great big cycle, consider

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 3 & 4 \end{pmatrix}.$$

This time the permutation decomposes into two disjoint cycles—this way of writing a permutation as disjoint cycles is always unique (up to order of composition, but since they're disjoint that does not affect the result).

On the other hand, writing a permutation as transpositions is not unique, but the *parity* of the number of transpositions is. ▲

Let A_n denote the subgroup of S_n consisting of ***even permutations***, called the ***alternating group***.

Definition 1.3.2 (Simple group)**.** A group G is called ***simple*** if G has no proper nontrivial subgroups.

Theorem 1.3.3. *The alternating group A_n is simple if and only if $n \neq 4$.*

1.4 Finitely generated abelian groups

Let G_1 and G_2 be two groups. Then $G_1 \times G_2$ is a group under the binary operation

$$(a_1, a_2)(b_1, b_2) = (a_1 b_1, a_2 b_2).$$

Theorem 1.4.1 (Fundamental theorem of finitely generated abelian groups)**.** *Every finitely generated abelian group G is isomorphic to*

$$\mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times \ldots \times \mathbb{Z}_{p_k^{r_k}} \times \mathbb{Z} \times \mathbb{Z} \times \ldots \times \mathbb{Z}$$

where p_i are primes (not necessarily distinct) and $r_i \in \mathbb{N}$.

In the event that G is finite, of course the $\mathbb{Z}$ terms disappear.

1.5 Group actions

Definition 1.5.1 (Group action)**.** An ***action*** of a group G on a set S is a function $G \times S \to S$, $(g, x) \mapsto gx \in S$, such that for all $x \in S$ and $g_1, g_2 \in G$, we have

$$ex = x$$

and

$$(g_1 g_2)x = g_1(g_2 x).$$

Proposition 1.5.2. *Let G be a group acting on a set S.*

(*a*) *The relation on S defined by $x \sim y$ if and only if $gx = y$ for some $g \in G$ is an equivalence relation.*

(*b*) *For each $x \in S$, define $G_x \coloneqq \{ g \in G \mid gx = x \}$. This is a subgroup of G, called the* **stabiliser** *of x.*

Definition 1.5.3 (Orbit)**.** Let G be a group acting on a set S, and let $x \in S$. The set $Gx = \{ gx \mid g \in G \} \subset S$ is called the ***orbit*** of x.

Theorem 1.5.4. *Let G be a group acting on S. Let $x \in S$. Then $|Gx| = [G : G_x]$.*

Proof. Consider the map $G/G_x \to Gx$ defined by $gG_x \mapsto gx$. We need to check that this is well-defined, that it is one-to-one, and that it is onto.

That it is one-to-one is clear: if $gG_x = g_1G_x$, then $g^{-1}g_1 \in G_x$, meaning that $g^{-1}g_1x = x$, and multiplying by g we get $g_1x = gx$.

That this is one-to-one follows immediately by the above argument, just following the converse direction at each step.

Finally that this map is onto is trivial since we have the map defined for all g, and so of course we'll cover all the gx in Gx. □

Example 1.5.5. Let G be a group. Then G acts on itself by conjugation, $G \times G \to G$ defined by $(g, x) \mapsto gxg^{-1}$.

The orbit of x is $Gx = \{ gxg^{-1} \mid g \in G \}$, called the ***conjugacy class*** of x. The stabiliser $G_x = \{ g \in G \mid gxg^{-1} = x \} = C_G(x)$ is called the ***centraliser*** of x; it is the set of all $g \in G$ that commute with x, since multiplying both sides of $gxg^{-1} = x$ by g gives $gx = xg$. ▲

Corollary 1.5.6. *Let G be a finite group. Let $Gx_1, Gx_2, \ldots, Gx_n$ be all distinct conjugacy classes of G. Then*

$$|G| = \sum_{k=1}^{n} [G : C_G(x_k)].$$

Proof. This follows immediately from $|Gx_i| = [G : C_G(x_i)]$. □

Lemma 1.5.7. *Let H be a group of order p^n, where p is a prime. Suppose H acts on a finite set S. If $S_0 \coloneqq \{ x \in S \mid hx = x \text{ for all } h \in H \}$, then*

$$|S| \equiv |S_0| \pmod{p}.$$

Proof. Write S as a disjoint union of orbits

$$S = S_0 \sqcup Hx_1 \sqcup Hx_2 \sqcup \cdots \sqcup Hx_k$$

with $|Hx_i| > 1$ (since otherwise $x_1 \in S_0$) for all $i = 1, 2, \ldots, k$. Note that

$$|Hx_i| = [H : H_{x_i}] \mid |H| = p^n,$$

implying that $p \mid |Hx_i|$, adding the cardinalates in the disjoint union, implies

$$|S| \equiv |S_0| \pmod{p}$$

as desired. □

Theorem 1.5.8 (Cauchy)**.** *If G is a finite group with $p \mid |G|$, where p is a prime, then G contains an element of order p.*

Lecture 2 Group Actions and Sylow Theorems

2.1 p-Groups

Proof of Theorem 1.5.8. Set $|G| = n$ and let

$$S = \left\{ (a_1, a_2, \ldots, a_p) \;\middle|\; a_i \in G, a_1 a_2 \cdots a_p = e \right\}.$$

Note that $a_p = (a_1 a_2 \cdots a_{p-1})^{-1}$ is uniquely determined. Then $|S| = n^{p-1}$. Since $p \mid n$, we consequently have $|S| \equiv 0 \pmod{p}$.

Let $\mathbb{Z}_p$ act on S by cyclic permutation, i.e., for $k \in \mathbb{Z}_p$ we have

$$k(a_1, a_2, \ldots, a_p) = (a_{k+1}, a_{k+2}, \ldots, a_p, a_1, a_2, \ldots, a_k).$$

It is clear that this is a group action—$k = 0$ clearly acts as the identity map, and the action is clearly associative.

Here $S_0 = \left\{ (a, a, \ldots, a) \in S \;\middle|\; a \in G \right\}$ since acting for instance by $k = 1$ we see that $a_1 = a_2$, $a_2 = a_3$, et cetera. Crucially we also have $|S_0| > 1$ since at least $(e, e, \ldots e) \in S_0$.

Hence by the lemma $1 < |S_0| \equiv |S| \equiv 0 \pmod{p}$, so $|S_0| \geq p$, implying that there exists some $a \in G$, $a \neq e$, such that $a \cdot a \cdots a = a^p = e$, implying that a has order p since p is a prime. □

Definition 2.1.1 (p-Group)**.** A group G is a ***p-group*** if the order of every element in G is some power of p, where p is a prime.

If H is a subgroup of a group G and H is a p-group, then H is called a ***p-subgroup***.

Corollary 2.1.2. *A finite group G is a p-group if and only if $|G|$ is a power of p.*

Proof. For the forwards direction, if $|G| \neq p^k$, then there exists some prime q with $q \mid |G|$, so by Cauchy's theorem there exists an element of order q, which is a contradiction.

The converse direction follows immediately from Lagrange's theorem. □

Definition 2.1.3 (Normaliser)**.** Let H be a subgroup of a group G. The ***normaliser*** of H in G is defined as

$$N_G(H) = \left\{ g \in G \;\middle|\; gHg^{-1} = H \right\}.$$

Remark 2.1.4. Note how H is a normal subgroup of $N_G(H)$, since for all $g \in N_G(H)$, $gH = Hg$ by definition.

Lemma 2.1.5. *If H is a p-subgroup of a finite group G, then*

$$[N_G(H) : H] \equiv [G : H] \pmod{p}.$$

Proof. Let S be the set of left cosets of H in G, so $|S| = [G : H]$. Let H act on S by left translation.

For $x \in G$ we then have $xH \in S_0$ if and only if $hxH = xH$ for all $h \in H$ if and only if $x^{-1}hxH = H$ for all $h \in H$ if and only if $x^{-1}hx \in H$ for all $h \in H$, which finally is equivalent to $x \in N_G(H)$ by definition.

Hence $|S_0| = [N_G(H) : H]$, which is congruent to $|S|$ modulo p by lemma, and $|S| = [G : H]$ as per above. □

Date: August 22nd, 2019.

Corollary 2.1.6. *If H is a p-subgroup of a finite group G such that $p \mid [G : H]$, then $N_G(H) \neq H$.*

Proof. By the lemma we have $[N_G(H) : H] \equiv [G : H] \equiv 0 \pmod{p}$, so $[N_G(H) : H] > 1$, meaning the two can't be equal. □

2.2 Sylow theorems

Theorem 2.2.1 (First Sylow theorem)**.** *Let G be a group of order $p^n \cdot m$ with $n \geq 1$, p prime, and $\gcd(p, m) = 1$. Then G contains a subgroup of order p^i for all $1 \leq i \leq n$, and every subgroup of p^i is normal in some subgroup of order p^{i+1} for $i < n$.*

Proof. We prove the theorem by induction on i. For $i = 1$, we want to find a subgroup of order $p^1 = p$, but $p \mid |G|$, so by Cauchy's theorem there exists some subgroup $\langle a \rangle$ of G with $|\langle a \rangle| = p$.

Assume H is a subgroup of G of order p^i for $1 \leq i < n$. Then $p \mid [G : H]$ (since there is at least one factor of p left over) and by the previous lemma $N_G(H) \neq H$.

Hence

$$1 < |N_G(H)/H| = [N_G(H) : H] \equiv [G : H] \equiv 0 \pmod{p}.$$

Hence $N_G(H)/H$ is a group and contains an element of order p by Cauchy's theorem. Call the subgroup generated by this element H_1. Then H_1/H is a subgroup of $N_G(H)/H$ of order p, so H_1 is a subgroup of $N_G(H)$ of order

$$|H_1| = |H| \cdot |H_1/H| = p^i \cdot p = p^{i+1}.$$

So $H < H_1 < N_G(H)$, and H is normal in $N_G(H)$, so H is normal in H_1 as well. □

Definition 2.2.2 (Sylow p-subgroup)**.** A subgroup $P \neq G$ of a group G is called a ***Sylow p-subgroup*** if P is a maximal p-subgroup of G, i.e., if $P < H < G$ and H is a p-subgroup, then $P = H$.

Remark 2.2.3. Note that P can be the trivial subgroup. If $|G| = p_1^{n_1} p_2^{n_2} \cdots p_k^{a_k}$ and P is a Sylow p-subgroup, then $|P| = p_i^{n_i}$ if $p = p_i$ for some i, and if $p \neq p_i$ for all $i = 1, 2, \ldots, k$, then $|P| = 1$.

Corollary 2.2.4. *Let G be a group of order $p^n \cdot m$ where p is prime and $\gcd(p, m) = 1$. Let H be a p-subgroup of G. Then*

(*a*) *H is a Sylow p-subgroup of G if and only if $|H| = p^n$, and*

(*b*) *every conjugate of a Sylow p-subgroup is a Sylow p-subgroup.*

Theorem 2.2.5 (Second Sylow theorem)**.** *If H is a p-subgroup of a finite group G and P is any Sylow p-subgroup of G, then there exists some $x \in G$ such that $H < xPx^{-1}$. In particular, any two Sylow p-subgroups of G are conjugate.*

Proof. Let $S = G/P$, the set of left cosets of P in G. Let H act on S by left translation. Then $|S_0| \equiv |S| \pmod{p}$, and $|S| = [G : P] \not\equiv 0 \pmod{p}$ since P has the maximal possible power of p for its order, so $S_0 \neq \varnothing$.

Hence $xP \in S_0$ if and only if $hxP = xP$ for all $h \in H$ if and only if $(x^{-1}hx)P = p$ for all $h \in H$ if and only if $x^{-1}hx \in P$ for all $h \in H$ if and only if $h \in xPx^{-1}$, so $H < xPx^{-1}$.

Hence taking in particular H to be the largest possible p-subgroup, we see that any Sylow p-subgroup is conjugate to it. □

Theorem 2.2.6 (Third Sylow theorem)**.** *If G is a finite group and p a prime, then the number of Sylow p-subgroups of G divides $|G|$ and is of the form $kp+1$ for some integer $k \geq 0$.*

Proof. By the Second Sylow theorem, the number of Sylow p-subgroups is the number of conjugates of any one of them, say P. This number if $[G : N_G(P)]$, and $[G : N_G(P)] \mid |G|$, so the number of Sylow p-subgroups divides $|G|$.

Secondly, let S be the set of all Sylow p-subgroups of G. Let P act on S by conjugation. Then $Q \in S_0$ if and only of $xQx^{-1} = Q$ for all $x \in P$, which is equivalent to $P < N_G(Q)$. Now Q and P are both Sylow p-subgroups of $N_G(Q)$, and Q is normal in $N_G(Q)$ by definition, and P and Q are conjugate by the Second Sylow theorem, so $Q = P$, meaning that $S_0 = \{ P \}$.

Hence since by our oft-used lemma

$$|S| \equiv |S_0| \pmod{p}$$

and $|S_0| = 1$, we have $|S| = kp + 1$ for some integer $k \geq 0$. □

Lecture 3 Review of Ring Theory

3.1 Rings

Definition 3.1.1 (Ring)**.** A ***ring*** $(R, +, \cdot)$ is a set R with two binary operations $+$ and $\cdot$ with the properties that

(*a*) $(R, +)$ is an abelian group,

(*b*) $(ab)c = a(bc)$ for all $a, b, c \in R$, and

(*c*) $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$ for all $a, b, c \in R$.

Example 3.1.2. The integers with ordinary addition and multiplication, written $(\mathbb{Z}, +, \cdot)$, is a ring. ▲

Example 3.1.3. The set of real 2×2 matrices with the usual matrix addition and multiplication, $(M_2(\mathbb{R}), +, \cdot)$, form a ring. ▲

We will have reason to recall rather a lot of standard definitions from ring theory.

Definition 3.1.4 (Commutative ring)**.** If for every a and b in a ring R we have $ab = ba$, then R is a ***commutative ring***.

Definition 3.1.5 (Ring with identity)**.** If a ring R contains an element 1_R such that $1_R a = a1_R = a$ for all $a \in R$, then R is called a ***ring with identity*** or ***ring with unity*** or ***unit ring***.

Date: August 27th, 2019.

Definition 3.1.6 (Zero divisor)**.** An element $a \neq 0$ in a ring R is called a ***zero divisor*** if there exists some $b \neq 0$ in R such that $ab = 0$.

Definition 3.1.7 (Unit)**.** An element $a \neq 0$ in a ring R with identity is called a ***unit*** if there exists some $b \in R$ such that $ab = ba = 1_R$.

Definition 3.1.8 (Integral domain)**.** A commutative ring with identity $1_R \neq 0$ and no zero divisors is called an ***integral domain***.

Definition 3.1.9 (Division ring)**.** A ring with identity in which every nonzero element is a unit is called a ***division ring***.

Definition 3.1.10 (Field)**.** A commutative division ring is called a ***field***.

Definition 3.1.11 (Ring homomorphism)**.** Let R and S be rings. A function $f\colon R \to S$ is a ***homomorphism of rings*** if $f(a + b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$ for all $a, b \in R$.

The ***kernel*** of f is defined as $\ker f = \left\{ r \in R \;\middle|\; f(r) = 0 \right\}$.

Definition 3.1.12 (Ideal)**.** Let R be a ring, and I a subring of R. We call I an ***ideal*** of R if $rI < I$ and $Ir < I$ for all $r \in R$.

Remark 3.1.13. We care about ideals for the same reason that we care about normal subgroups: for any old subgroup H of a group G, the set of left cosets G/H need not have group structure, but it will if H is a normal subgroup.

In the same way, for any old subring S of a ring R, R/S need not have a ring structure, but it does if S is an ideal.

More precisely, if I is an ideal of R, then R/I is a ring with the natural binary operations,

$$(a + I) + (b + I) = (a + b) + I$$

and

$$(a + I)(b + I) = (ab) + I.$$

Note how the first of these is automatic; since $(R, +)$ is an abelian group, as an additive subgroup I is automatically normal.

Exercise 3.1.14. Let $f\colon R \to S$ be a ring homomorphism. Then $\ker f$ is an ideal of R, and $R/\ker f \cong \operatorname{Im} f$ as rings, not just groups.

Solution. We need only check the properties of the multiplication, since the group structure of $(R, +)$ guarantees the right properties of addition.

So first let $a, b \in \ker f$, i.e., $f(a) = f(b) = 0$. Then $f(ab) = f(a)f(b) = 0$, so $ab \in \ker f$, making $\ker f$ a subring of R.

To see that it is an ideal, we play the same game, but this time we take $a \in \ker f$ and $r \in R$. Then $f(ar) = f(a)f(r) = 0 \cdot f(r) = 0$, and similarly $f(ra) = 0$, so $r\ker(f) < \ker(f)$ and $\ker(f)r < \ker(f)$ for all $r \in R$.

To show the first isomorphism theorem, consider the diagram

$$\begin{array}{ccc} R & \xrightarrow{g} & R/\ker f \\ & \searrow^{f} & \downarrow{\scriptstyle h} \\ & & \operatorname{Im} f, \end{array}$$

where g is the projection and h is inclusion, and then $f = h \circ g$. Clearly h is an injection, being the inclusion map, and it remains to show that it is also surjective. But the diagram commutes, and f is of course surjective, so since $f = h \circ g$ must be too. ♦

Definition 3.1.15 (Principal ideal)**.** An ideal $I = \langle a \rangle$ generated by a single element a is called a ***principal ideal***.

A ***principal ideal domain***, or ***PID*** is an integral domain in which every ideal is principal.

Example 3.1.16. The integers $(\mathbb{Z}, +, \cdot)$ form a principal ideal domain, specifically because it possesses a division algorithm.

For the same reason, the set of polynomials $k[x]$ over a field k is a principal ideal domain. ▲

In the sequel, unless otherwise stated, rings under consideration will be commutative rings with identity $1 \neq 0$.

Definition 3.1.17 (Prime ideal)**.** A ***prime ideal*** $P \neq R$ in a ring R is an ideal such that for all $a, b \in R$, if $ab \in P$, then $a \in P$ or $b \in P$.

Example 3.1.18. The motivation for this definition comes from mimicking the prime numbers in $\mathbb{Z}$. In $\mathbb{Z}$, the primes of course are $2, 3, 5, 7, \ldots$, numbers with the property that their only positive divisors are 1 and themselves. Another equivalent description is to say that if $p \mid ab$, with p prime, then either $p \mid a$ or $p \mid b$. This is the definition we generalise.

Consider the prime ideals $\langle 2 \rangle, \langle 3 \rangle, \langle 5 \rangle, \langle 7 \rangle, \ldots$. The division property directly translated to $ab \in \langle p \rangle$ implying that $a \in \langle p \rangle$ or $b \in \langle p \rangle$.

Note also how we require, in the definition, that a prime ideal $P \neq R$. One (of many) reasons for this is that otherwise $R = \langle 1 \rangle$ would be a prime ideal, corresponding in $\mathbb{Z}$ to 1 being a prime number, which we generally don't want (for reasons like unique factorisation).

That said, note how (maybe sneakily), the trivial ideal 0 is a prime ideal in $\mathbb{Z}$. ▲

Theorem 3.1.19. *Let R be a commutative ring with identity $1 \neq 0$. Let P be an ideal of R. Then P is prime if and only if R/P is an integral domain.*

Proof. In the forward direction, we need to show that R/P has no zero divisors. Suppose, to that end, that $(a + P)(b + P) = P$ (since P is the additive identity in R/P). In other words, $(ab) + P = P$, implying that $ab \in P$. But since P is a prime ideal, this implies $a \in P$ or $b \in P$, equivalent, respectively, to $a + P = P$ or $b + P = P$.

For the converse direction, suppose $ab \in P$. This implies $(ab) + P = P$, so $(a + P)(b + P) = P$. But R/P is an integral domain, so has no zero divisors, meaning that either $a + P = P$ or $b + P = P$, ergo $a \in P$ or $b \in P$. □

Definition 3.1.20 (Maximal ideal)**.** An ideal M in a ring R is called ***maximal*** if $M \neq R$ and for every ideal N such that $M \subset N \subset R$, we have $N = M$ or $N = R$.

Example 3.1.21. In $\mathbb{Z}$, the ideal $\langle 2 \rangle$ is maximal. A good way to think of this is to consider some element $m \notin \langle 2 \rangle$, meaning that $\gcd(m, 2) = 1$. By Bézout's

lemma, there must then exist $k, h \in \mathbb{Z}$ such that $km + 2h = 1$. So if we were to have $\langle 2\rangle \subset \langle m\rangle \subset \mathbb{Z}$, then $1 \in \langle m\rangle$, since 1 would be a linear combination of things in $\langle m\rangle$, so it is the whole ring.

For precisely the same reason $\langle p\rangle$ is maximal in $\mathbb{Z}$ for all prime numbers p.

On the other hand, $\langle mn\rangle \subset \langle m\rangle$, so indeed $\langle p\rangle$ are the only maximal ideals in $\mathbb{Z}$. ▲

Theorem 3.1.22. *Let R be a commutative ring with identity $1 \neq 0$. Let M be an ideal of R. Then M is maximal if and only if R/M is a field.*

Hence all maximal ideals are prime ideals, since all fields are integral domains.

Proof. For the forward direction, let $a \notin M$, so $a + M \neq M$. Then $\langle a\rangle + M = R$ since M is maximal. Since $1 \in R$, we get $ar + m = 1$ for some $r \in R$ and $m \in M$, meaning that $(ar) + M = 1 + M$, or $(a + M)(r + M) = 1 + M$, so $(a + M)$ has a multiplicative inverse in R/M.

For the converse direction, suppose $M \subsetneq N \subset R$, with N an ideal. We need to show that $N = R$. Take $a \in N \setminus M$. Then $a + M \neq M$ has a multiplicative inverse in R/M, being a field, i.e., there exists some $r \in R$ such that $(a + M)(r + M) = 1 + M$.

But this means $(ar) + M = 1 + M$, implying that $1 - ar \in M \subset N$. Hence

$$1 = (1 - ar) + ar \in N$$

since $1 - ar \in N$ and $ar \in N$ (since $a \in N$ and N is an ideal), so $N = R$. □

Remark 3.1.23. This means that R is a field if and only if the zero ideal $0 = \langle 0\rangle$ is maximal. The forwards direction is trivial: a field has only two ideals, 0 and itself, and maximal ideals are by definition not the whole ring, so 0 is maximal.

The converse direction is our above theorem: if 0 is maximal, then $R/0 = R$ is a field.

3.2 Solutions to algebraic equations

The main question we are looking to answer in this class is the following. Let k be a field, and consider some polynomial equation

$$a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_{n-1}x + a_n = 0$$

where $a_i \in k$ and $a_0 \neq 0$. Since $a_0 \neq 0$ and we are in a field, we can divide by a_0 and acquire a monic polynomial.

The question is this: is it possible to solve this equation with radicals, in the sense of writing down the solutions to the equation in terms of the coefficients, multiplication, division, addition, and subtraction, along with various radicals?

Take, for instance, $k = \mathbb{Q}$, $k = \mathbb{R}$, or $k = \mathbb{C}$.

Example 3.2.1. Let $n = 1$, so that we are solving $x + a = 0$. Clearly $x = -a$, so the answer is yes. ▲

Example 3.2.2. If $n = 2$ we are solving $x^2 + ax + b = 0$, and this time (by completing the square),

$$x = \frac{-a \pm \sqrt{a^2 - 4b}}{2},$$

so again the answer is yes. ▲

Example 3.2.3. When $n = 3$, the equation becomes

$$x^3 + ax^2 + bx + c = 0.$$

The solution then looks like

$$x = -\frac{a}{3} + \omega^i \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} + \omega^{3-i} \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}}$$

where

$$p = b - \frac{a^2}{3}, \quad q = c - \frac{ab}{3} + \frac{2a^3}{27}, \quad \text{and} \quad \omega = \frac{-1 + \sqrt{-3}}{2}$$

for $i = 0, 1, 2$, so again the answer is yes. ▲

Example 3.2.4. If $n = 4$, we are solving $x^4 + ax^3 + bx^2 + cx + d = 0$. This time

$$x = -\frac{a}{4} \pm \sqrt{-\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - r}}$$

if $q = 0$ and

$$x = -\frac{a}{4} \pm \frac{A}{2} \pm \sqrt{-\frac{t_0}{2} - \frac{p}{4} - \frac{q}{4a}}$$

if $q \neq 0$, where

$$p = b - \frac{3a^2}{8}, \quad q = c - \frac{ab}{2} + \frac{a^3}{8}, \quad r = d - \frac{ac}{4} + \frac{a^2 b}{16} - \frac{3a^4}{256},$$

and

$$A = \sqrt{2t_0 - p},$$

where finally t_0 is any root of $8t^3 - 4pt^2 - 8rt + 4pr - q^2 = 0$. ▲

Fascinatingly, and one of the goals of this class, there is no such formula in general if $n \geq 5$.

That said, there are some special cases.

Example 3.2.5. Consider $x^2 - 1 = 0$, for which clearly $x = \pm 1$. Similarly, $x^3 - 1 = (x - 1)(x^2 + x + 1) = 0$, so we can solve for x with the quadratic formula.

The case $x^4 - 1 = 0$ is uninteresting, since it factors directly as $(x^2 - 1)(x^2 + 1) = 0$, which we can handle as above.

For $x^5 - 1 = 0$ we again factor as $(x - 1)(x^4 + x^3 + x^3 + x^2 + x + 1) = 0$, and so we are left with finding roots of the second factor. The standard trick here is to notice that this looks nice if we divide through by x^2, and taking $y = x + \frac{1}{x}$ we get

$$y^2 + y - 1 = 0,$$

which we can solve with the quadratic equation again.

Likewise for $x^7 - 1 = 0$ we factor out $x - 1$ and we're left with $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = 0$, which we divide through by x^3 and use the same trick to get $y^3 + y^2 - 2y - 1 = 0$. ▲

It turns out, but is highly nontrivial, that $x^n - 1 = 0$ in general can have its roots written in terms of radicals. This is due to Gauss around 1800.

Later on, Abel around 1820 showed that if the Galois group of the algebraic extension is abelian (all words we will make sense of shortly), then the roots can be expressed by radicals.

More generally, Galois, around 1830, finally solved the problem in some kind of generality by showing that the roots of an algebraic equation can be expressed by radicals if and only if the Galois group of the extension is solvable.

Lecture 4 Field Extensions

4.1 Algebraic and transcendental numbers

Definition 4.1.1 (Field extension)**.** Let k be a field and let E be a field containing k. Then we say that E/k is a ***field extension***.

Of some import, E is a vector space over k, and hence it has a dimension over k, denoted

$$\dim_k(E) = [E : k],$$

which we call the ***degree*** of the extension E/k.

Note that the degree of a field extension might be infinite.

Example 4.1.2. The complex numbers $\mathbb{C}$ is an extension of degree 2 of $\mathbb{R}$. ▲

Example 4.1.3. The real numbers $\mathbb{R}$ is an extension of infinite degree over $\mathbb{Q}$. ▲

Definition 4.1.4 (Algebraic and transcendental numbers)**.** Let E/k be a field extension. An element $\alpha \in E$ is called ***algebraic*** over k if

$$a_0\alpha^n + a_1\alpha^{n-1} + \ldots + a_{n-1}\alpha + a_n = 0$$

for some $a_i \in k$ not all equal to zero. In other words, α is a root of some nonzero polynomial

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \in k[x].$$

On the other hand, an element $\alpha \in E$ is said to be ***transcendental*** over k if it is not algebraic over k.

Example 4.1.5. For instance, $\sqrt{2}$ is algebraic over $\mathbb{Q}$ since it is a root of $x^2 - 2$, but π is transcendental over $\mathbb{Q}$. This second fact is very much not obvious, and was proved in 1882 by Lindemann. ▲

Let E/k be a field extension and fix an $\alpha \in E$. Consider the evaluation homomorphism $\varphi_\alpha \colon k[x] \to E$ defined by $f(x) \mapsto f(\alpha)$. Then $\ker \varphi_\alpha$ is an ideal of $k[x]$, which is an integral domain, meaning that $\ker \varphi_\alpha = \langle p(x) \rangle$ for some $p(x) \in k[x]$.

There are two cases to consider. First, if $\ker \varphi_\alpha = \langle 0 \rangle$. This is equivalent to α being transcendental, since it means the only polynomial in $k[x]$ with α as

Date: August 29th, 2019.

a root is 0, and it is also equivalent with φ_α being injective, since its kernel is trivial.

Second, if $\ker \varphi_\alpha = \langle p(x) \rangle \neq \langle 0 \rangle$. Then $p(\alpha) = 0$, so α is algebraic over k, and by the First isomorphism theorem,

$$k[x]/\langle p(x) \rangle \cong \operatorname{Im} \varphi_\alpha \subset E.$$

Since E is a field, and hence in particular an integral domain, $\operatorname{Im} \varphi_\alpha$ must also be an integral domain. But we showed last time that this is equivalent with $\langle p(x) \rangle$ being a prime ideal, which further implies $p(x)$ is irreducible (since of $a(x)b(x) \in \langle p(x) \rangle$, either $a(x) \in \langle p(x) \rangle$ or $b(x) \in \langle p(x) \rangle$). But the ideal generated by an irreducible polynomial must be maximal, so $k[x]/\langle p(x) \rangle$ is a field.

Hence

$$\begin{aligned} \operatorname{Im} \varphi_\alpha &= \left\{ f(\alpha) \;\middle|\; f \in k[x] \right\} = k[\alpha] \\ &= \left\{ a_n \alpha^n + \ldots + a_1 \alpha + a_0 \;\middle|\; a_i \in k \text{ and } n \in \mathbb{N} \setminus \{ 0 \} \right\} \end{aligned}$$

is a field.

In summary, then, if α is algebraic over k, then $k[\alpha]$ is a field.

4.2 Algebraic extensions

Definition 4.2.1 (Algebraic extension)**.** A field extension E/k is ***algebraic*** if every element of E is algebraic over k.

Proposition 4.2.2. *Every finite extension is algebraic.*

Proof. We have $\dim_k(E) = [E : k] = n < \infty$. Let $\alpha \in E$ and consider the set $\left\{ 1, \alpha, \alpha^2, \ldots, \alpha^n \right\} \subset E$. This set contains $n+1$ elements, but E is n-dimensional as a vector space over k, so it must be k-linearly dependent. In other words there exist $a_i \in k$ not all zero such that

$$a_0 \cdot 1 + a_1 \alpha + \ldots + a_n \alpha^n = 0,$$

meaning that α is algebraic over k. □

The converse is not true, i.e., there are algebraic extensions that aren't finite.

Example 4.2.3. Consider $\mathbb{C} \supset \overline{\mathbb{Q}}$, the set of all elements algebraic over $\mathbb{Q}$. This is a field. To see this, take any two elements $a, b \in \overline{\mathbb{Q}}$. Since a is algebraic over $\mathbb{Q}$, $\mathbb{Q}[\alpha]$ is a field by the above discussion, and so moreover is b over $\mathbb{Q}[\alpha]$, so $\mathbb{Q}[\alpha, \beta]$ contains both their inverses and products and so forth, and these extensions are contained in $\overline{\mathbb{Q}}$.

Moreover, $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$. The easiest way to see this is to note that $p_n(x) = x^n - 2$ is an irreducible polynomial over $\mathbb{Q}$ for all $n = 1, 2, 3, \ldots$ (since it is Eisenstein). But $p_n(\alpha) = 0$ for some $\alpha \in \mathbb{C}$ by the Fundamental theorem of algebra, so $\alpha \in \overline{\mathbb{Q}}$. But that means the extension we get by just adjoining α to $\mathbb{Q}$ is of degree n over $\mathbb{Q}$, and this is contained in $\overline{\mathbb{Q}}$ for all n, so the degree of $\overline{\mathbb{Q}}$ over $\mathbb{Q}$ is larger than all positive integers n. ▲

Proposition 4.2.4. *Let $E \supset F \supset k$ be a chain of field extensions. Suppose $\left\{ x_i \;\middle|\; i \in I \right\}$ is a basis of F/k and $\left\{ y_j \;\middle|\; j \in J \right\}$ is a basis of E/F. Then $\left\{ x_i y_j \;\middle|\; i \in I \text{ and } j \in J \right\}$ is a basis of E/k.*

Proof. Since $\{ y_j \}$ make a basis of E/F, we have for any $\alpha \in E$ and some $a_j \in F$, not all zero,

$$\sum_{j \in J} a_j y_j = \alpha.$$

Then since $\{ x_i \}$ is a basis of F/k, we have for some $b_{ij} \in k$, not all zero,

$$\sum_{i \in I} b_{ij} x_i = a_j$$

for any $a_j \in F$. Combining these we get

$$\sum_{i \in I} \sum_{j \in J} b_{ij} x_i y_j = \alpha,$$

so some k-linear combination of $x_i y_j$ is α. □

From this proposition we get immediately that

$$[E : k] = [E : F] \cdot [F : k].$$

Corollary 4.2.5. *Let $E \supset F \supset k$ be a chain of field extensions. The extension E/k is finite if and only if E/F and F/k are finite.*

Definition 4.2.6 (Simple extension)**.** Let E/k be a field extension, and let $\alpha \in E$. Define $k(\alpha)$ to be the smallest subfield of E containing k and α. We call $k(\alpha)$ a ***simple extension*** of k.

Note that $k[\alpha] = \{ f(\alpha) \,|\, f(x) \in k[x] \}$ is the smallest subring of E containing k and α. Since k is a field, $k[\alpha]$ is a domain, meaning that it has a quotient field, so

$$k(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} \;\middle|\; f(x), g(x) \in k[x] \right\}.$$

Hence $k(\alpha)$ is the quotient field of $k[\alpha]$, and if α is algebraic over k, $k[\alpha] = k(\alpha)$.

Lecture 5 Algebraic Field Extensions

5.1 Minimal polynomials

Definition 5.1.1 (Minimal polynomial)**.** Let E/k be a field extension and let $\alpha \in E$. Suppose α is algebraic over k, meaning that α is the root of some polynomial in $k[x]$. Then monic polynomial in $k[x]$ of smallest degree with α as a root, denoted $\mathrm{Irr}(\alpha; k, x)$, is called the ***minimal*** or ***irreducible polynomial*** of α over k.

We discussed last time how the evaluation homomorphism $\varphi_\alpha \colon k[x] \to E$ defined by $f(x) \mapsto f(\alpha)$ has as kernel $\ker \varphi_\alpha = \langle p(x) \rangle$ for some $p(x) \in k[x]$, since there being a division algorithm on $k[x]$ means it is a principal ideal domain. Then we must have $\ker \varphi_\alpha = \langle \mathrm{Irr}(\alpha; k, x) \rangle$ by definition.

Hence also $k[x]/\langle \mathrm{Irr}(\alpha; k, x) \rangle \cong k[\alpha]$, where we can view both (being isomorphic) as field extensions of, and hence vector spaces over, k.

Date: September 3rd, 2019.

Supposing for sake of argument that $\mathrm{Irr}(\alpha; k, x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0$ in $k[x]/\langle \mathrm{Irr}(\alpha; k, x)\rangle$, we have then that $\left\{ 1, x, x^2, \ldots, x^{n-1} \right\}$ is a basis for $k[x]/\langle \mathrm{Irr}(\alpha; k, x)\rangle$ over k, so

Proposition 5.1.2. *Suppose α is algebraic over k. Then*

$$[k(\alpha) : k] = \deg \mathrm{Irr}(\alpha; k, x).$$

Remark 5.1.3. Let $E \supset F \supset k$ be a chain of fields. If $\alpha \in E$ is algebraic over k, then α is also algebraic over F. This is fairly obvious: α being algebraic over k means there is some polynomial with coefficients in k for which α is a root, but since k is contained in F, that polynomial also has coefficients in F.

Proposition 5.1.4. *Let E/k be a field extension. Let $\alpha_1, \alpha_2, \ldots, \alpha_n \in E$ be algebraic over k. Then $k(\alpha_1, \alpha_2, \ldots, \alpha_n)/k$ is algebraic.*

Proof. Working one element at a time, if α_1 is algebraic over k, then $[k(\alpha_1) : k] < \infty$. Next α_2 being algebraic over k means it is also algebraic over $k(\alpha_1)$ by the above remark, and so $[k(\alpha_1, \alpha_2) : k(\alpha_1)] < \infty$, and

$$[k(\alpha_1, \alpha_2) : k] = [k(\alpha_1, \alpha_2) : k(\alpha_1)] \cdot [k(\alpha_1) : k] < \infty,$$

so $k(\alpha_1, \alpha_2)/k$ is an algebraic extension. Now repeat this argument. □

Maybe counterintuitively, this is true even if we aren't adjoining a finite number of α:

Proposition 5.1.5. *Let E/k be a field extension, and let $\alpha_\lambda \in E$ be algebraic over k for all $\lambda \in \Lambda$, some arbitrary index set. Then $k(\alpha_\lambda \,|\, \lambda \in \Lambda)/k$ is algebraic.*

Proof. If $\beta \in k(\alpha_\lambda \mid \lambda \in \Lambda)$, then $\beta = a_1\alpha_{\lambda_1} + a_2\alpha_{\lambda_2} + \ldots + a_n\alpha_{\lambda_n}$, with $a_i \in k$ and $\alpha_{\lambda_i} \in \Lambda$. The crucial point is that β is a k-linear combination of only *finitely* many α_λ.

Hence $\beta \in k(\alpha_{\lambda_1}, \alpha_{\lambda_2}, \ldots, \alpha_{\lambda_n})$, which is an algebraic extension of k by the above proposition, and so β is algebraic over k. □

Though an element being algebraic by definition means there exists some polynomial of which it is a root, it is generally speaking hard to find the polynomial, and comparatively easy to show that the element is algebraic.

Proposition 5.1.6. *Let $E \supset F \supset k$ be a chain of field extensions. Then E/k is algebraic if and only if E/F and F/k are algebraic.*

Proof. The forward direction is trivial, and more to the point we showed it in an earlier remark.

For the converse direction we need a little bit more care. Let $\beta \in E$ be algebraic over F, so that

$$p(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in F[x]$$

with $p(\alpha) = 0$. Then β is algebraic over $k(a_{n-1}, a_{n-2}, \ldots, a_0)$, meaning that $[k(a_{n-1}, \ldots, a_0, \beta) : k(a_{n-1}, \ldots, a_0)] < \infty$. Each of these $a_i \in F$, since F/k is algebraic by hypothesis, are algebraic over k, so $k(a_{n-1}, \ldots, a_0)/k$ is algebraic, meaning that $[k(a_{n-1}, \ldots, a_0) : k] < \infty$.

Therefore finally $[k(a_{n-1}, a_{n-2}, \ldots, a_0, \beta) : k] < \infty$, and so β is algebraic also over k. □

Let E/k be a field extension and let $\alpha \in E$ be algebraic over k. Pick any $\beta \neq 0$ in $k[\alpha] = k(\alpha)$ (equal since α is algebraic over k). A natural question to ask is this: how would we compute the inverse β^{-1} in terms of α?

Given the minimal polynomial $\mathrm{Irr}(\alpha; k, x) = p(x) \in k[x]$ of α over k, as well as how to write β in terms of powers of α (which form a basis of $k[\alpha]$ over k, of course), say $\beta = g(\alpha)$ for some $g(x) \in k[x]$, we can do this by essentially the same algorithm one uses to compute inverses in $\mathbb{Z}/n\mathbb{Z}$.

Note that $p(x)$ is irreducible and $p(x) \nmid g(x)$ (since otherwise $g(\alpha) = \beta = 0$), meaning that $\gcd(p(x), g(x)) = 1$. Hence by the Euclidean algorithm repeatedly there exist $A(x), B(x) \in k[x]$ such that

$$A(x)p(x) + B(x)g(x) = 1.$$

Evaluating this at $x = \alpha$, we get $B(\alpha)g(\alpha) = 1$, so and $g(\alpha) = \beta$, so $b^{-1} = B(\alpha)$.

5.2 Composites of fields

Definition 5.2.1 (Composite field)**.** Let $E, F \subset L$ be subfields of L. The smallest subfield of L that contains both E and F is called the ***composite*** of E and F, denoted EF.

Recall how in a ring R, if A and B are ideals, then we define

$$AB = \left\{ \sum_{\text{finite}} a_i b_i \;\middle|\; a_i \in A, b_i \in B \right\}$$

is the smallest ideal containing A and B. In general, however,

$$EF \neq \left\{ \sum_{\text{finite}} e_i f_i \;\middle|\; e_i \in E, f_i \in F \right\}$$

since the right-hand side does not include inverses, unless:

Proposition 5.2.2. *Suppose we have a chain of field extensions $k \subset E \subset L$ and $k \subset F \subset L$. Suppose E/k or F/k is algebraic. Then*

$$EF = \left\{ \sum_{\textit{finite}} e_i f_i \;\middle|\; e_i \in E, f_i \in F \right\}.$$

Proof. We have, in general, $EF = E(F) = F(E)$, since by definition this includes the inverses. Suppose, without loss of generality, that F/k is algebraic. Then

$$EF = E(f \mid f \in F) = E[f \mid f \in F] = \left\{ \sum_{\text{finite}} e_i f_i \;\middle|\; e_i \in E, f_i \in F \right\}. \qquad \square$$

5.3 Algebraic closure

Let k be a field. We want to construct a field $K \supset k$ such that K/k is algebraic and every irreducible polynomial in $K[x]$ has a root in K.

Definition 5.3.1 (Algebraically closed)**.** A field L is called ***algebraically closed*** if every polynomial in $L[x]$ has a root in L.

Example 5.3.2. The complex numbers $\mathbb{C}$ are algebraically closed. The reals $\mathbb{R}$ are not, however: for instance $f(x) = x^2 + 1 \in \mathbb{R}[x]$ has no roots in $\mathbb{R}$. ▲

Remark 5.3.3. (*i*) If L is algebraically closed, then all the roots of every polynomial in $L[x]$ are in L (one is by definition; divide that factor away and repeat). Hence

(*ii*) if L is algebraically closed, then every polynomial can be written as a product of linear factors in L.

Note that we are after an extension that is both algebraic over k and algebraically closed. First we give a partial result:

Theorem 5.3.4. *Let k be an arbitrary field. Then there exists an extension E/k such that E is algebraically closed.*

To prove it we use the following lemma:

Lemma 5.3.5. *Let $p(x) \in k[x]$ be irreducible. Then there exists some field extension E/k such that E contains a root of $p(x)$.*

Proof. Let $E = k[x]/\langle p(x)\rangle$. This is a field since $p(x)$ is irreducible, whence $\langle p(x)\rangle$ is maximal.

Now k embeds naturally in E by $a \mapsto a + \langle p(x)\rangle$, which is one-to-one, so we can identify k as a subfield of E, say $\hat{k}$. So if $p(x) = a_n x^n + \ldots + a_0 \in k[x]$, this corresponds to $(a_n + \langle p(x)\rangle)x^n + \ldots + (a_0 + \langle p(x)\rangle) \in \hat{k}[x]$, so letting $\bar{x} = x + p(x)$, $p(\bar{x}) = (a_n x^n + \ldots + a_0) + \langle p(x)\rangle = p(x) + \langle p(x)\rangle = 0$ in E. Hence E has a zero of $p(x)$ inside of it. □

Remark 5.3.6. (*i*) Let $f(x) \in k[x]$. Then there exists some extension E/k such that E has a root of $f(x)$ in it. This follows immediately: if $f(x)$ is irreducible, then it's the lemma, and if it isn't, factor it into irreducible parts and use the lemma.

(*ii*) Let $f_1(x), f_2(x), \ldots, f_n(x) \in k[x]$. Then there exists a field extension E/k such that E has a root of $f_i(x)$ for every i.

Lecture 6 Algebraic Closure

6.1 Existence of algebraic closure

We start by proving the theorem toward the end of last lecture.

Proof. Let $\left\{ f_\lambda(x) \;\middle|\; \lambda \in \Lambda \right\}$ be the set of all irreducible polynomials of degree > 1 in $k[x]$. Let $\left\{ x_\lambda \;\middle|\; \lambda in \Lambda \right\}$ be a set of variables, one for each irreducible polynomial. Define $R \coloneqq k[x_\lambda \mid \lambda \in \Lambda]$, and let A be the ideal of R generated by $f_\lambda(x_\lambda)$ for every $\lambda \in \Lambda$.

Then $A \neq R$, i.e., A is a proper ideal of R. By way of contradiction, suppose not. Then

$$1 = g_{\lambda_1} f_{\lambda_1}(x_{\lambda_1}) + g_{\lambda_2} f_{\lambda_2}(x_{\lambda_2}) + \ldots + g_{\lambda_r} f_{\lambda_r}(x_{\lambda_r})$$

Date: September 5th, 2019.

for some finite set $\{ \lambda_1, \lambda_2, \ldots, \lambda_r \} \subset \Lambda$, and $g_{\lambda_1}, g_{\lambda_2}, \ldots, g_{\lambda_r} \in R$. By the second remark just above, there exists an extension F of k such that F has a root, say α_λ, of $f_{\lambda_i}(x_{\lambda_i})$ for each $i = 1, 2, \ldots, r$. But then if we evaluate the equation above at $x_{\lambda_i} = \alpha_{\lambda_i}$, for $i = 1, 2, \ldots, r$, we get $1 = 0$, a contradiction.

Hence A is a proper ideal of R. Now R/A might not be a field, since A need not be maximal, but there must exist a maximal ideal containing A, say M. Then $E_1 \coloneqq R/M$ is a field. Letting $\alpha_\lambda = x_\lambda + M$, then we get

$$f_\lambda(\alpha_\lambda) = f_\lambda(x_\lambda) + M = 0$$

since $f_\lambda \in A \subset M$. In other words, every irreducible polynomial in $k[x]$ has a root in E_1.

This is not quite what we need—we want every every polynomial in $E_1[x]$ to have a root in E_1. This needn't be the case, but we can repeat this process, taking E_1 in place of k, obtaining a new field E_2, and so on:

$$k = E_0 \subset E_1 \subset E_2 \subset \ldots \subset E_n \subset \ldots,$$

and every irreducible polynomial in $E_n[x]$ has a root in E_{n+1} for all $n \geq 0$. Now set

$$E \coloneqq \bigcup_{n=0}^{\infty} E_n.$$

This is a field (since any two $a, b \in E$ belong to some E_n, which is a field). Moreover for any irreducible $p(x) \in E[x]$ we must have $p(x) \in E_m[x]$ for some m, and so E_{m+1} contains a root of $p(x)$, but $E_{m+1} \subset E$, so E also contains a root of $p(x)$. Therefore E is algebraically closed. □

Definition 6.1.1 (Algebraic closure)**.** An extension K of a field k is an ***algebraic closure*** of k if K/k is algebraic and K is algebraically closed.

Lemma 6.1.2. *Let E/k be a field extension and let A be the set of all elements in E algebraic over k. Then A is a field.*

Moreover, if E is algebraically closed, then A is algebraically closed.

Proof. Take $\alpha, \beta \in A$. Then α is algebraic over k, so $[k(\alpha) : k] < \infty$, and β is algebraic over k, and hence over $k(\alpha)$, so $[k(\alpha, \beta) : k(\alpha)] < \infty$. This means that

$$[k(\alpha, \beta) : k] = [k(\alpha, \beta) : k(\alpha)] \cdot [k(\alpha) : k] < \infty,$$

so $k(\alpha, \beta)/k$ is algebraic, meaning that $\alpha \pm \beta$, $\alpha\beta$, and α/β are all in $k(\alpha, \beta)$, so they are in A, and hence A is a field.

Now assume E is algebraically closed, and let $f(x) \in A[x]$. Then since $A[x] \subset E[x]$, and E is algebraically closed, $f(x)$ has a root α in E. We need to show that such a root is algebraic over k, so that it is also in A.

Now writing $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, we have α is algebraic over $k(a_{n-1}, \ldots, a_0)$. Hence since $[k(a_{n-1}, \ldots, a_0) : k] < \infty$ and $[k(a_{n-1}, \ldots, a_0, \alpha) : k(a_{n-1}, \ldots, a_0)] < \infty$, we have

$$[k(a_{n-1}, \ldots, a_0, \alpha) : k] < \infty$$

meaning that $k(a_{n-1}, \ldots, a_0, \alpha)$ is algebraic over k, so α is algebraic over k. Hence $\alpha \in A$, and so A is algebraically closed. □

Corollary 6.1.3. *Let k be a field. Then there exists an extension K/k such that K is algebraic over k and K is algebraically closed. In other words, k has an algebraic closure.*

Lecture 7 Field Embeddings

7.1 Uniqueness of algebraic closure

Definition 7.1.1. An ***embedding*** of a field E into another field L is an injective homomorphism from E to L. That is, $\tau\colon E \to E' \subset L$, with $E' = \tau(E) \cong E$ as fields.

Example 7.1.2. Consider the field $E = \mathbb{Q}(\sqrt{2})$. We can embed E into $\mathbb{C}$ by the identity mapping. On the other hand, noting how

$$\mathbb{Q}(\sqrt{2}) = \left\{ a + \sqrt{2}b \;\middle|\; a, b \in \mathbb{Q} \right\},$$

$\tau\colon \mathbb{Q}(\sqrt{2}) \to \mathbb{C}$ defined by $\tau\colon a + b\sqrt{2} \mapsto a - b\sqrt{2}$ is also an embedding of $\mathbb{Q}(\sqrt{2})$ into $\mathbb{C}$.

These are the only two, as it turns out. To see this, suppose we have an embedding $\tau\colon \mathbb{Q}(\sqrt{2}) \hookrightarrow \mathbb{C}$. This is a homomorphism, so $\tau(1) = 1$, and hence also for $n \in \mathbb{Z}$ we have $\tau(n) = n$. It must also preserve quotients, so for any $r \in \mathbb{Q}$ we have $\tau(r) = r$. So τ must fix $\mathbb{Q}$, meaning that

$$\tau(a + b\sqrt{2}) = \tau(a) + \tau(b)\tau(\sqrt{2}) = a + b\tau(\sqrt{2}),$$

and therefore τ is completely determined by its value on $\sqrt{2}$. However

$$\tau(\sqrt{2})^2 = \tau(\sqrt{2})\tau(\sqrt{2}) = \tau(\sqrt{2}\sqrt{2}) = \tau(2) = 2,$$

so $\tau(\sqrt{2})$ must be some kind of square root of 2, so the only options are $\tau(\sqrt{2}) = \sqrt{2}$, leading to the identity mapping, or $\tau(\sqrt{2}) = -\sqrt{2}$, leading to the second embedding above. ▲

Example 7.1.3. Let $E = \mathbb{Q}(\sqrt[3]{2})$. We wish to list all embeddings of E into $\mathbb{C}$.

Now

$$\mathbb{Q}(\sqrt[3]{2}) = \left\{ a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \;\middle|\; a, b, c \in \mathbb{Q} \right\},$$

where the dimension is rightly 3 since the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ is $x^3 - 2$. Now go construct an embedding $\tau\colon E \hookrightarrow \mathbb{C}$ we need only fix $\tau(\sqrt[3]{2})$ by the same reasoning as above, and similarly $\tau(\sqrt[3]{2})^3 = 2$.

The equation $x^3 - 2 = 0$ has roots $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, and $\sqrt[3]{2}\omega^2$, where

$$\omega = \frac{-1 + \sqrt{-3}}{2} \qquad \text{and} \qquad \omega^2 = \frac{-1 - \sqrt{-3}}{2}$$

are the nontrivial cubic roots of unity.

Hence there are three possible embeddings: the identity mapping, from $\tau(\sqrt[3]{2}) = \sqrt[3]{2}$; the embedding from $\tau(\sqrt[3]{2}) = \sqrt[3]{2}\omega$; and the one from $\tau(\sqrt[3]{2}) = \sqrt[3]{2}\omega^2$. ▲

Example 7.1.4. When $E = \mathbb{Q}(\sqrt[3]{2}, \omega)$, there are six possible embeddings $\tau\colon E \hookrightarrow \mathbb{C}$; there are three options for $\tau(\sqrt[3]{2})$, and the minimal polynomial of ω is of degree two, since $0 = x^3 - 1 = (x - 1)(x^2 + x + 1)$, so there are two possible options for $\tau(\omega)$. ▲

Date: September 10th, 2019.

More generally,

Example 7.1.5. Consider the field $\mathbb{Q}(\alpha)$, with α algebraic over $\mathbb{Q}$, and an embedding $\tau\colon \mathbb{Q}(\alpha) \hookrightarrow \mathbb{C}$. Then α has a minimal polynomial over $\mathbb{Q}$, living in $\mathbb{Q}[x]$, so τ doesn't affect its coefficients, meaning that $\tau(\alpha)$ must be a root of the same minimal polynomial. ▲

Definition 7.1.6. Consider a diagram of field extensions

$$\begin{array}{ccc} E & \xrightarrow{\quad\tau\quad} & L \\ \Big| & & \Big| \\ k & \xrightarrow[\cong]{\sigma} & k' = \sigma(k) \end{array}$$

Suppose that $\tau|_k = \sigma$. Then we say that τ is a ***lift*** of σ.

Suppose $k' = k$, $\sigma = \mathrm{Id}$. Then we call τ a ***k-embedding***, i.e., $\tau|_k = \mathrm{Id}$, so the embedding fixes k.

Proposition 7.1.7. *Consider the diagram*

$$\begin{array}{ccc} & & L \\ & & \Big| \\ & E & \\ {\scriptstyle algebraic}\Big| & & \Big| \\ k & \xrightarrow[\cong]{\sigma} & k' \end{array}$$

of fields, where L is algebraically closed. Then there exists a field $E' \subset L$ and an embedding τ of E into L such that $\tau(E) = E'$ and $\tau|_k = \sigma$.

In other words, σ can be lifted to any algebraic extension, provided L is algebraically closed.

Proof. This is a proof by Zorn's lemma. To that end, let

$$S = \left\{ (F, \rho) \;\middle|\; E \supset F \supset k, \rho\colon F \hookrightarrow L, \rho|_k = \sigma \right\},$$

the family of extensions of k and lifts of σ. This family is nonempty since at the very least $(k, \sigma) \in S$. We can equip this set with a partial order by $(F_1, \rho_1) < (F_2, \rho_2)$ if and only if $F_1 \subset F_2$ and $\rho_2|_{F_1} = \rho_1$. Thus S is a partially ordered set, and so if we can show that every ***chain***, or totally ordered subset, of S has an upper bound, then by Zorn's lemma S has a maximal element.

But this is not too hard: let $C \subset S$ be totally ordered. Then take

$$(F, \rho) = \bigcup_{(F_\lambda, \rho_\lambda) \in C} (F_\lambda, \rho_\lambda),$$

where by union on the fields we mean simply set unions, and by union of the embeddings we mean that ρ on an element from a field F_λ just uses the corresponding ρ_λ. That this is an upper bound is clear, also $E \subset F \subset k$, with $\rho|_k = \sigma$, so $(F, \rho) \in S$.

Hence by Zorn's lemma S has a maximal element, say $M = (K, \tau) \in S$. We now need to show that $K = E$. So suppose $K \neq E$, so K is strictly smaller

than E. Pick an $\alpha \in E \setminus K$. Since E is algebraic over k, it is also algebraic over K, and so α is algebraic over K.

Let $p(x)$ be the minimal polynomial of α over K, say $p(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in K[x]$. This is irreducible and so $p^\tau(x) = x^n\tau(a_{n-1})x^{n-1} + \ldots + \tau(a_0)$ is also irreducible, since $K \cong \tau(K)$. Hence

$$K(\alpha) \cong \frac{K[x]}{\langle p(x)\rangle} \cong \frac{\tau(K)[x]}{\langle p^\tau(x)\rangle} \cong \tau(K)[\beta],$$

where β is any root of $p^\tau(x)$. Thus there exists some $\tau_\alpha \colon K(\alpha) \to \tau(K)(\beta) \subset L$ with $\tau_\alpha|_k = \tau$, meaning that $(K(\alpha), \tau_\alpha) \in S$, but then $(K(\alpha), \tau_\alpha) > (K, \tau)$ strictly in our order, which contradicts the maximality of (K, τ). Hence $K = E$, and we are done. □

Now assume E/k is algebraic and E is algebraically closed. Suppose L/k' is also algebraic, and L is algebraically closed, and as before $k \cong k'$ by σ. Then by the proposition, there exists an embedding τ of E into L such that $\tau(E) = E' \subset L$. Since L/k' is algebraic, L/E' is algebraic. Moreover E is algebraically closed, and $E \cong E'$, so E' must also be algebraically closed, but that must mean $L = E'$, thus $E \cong L$.

Taking $k = k'$, $\sigma = Id$, this discussion proves

Theorem 7.1.8 (Uniquness of algebraic closure)**.** *Suppose K and E are both algebraic closures of k. Then there exists an isomorphism $\tau \colon K \to E$ such that $\tau|_k = \mathrm{Id}$.*

In other words, the algebraic closure of a field is unique up to isomorphism.

For this reason we will routinely denote *the* algebraic closure (up to isomoprhism) of a field k by $\overline{k}$.

Example 7.1.9. For instance, $\overline{Q}$, the set of all elements $\alpha \in \mathbb{C}$ algebraic over $\mathbb{Q}$ is the algebraic closure of $\mathbb{Q}$. Note that $\overline{Q} \neq \mathbb{C}$, since for example π is not algebraic over $\mathbb{Q}$. ▲

Definition 7.1.10. Let k be a field. Let $\mathrm{Aut}(k)$ denote the group of all automorphisms of k, meaning isomorphisms from k to itself, called the ***automorphism group*** of k.

Similarly, for a field extension E/k, $\mathrm{Aut}_k(E)$ is the subgroup of $\mathrm{Aut}(E)$ containing all elements which restricts to the identity map on k.

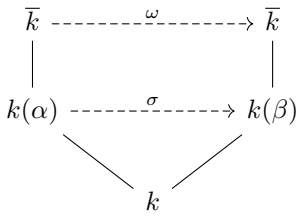
Theorem 7.1.11. *Let $\overline{k} \supset E \supset k$. Suppose $\sigma \colon E \to \overline{k}$ is a k-embedding into $\overline{k}$. Then there exists $\tau \in \mathrm{Aut}_k(\overline{k})$ such that $\tau|_E = \sigma$. So all embeddings of an algebraic extension can be lifted to the algebraic closure.*

Theorem 7.1.12. *Let $\overline{k}$ be an algebraic closure of k. Let $\alpha, \beta \in \overline{k}$. Then the following two are equivalent:*

(*i*) *α and β are roots of the same irreducible polynomials in $k[x]$,*

(*ii*) *there exists some $\omega \in \mathrm{Aut}_k(\overline{k})$ such that $\omega(\alpha) = \beta$.*

Proof. For (i) implying (ii), we have the diagram



where σ is the embedding sending α to β, since they are roots of the same irreducible polynomial. Then the lift ω exists by the previous results.

For (ii) implying (i), note that if α is a root of $p(x) \in k[x]$, then $p^\omega(x) = p(x)$ since ω fixes k, and β is a root of $p^\omega(x)$, since $\omega(p(\alpha)) = p^\omega(\omega(\alpha)) = p^\omega(\beta)$. □

Lecture 8 Splitting Fields

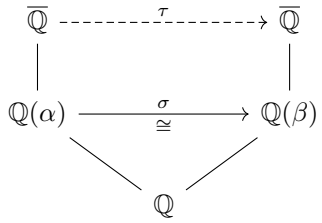
8.1 Lifts are not unique

We discussed previously how an embedding can always be lifted to the algebraic closure. However, such a lift is not unique:

Example 8.1.1. Let $k = \mathbb{Q}$, $\alpha = \sqrt[3]{2}$, and $\beta = \sqrt[3]{2}\omega$, with $\omega = \frac{-1+\sqrt{-3}}{2}$, as before. Then both α and β are roots of $x^3 - 2$, and so

$$\mathbb{Q}(\alpha) \cong \frac{k[x]}{\langle x^3 - 2\rangle} \cong \mathbb{Q}(\beta).$$

Let $\sigma\colon \mathbb{Q}(\alpha) \to \mathbb{Q}(\beta)$ be the $\mathbb{Q}$-embedding sending α to β. We know that this can be lifted to $\tau\colon \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}$, woth $\tau|_{\mathbb{Q}(\alpha)} = \sigma$. Diagramatically,



This lift τ is not unique. For instance, it must send $\sqrt[3]{2}\omega$ to another root of $x^3 - 2$, i.e., $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, or $\sqrt[3]{2}\omega^2$. It is, however, a lift of σ, and σ sends $\sqrt[3]{2}$ to $\sqrt[3]{2}\omega$, and being one-to-one and onto, only $\sqrt[3]{2}$ can be sent there. This leaves two options for $\tau(\sqrt[3]{2}\omega)$, but two is enough to make it not unique.

That is not all, however: there are many other elements in $\overline{\mathbb{Q}}$ that τ has to same somewhere, elements that are not in $\mathbb{Q}(\alpha)$ ans so are not already fixed. For instance, $\tau\sqrt{2}$ can be either $\sqrt{2}$ or $-\sqrt{2}$. ▲

Definition 8.1.2. Let $\overline{k} \supset k$ and let $f(x) \in k[x]$. Then

$$f(x) = c(x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n)$$

Date: September 12th, 2019.

for $\alpha_i \in \overline{k}$, with α_i not necessarily distinct.

Let $E = k(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Then E is called the ***splitting field*** of $f(x)$.

Remark 8.1.3. The splitting field E of $f(x)$ does not depend on the choice of algebraic closure $\overline{k}$.

Lecture 9 Normal Extensions

9.1 Splitting fields and normal extensions

First, note that by the previous discussion, if E is the splitting field of some polynomial $f(x) \in k[x]$, then a k-embedding σ must have the property that for any root α_i of $f(x)$, $\sigma(\alpha_i)$ is also a root of $f(x)$. Hence $\sigma(E) \subset E$.

Example 9.1.1. Let $k = \mathbb{Q}$ and $\overline{k} = \overline{Q} \subset \mathbb{C}$. Consider the polynomial $f(x) = x^3 - 2 \in \mathbb{Q}[x]$. The roots of $f(x)$ are $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, and $\sqrt[3]{2}\omega^2$, where $\omega = \frac{-1}{+}\sqrt{-3}2$. Hence the splitting field of $f(x)$ is $E = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2) = \mathbb{Q}(\sqrt[3]{2}, \omega)$. (That these extensions are equal is fairly easy to see: definitely the former is contained in the latter, and since $\sqrt[3]{2}\omega^2/(\sqrt[3]{2}\omega) = \omega$, the latter is contained in the former.)

In similar fashion, the splitting field of the polynomial $g(x) = (x^3 - 2)(x^2 + 1) \in \mathbb{Q}[x]$ is $E = \mathbb{Q}(\sqrt[3]{2}, \omega, \sqrt{-1})$. ▲

Definition 9.1.2 (Normal extension)**.** An algebraic extension E/k is ***normal*** if for all $\sigma\colon E \to \overline{k}$, k-embeddings, we have $\sigma(E) = E$.

Example 9.1.3. The extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not normal, since $\sigma(\sqrt[3]{2})$ can be $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, or $\sqrt[3]{2}\omega^2$, only one of which satisfies the above condition. ▲

Example 9.1.4. The extension $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$ is normal. This is quite clear: the image of $\sigma(\sqrt[3]{2})$, as per above, is either $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, or $\sqrt[3]{2}\omega^2$, all of which are in $\mathbb{Q}(\sqrt[3]{2}, \omega)$, and similarly the $\sigma(\omega)$ must be ω or ω^2, both of which again are in $\mathbb{Q}(\sqrt[3]{2}, \omega)$. ▲

Remark 9.1.5. The original definition of a normal extension is this: E/k is ***normal*** if for any $L \supset E \supset k$ and any embedding $\sigma\colon E \hookrightarrow L$, we have $\sigma(E) = E$.

It is possible to prove that any transcendental extension is not normal by this definition, hence the requirement of E/k being algebraic in the definition we chose. The proof, however, is not easy.

We will make frequent use of the following lemma:

Lemma 9.1.6. *Let E/k be an algebraic extension and suppose $\sigma\colon E \to E$ is a k-embedding. Then $\sigma(E) = E$.*

In other words, the embedding being one-to-one must automatically be onto if E/k is algebraic. This is not true if the extension is not algebraic:

Counterexample 9.1.7. Consider the fields $\mathbb{C}(x) \supset \mathbb{C}(x^2)$ and the map $\sigma\colon \mathbb{C}(x) \to \mathbb{C}(x^2)$ defined by $\sigma(x) = x^2$. This is a $\mathbb{C}$-embedding (it fixes $\mathbb{C}$), and so one-to-one. However $\mathbb{C}(x) \cong \mathbb{C}(x^2)$, and the image of σ misses all terms with just x, so it is not onto. ▲

Date: September 17th, 2019.

Proof of lemma. Let $\alpha \in E$. We need to show that $\alpha \in \sigma(E)$. Let $p(x) = \mathrm{Irr}(\alpha; k, x)$. Then

$$p(x) = (x-\alpha_1)^{e_1}(x-\alpha_2)^{e_2}\cdots(x-\alpha_r)^{e_r}g(x) \in E[x],$$

where $g(x)$ has no roots in E, and $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_r$ are distinct roots of $p(x)$ in E.

Letting, for any $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \in E[x]$,

$$f^\sigma(x) = \sigma(a_0)x^n + \sigma(a_1)x^{n-1} + \ldots + \sigma(a_{n-1})x + \sigma(a_n) \in E[x],$$

we get $p^\sigma(x) = p(x)$ since σ is a k-embedding, meaning it fixes k, an p has coefficients in k. Hence

$$p(x) = (x-\sigma(\alpha_1))^{e_1}(x-\sigma(\alpha_2))^{e_2}\cdots(x-\sigma(\alpha_r))^{e_r}g^\sigma(x).$$

Now $\{\alpha_1, \alpha_2, \ldots, \alpha_r\}$ are distinct roots of $p(x)$ in E with total multiplicity $e_1+e_2+\ldots+e_r$, and so is $\{\sigma(\alpha_1), \sigma(\alpha_2), \ldots, \sigma(\alpha_r)\}$. Hence the sets are equal, meaning $\alpha = \alpha_1 = \sigma(\alpha_i)$ for some i, and therefore σ is surjective. □

Theorem 9.1.8. *Let $\overline{k} \supset K \supset k$. The following conditions are equivalent:*

(*i*) *For all $\sigma \in \mathrm{Aut}_k(\overline{k})$, $\sigma(K) = K$, i.e., K/k is normal.*

(*ii*) *K is a splitting field of a family of polynomials of $k[x]$.*

(*iii*) *If $\alpha \in K$ and $p(x) = \mathrm{Irr}(\alpha; k, x)$, then all roots of $p(x)$ are in K.*

Proof. First let us show that (*i*) implies (*ii*) and (*i*) implies (*iii*). For any $\alpha \in K$, let $p_\alpha(x) = \mathrm{Irr}(\alpha; k, x)$. Then, say $\alpha = \alpha_1$,

$$p_\alpha(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n) \in \overline{k}[x].$$

For any α_i, there exists some $\sigma \in \mathrm{Aut}_k(\overline{k})$ such that $\sigma(\alpha) = \alpha_i$. But (*i*) implies $\alpha_i \in K$ (which implies (*iii*)), and so K contains $k(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Hence K is the splitting field of $p_\alpha(x)$ for $\alpha \in K$, so this implies (*ii*).

Next, let us show that (*ii*) implies (*i*). Assume $K = k(\alpha_{i,\lambda} | i = 1, 2, \ldots, j_\lambda, \lambda \in \Lambda)$, where $\{\alpha_{1,\lambda}, \alpha_{2,\lambda}, \ldots, \alpha_{j_\lambda,\lambda}\}$ are the roots of $f_\lambda(x) \in k[x]$ in $\overline{k}$. Assume $f_\lambda(x)$ are all irreducible.

Then for any $\sigma \in \mathrm{Aut}_k(\overline{k})$, $\sigma(\alpha_{i,\lambda}) = \alpha_{\ell,\lambda} \in K$ for some ℓ, so $\sigma(K) \subset K$, and hence by the lemma $\sigma(K) = K$. Hence K/k is normal.

Finally let us tackle (*iii*) implying (*i*). Let $\alpha \in K$ and take $p(x) = \mathrm{Irr}(\alpha; k, x)$. Then for any $\sigma \in \mathrm{Aut}_k(\overline{k})$, $p^\sigma(x) = p(x)$, so $\sigma(\alpha)$ is also a root of $p(x)$. By (*iii*) this means $\sigma(\alpha) \in K$, so $\sigma(K) \subset K$, and hence $\sigma(K) = k$ by the lemma, and finally then K/k is normal. □

Example 9.1.9. Consider the chain $\overline{Q} \supset \mathbb{Q}(\sqrt[4]{2}) \supset \mathbb{Q}(\sqrt{2}) \supset \mathbb{Q}$. Let us study this one step at a time.

First, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is normal, because $\mathrm{Irr}(\sqrt{2}; \mathbb{Q}, x) = x^2 - 2$, and both its roots $\sqrt{2}$ and $-\sqrt{2}$ are in $\mathbb{Q}(\sqrt{2})$.

Second, $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ is also normal: $\mathrm{Irr}(\sqrt[4]{2}; \mathbb{Q}(\sqrt{2}), x) = x^2 - \sqrt{2}$, the roots of which are $\pm\sqrt[4]{2} \in \mathbb{Q}(\sqrt[4]{2})$.

What about $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$? We have $\mathrm{Irr}(\sqrt[4]{2}; \mathbb{Q}, x) = x^4 - 2$, the roots of which is $\pm\sqrt[4]{2}$ and $\pm\sqrt[4]{2}i$, but the latter two are not in $\mathbb{Q}(\sqrt[4]{2})$, so this extension is not normal. ▲

Note that this tells us that extensions being normal is not a transitive relation.

Definition 9.1.10. Let K/k be any transcendental extension. A subset $\{ x_\lambda | \lambda \in \Lambda \} \subset K$ is called a ***transcendental basis*** of K/k if

(*i*) $\{ x_\lambda \mid \lambda \in \Lambda \}$ is an algebraically independent set (meaning they are not roots of any nontrivial polynomial equations, cf. linearly independent meaning not roots of nontrivial linear equations). Another way of saying this, $\varphi\colon k[y_\lambda \,|\, \lambda \in \Lambda] \to k[x_\lambda \,|\, \lambda \in \Lambda]$ defined by $y_\lambda \mapsto x_\lambda$ is an isomorphism (i.e., each x_λ behaves as though it were a variable).

(*ii*) $K/k(x_\lambda \mid \lambda \in \Lambda)$ is an algebraic extension.

Example 9.1.11. Consider the field $K = \mathbb{Q}(\sqrt{2}, e)$. Then $\{ e \}$ is a transcendental basis of $K/\mathbb{Q}$; $\mathbb{Q}(e)/\mathbb{Q}$ is a transcendental extension, and $K/\mathbb{Q}(e)$ is algebraic. ▲

Definition 9.1.12. If $k(x_\lambda \mid \lambda \in \Lambda) = K$, then K is called a ***purely transcendental extension***.

Remark 9.1.13. A purely transcendental extension K/k has no algebraic elements over k not in k.

Remark 9.1.14. A transcendental basis always exists (this, like the existence of bases in general, is proved by the standard Zorn's lemma technique), and moreover all such bases have the same cardinality.

This means that an transcendental extension can always be split into a purely transcendental part and an algebraic part, where the algebraic part can be trivial if the original extension was purely transcendental.

Example 9.1.15. The extension $\mathbb{R}/\mathbb{Q}$ is transcendental because, for example, π and e are transcendental over $\mathbb{Q}$. However it is not purely transcendental since e.g.,$\sqrt{2}$ is in $\mathbb{R}$, which is algebraic over $\mathbb{Q}$.

Note finally that a transcendental basis for this extension has infinite cardinality. ▲

Definition 9.1.16. A class $\mathcal{C}$ of field extensions is called ***distinguished*** if

(*i*) it is transitive, i.e.,$E/k \in \mathcal{C}$ if and only if $E/F \in \mathcal{C}$ and $F/k \in \mathcal{C}$ for every $E \supset F \supset k$.

(*ii*) it has a lifting property, meaning if $E/k \in \mathcal{C}$, and F/k is any extension such that $E, F \subset L$ for some L, then $EF/F \in \mathcal{C}$.

(*iii*) it has a composite property, if $E/k \in \mathcal{C}$ and $F/k \in \mathcal{C}$ and $E, F \subset L$ for some L, then $EF/k \in \mathcal{C}$.

Example 9.1.17. Let $\mathcal{C}$ be the class of all finite extensions. This is distinguished. ▲

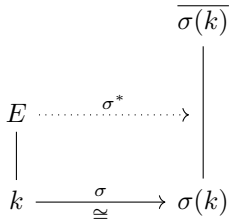
Example 9.1.18. The class $\mathcal{C}$ of all algebraic extensions is also distinguished. ▲

Example 9.1.19. The class $\mathcal{C}$ of all normal extensions is not distinguished—we have already discussed how it is not transitive. However it does have both the lifting and composite properties. ▲

Lecture 10 Separable Extension

10.1 Separable degree

Let E/k be an algebraic extension, and let $\sigma\colon k \hookrightarrow \sigma(k) \subset \overline{\sigma(k)}$ be an embedding of k. We know from earlier that σ can be lifted to $\sigma^*\colon E \to \overline{\sigma(k)}$,



We have also learned, however, that this lift is not unique. For this reason, consider

$$S_\sigma = \left\{ \sigma^*\colon E \hookrightarrow \overline{\sigma(k)} \text{ an embedding such that } \sigma^*|_k = \sigma \right\}.$$

Now define $[E : k]_s = |S_\sigma|$, called the ***separable degree*** of E/k.

Note how $|S_\sigma|$ depends on σ and the choice of closure $\overline{\sigma(k)}$. We want to show that $[E : k]_s$ is independent of both of these.

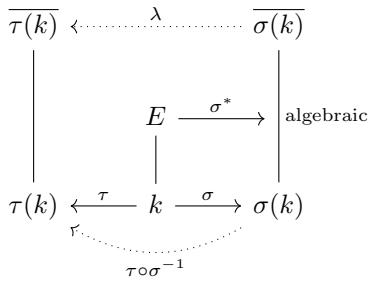
Lecture 11 Simple Extensions

11.1 Separable extensions

To see that $[E : k]_s$ is independent of both σ and the algebraic closure $\overline{\sigma(k)}$, suppose we have another embedding $\tau\colon k \hookrightarrow \tau(k)$, with its own algebraic closure $\overline{\tau(k)}$.

Then because there exists some $\lambda\colon \overline{\sigma(k)} \to \overline{\tau(k)}$ such that $\lambda|_{\sigma(k)} = \tau \circ \sigma^{-1}$.

In a picture,



This by way of saying that we want to find a lift of τ, say τ^*, corresponding to σ^*. This is a matter of following the diagram around: define $\tau^* = \lambda \circ \sigma^*$; then $\tau^*|_k = \tau$, since

$$\tau^*\Big|_k = \lambda \circ \sigma^*\Big|_k = \lambda \circ \sigma\Big|_k = \tau \circ \sigma^{-1} \circ \sigma = \tau.$$

Date: September 19th, 2019.
Date: September 24th, 2019.

Hence given a lift σ^* of σ we have a τ^*, and vice versa, so there is a one-to-one correspondence from S_σ to $\S_\tau$ defined by $\sigma^* \mapsto \tau^* = \lambda \circ \sigma$ (and inverse $\tau^* \mapsto \sigma^* = \lambda^{-1} \circ \tau^*$). Therefore $|S_\sigma| = |S_\tau|$, and S_σ does not depend on the choice of σ or closure $\overline{\sigma(k)}$.

In other words we can fix an algebraic closure $\overline{k}$ and take $\sigma = \mathrm{Id}$, and $|S_\sigma| = |S_{\mathrm{Id}}|$, and then $[E : k]_s$ is precisely the number of k-embeddings of E.

We can characterise the separable degree in other ways too. For instance, consider fields $\overline{k} \supset E \supset k$, and suppose $E = k(\alpha)$ for some $\alpha \in E$, and let $p(x)$ be the minimal polynomial of α over k. Then σ is completely determined by its image of α, so $\sigma(E) = k(\beta)$ for some root β of $p(x)$.

Hence $[E : k]_s$ is the number of distinct roots of $p(x)$ in $\overline{k}$.

Example 11.1.1. Consider $p(x) = x^3 + x + 1 \in \mathbb{Q}[x]$, which is irreducible (it has no rational roots, and is of degree less than or equal to three). Let $\alpha \in \overline{\mathbb{Q}}$ with $p(\alpha) = 0$. Then $[Q(\alpha) : Q]_s = 3$ since $p(x)$ has three distinct roots.

Note, maybe out of curiosity, how this is also the degree of $p(x)$, and hence $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. ▲

This last remark need not always be the case:

Example 11.1.2. Let $\mathbb{F}_q$ denote the finite field of $q = p^n$ elements, p a prime, and let $k = \mathbb{F}_q(x)$, x a variable, be the function field over it. Now consider $p(t) = t^p - x \in k[t]$. In $\overline{k}$, which must exist, take some $\alpha \in \overline{k}$ such that $p(\alpha) = 0$. Then $p(\alpha) = \alpha^p - x = 0$, so $x = \alpha^p$, and hence

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

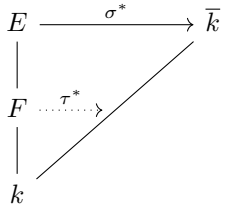
in $\overline{k}[t]$, since k has characteristic p. This means $p(t)$ has only one distinct root in $\overline{k}$, so $[k(\alpha) : k]_s = 1$, but because $p(t) = t^p - x$ is irreducible over k, $[k(\alpha) : k] = p$. ▲

In other words, the degree of an extension is not necessarily equal to the degree of the extension. That said, they do behave similarly in many ways.

Theorem 11.1.3. *Let $E \supset F \supset k$ be a chain of algebraic extensions. Then*

$$[E : k]_s = [E : F]_s [F : k]_s.$$

Proof. Consider the diagram



where σ^* a k-embedding of E, i.e., $\sigma^*|_k = \mathrm{Id}_k$, and $\sigma^*|_F = \tau^*$, with $\tau^*|_k = \sigma^*|_k = \mathrm{Id}_k$.

Then for each τ^* there are by definition $[E : F]_s$ lifts σ^*, and there are $[F : k]_s$ different τ^* to start with, giving us the right-hand side. On the other hand, there are $[E : k]_s$ ways to do this all together. □

Corollary 11.1.4. *If $[E : k] < \infty$, then $[E : k]_s \leq [E : k]$.*

Proof. Since E is a finite extension of k we can write $E = k(\alpha_1, \alpha_2, \ldots, \alpha_n)$ for some $\alpha_i \in E$. Then

$$k \supset k(\alpha_1) \supset k(\alpha_1, \alpha_2) \subset \ldots \subset k(\alpha_1, \alpha_2, \ldots, \alpha_n) = E.$$

Note how, at any individual step, $[k(\alpha) : k]_s \leq [k(\alpha) : k]$ since the left-hand side is the number of distinct roots of $\mathrm{Irr}(\alpha; k, x)$, whereas the right-hand side is the degree, and hence total number of roots, with multiplicity, of same.

By the previous theorem,

$$[k(\alpha_1, \alpha_2, \ldots, \alpha_n) : k]_s = [k(\alpha_1, \alpha_2, \ldots, \alpha_n) : k(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})]_s \cdots [k(\alpha_1) : k]_s,$$

and each factor is bounded their respective degrees, so the product is bounded by $[k(\alpha_1, \alpha_2, \ldots, \alpha_n) : k]$. □

Corollary 11.1.5. *Let $E \supset F \supset k$ be a chain of finite extensions. Then $[E : k]_s = [E : k]$ if and only if $[E : F]_s = [E : F]$ and $[F : k]_s = [F : k]$.*

Proof. In the proof of the previous corollary, for there to be equality each of the individual steps in the end have to be equalities. □

Definition 11.1.6. A finite extension E/k is ***separable*** if $[E : k]_s = [E : k]$.

Definition 11.1.7. Let k be a field and $\overline{k}$ an algebraic closure, and take $\alpha \in \overline{k}$. We say that α is ***separable*** over k if $[k(\alpha) : k]_s = [k(\alpha) : k]$.

In other words, α is separable over k if and only if $\mathrm{Irr}(\alpha; k, x)$ has no repeated roots in $\overline{k}$.

Definition 11.1.8. A polynomial $f(x) \in k[x]$ is ***separable*** if $f(x)$ has no repeated roots in $\overline{k}$.

Example 11.1.9. In our previous example, $f(t) = t^p - x \in \mathbb{F}_q(x)[t]$ is irreducible over $\mathbb{F}_q(x)$ but not separable. ▲

These definitions are compatible:

Theorem 11.1.10. *Let E/k be a finite extension. Then E/k is separable if and only if all elements $\alpha \in E$ are separable over k.*

Proof. For any $\alpha \in E$,

$$[E : k] = [E : k(\alpha)][k(\alpha) : k]$$

and

$$[E : k]_s = [E : k(\alpha)]_s [k(\alpha) : k]_s.$$

For the forward direction, assume E/k is separable, so $[E : k]_s = [E : k]$. Hence for all $\alpha \in E$, $[k(\alpha) : k]_s = [k(\alpha) : k]$ by the corollary above, so α is separable over k.

For the converse direction, E/k is a finite extension so $E = k(\alpha_1, \alpha_2, \ldots, \alpha_n)$ for some $\alpha_1, \alpha_2, \ldots, \alpha_n \in E$.

In general, for $E \supset F \supset k$, E/k being separable implies E/F is separable, so since

$$\begin{aligned}[E : k]_s &= [E : k(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})]_s \cdots [k(\alpha_1) : k]_s \\ &= [E : k(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})] \cdots [k(\alpha_1) : k] = [E : k]\end{aligned}$$

since each extension along the way is adjoining just a single element. □

From this proof we see in particular that

Corollary 11.1.11. *Let $E = k(\alpha_1, \alpha_2, \ldots, \alpha_n)$ with α_i algebraic over k. Then E/k is separable if and only if $\alpha_1, \alpha_2, \ldots, \alpha_n$ are separable over k.*

In other words, it is enough to study a set of generators.

All of the previous discussion have required extensions be finite, since we are comparing degrees.

Definition 11.1.12. Let E/k be an algebraic extension, possibly infinite. We say that E/k is ***separable*** if every finite extension of k in E is separable.

I.e., for any F such that $E \supset F \supset k$ with $[F : k] < \infty$, F is separable over k. Or, another way of saying the same thing: for any $\alpha \in E$, α is separable over k.

Theorem 11.1.13. *Let $E \supset F \supset k$ be a chain of algebraic extensions. Then E/k is separable if and only if E/F and F/k are separable.*

Proof. Using the last statement in the definition above, consider for the forward direction any element $\alpha \in E$. This is separable over k, so $\mathrm{Irr}(\alpha; k, x)$ has no repeated roots in E. But then it also can't have repeated roots in F, nor can the minimal polynomial of α over F have repeated roots in E.

Similarly for the converse. □

11.2 Simple extensions

Definition 11.2.1. An algebraic extension E/k is called ***simple*** if there exists some $\alpha \in E$ such that $E = k(\alpha)$.

In particular, $[E : k] < \infty$, so a simple extension is always finite.

Definition 11.2.2. Let E/k be an algebraic extension. Suppose $E = k(\alpha)$. Then α is called a ***primitive element***.

This makes us wonder when, in general, a finite extension is simple.

Theorem 11.2.3 (Primitive element theorem)**.** *Let E/k be a finite extension.*

(*i*) *Suppose E/k possesses only finitely many intermediate subfields. Then E/k is simple. The converse also holds.*

(*ii*) *If E/k is separable, then E/k is simple.*

Proof. For the forward direction of (i), suppose there are only finitely many intermediate fields F, $k \subset F \subset E$. Pick up any $\alpha, \beta \in E$. We claim that $k(\alpha, \beta) = k(\gamma)$ for some $\gamma \in E$.

If true, this claim solves our problem: since E/k is finite, $E = k(\alpha_1, \alpha_2, \ldots, \alpha_n)$ for some α_i, and we can reduce this one at a time until it is a simple extension, using the claim.

Consider $k(\alpha + c\beta)$ for $c \in k$. Clearly $k \subset k(\alpha + c\beta) \subset k(\alpha, \beta)$. By assumption, i.e., there being only finitely many intermediate fields, there can only be finitely many $k(\alpha + c\beta)$, so there must exist some distinct $c_1, c_2 \in k$ such that $k(\alpha + c_1\beta) = k(\alpha + c_2\beta) = K \subset k(\alpha, \beta)$.

Hence $(c_1 - c_2)\beta \in K$, and $c_1 - c_2 \neq 0$, so $\beta \in K$, and then also $\alpha \in K$, so $k(\alpha, \beta) \subset K \subset k(\alpha, \beta)$, meaning that $K = k(\alpha, \beta)$.

Lecture 12 Simple Extensions, continued

12.1 Primitive element theorem, continued

Proof continued. For the converse direction of (i), assume $E = k(\alpha)$ is simple, and let $p(x) = \mathrm{Irr}(\alpha; k, x)$. For any field F with $E \supset F \supset k$, let $g_F(x) = \mathrm{Irr}(\alpha; F, x)$. Then $g_F(x) \mid p(x)$, and there are only finitely many such choices of divisors, since $p(x)$ has only finitely many factors in $\overline{k}[x]$. Define $\varphi\colon F \mapsto g_F(x)$ with

$$g_F(x) \in \left\{ g(x) \;\middle|\; g(x) \mid p(x) \text{ in } \overline{k}[x] \right\}.$$

We claim that this is one-to-one. To see this, write $g_F(x) = x^m + \beta_1 x^{m-1} + \ldots + \beta_m$ with $\beta_i \in F$, and let $F_0 = k(\beta_1, \beta_2, \ldots, \beta_m) \subset F$. Now by construction $g_F(x) = \mathrm{Irr}(\alpha; F, x) = \mathrm{Irr}(\alpha; F_0, x)$, so the degrees $[F(\alpha)\colon F] = [F(\alpha) : F_0]$, meaning $F = F_0$. Now F_0 is completely determined by $G_F(x)$, so φ is one-to-one.

Lecture 13 Normal and Separable Closures

First let us finish up the overdue proof.

Proof continued. It remains to show (ii), i.e., if E/k is separable, then E is a simple extension of k.

There is a trivially easy case: if $|k| < \infty$, then $|E| < \infty$ too since E/k is a finite extension, and hence E/k has only finitely many intermediate fields, so by (i), E/k is simple.

So let us assume $|k| = \infty$. Then E/k is still a finite extension, being separable, so $E = k(\alpha_1, \alpha_2, \ldots, \alpha_n)$ for some $\alpha_i \in E$. By the same argument as in (i), it suffices to consider $E = k(\alpha, \beta)$, and showing that this is simple.

Let $[E : k] = n = [E : k]_s$, since E/k is separable by assumption. Then there exists n distinct k-embeddings of E into $\overline{k}$, say $\left\{ \sigma_1, \sigma_2, \ldots, \sigma_n \right\}$. There are determined by their values on α and β.

Define

$$p(x) = \prod_{1 \le i \ne j \le n} (\sigma_i(\alpha) - \sigma_j(\alpha) + (\sigma_i(\beta) - \sigma_j(\beta))x).$$

We claim that $p \ne 0$. Suppose not, i.e., suppose $p(x) = 0$ for all $x \in k$. Then there exists $i \ne j$ such that

$$\sigma(\alpha) - \sigma_j(\alpha) + (\sigma_i(\beta) - \sigma_j(\beta))x = 0$$

for infinitely many $x \in k$. This implies $\sigma_i(\alpha) - \sigma_j(\alpha) = 0$ and $\sigma_i(\beta) - \sigma_j(\beta) = 0$, which means $\sigma_i = \sigma_j$, contradicting all the σ_i being distinct.

By this claim there must then exist some $c \in k$ such that $p(c) \ne 0$, so that

$$\sigma_i(\alpha) - \sigma_j(\alpha) + (\sigma_i(\beta) - \sigma_j(\beta))c \ne 0$$

for all $i \ne j$. Since $c \in k$ and all our σ_i are k embeddings, we can bring c inside getting $\sigma_i(\alpha + c\beta) \ne \sigma_j(\alpha + c\beta)$ for all $i \ne j$.

Date: September 26th, 2019.
Date: October 1st, 2019.

Now consider the fields $E = k(\alpha, \beta) \supset k(\alpha + c\beta) \supset k$. Then we have

$$[k(\alpha + c\beta) : k] \leq [k(\alpha, \beta) : k] = n,$$

and by our calculation above there exist at least n distinct k-embeddings of $k(\alpha + c\beta)$, so

$$n \leq [k(\alpha + c\beta) : k]_s \leq [k(\alpha + c\beta) : k],$$

together giving us

$$n = [k(\alpha + c\beta) : k] = [k(\alpha, \beta) : k].$$

Hence $k(\alpha + c\beta) = k(\alpha, \beta) = E$, so E is simple. □

13.1 Normal closure

Definition 13.1.1. Let E/k be an algebraic extension (possibly infinite), and take $\overline{k} \supset E \supset k$. The ***normal closure*** of E/k in $\overline{k}$ is the intersection of all fields F such that $\overline{k} \supset F \supset k$ and F/k is normal.

In other words, the normal closure of E/k in $\overline{k}$ is the smallest normal extension of k containing E.

Note that $\overline{k}/k$ is normal, so F exists.

Example 13.1.2. Consider $\overline{\mathbb{Q}} \supset E = \mathbb{Q}(\sqrt[3]{2}) \supset \mathbb{Q}$. The normal closure of E in $\overline{\mathbb{Q}}$ is $F = \mathbb{Q}(\sqrt[3]{2}, \omega)$. ▲

Example 13.1.3. Suppose $\overline{k} \supset E \supset k$ and let $\left\{ \sigma_i \;\middle|\; i \in I \right\}$ be the set of all distinct k-embeddings of E into $\overline{k}$.

If $I = \left\{ 1, 2, \ldots, n \right\}$, i.e., $[E : k]_s = n < \infty$, then $\sigma_i(E) \subset \overline{k}$ for each i. Then the normal closure of E/k is

$$F = \sigma_1(E)\sigma_2(E) \cdots \sigma_n(E).$$

Notice how if $\tau \colon F \hookrightarrow \overline{k}$ is a k-embeddings, then $\tau(F) \subset F$, so $\tau(F) = F$, being algebraic, whence F/k is normal, and it contains at least the things we need, and no more. ▲

Example 13.1.4. Playing the same game, if $|I| = [E : k]_s = \infty$, then the normal closure of E/k is, again, the smallest field that contains all $\sigma_i(E)$ for all $i \in I$, but unlike the finite case this might not be the composition. ▲

13.2 Separable closure

Let E/k be an algebraic extension, possibly infinite. Then, as we have preciously discussed, E/k is separable if and only if every finite subextension is separable, if and only if every element of E is separable over k. Hence:

Definition 13.2.1. Let $\overline{k} \supset E \supset k$. The ***separable closure*** F of k in E is the set of all separable elements of E over k.

Note that this is a field. The easy way to see this is to note that consider see that $k(\alpha, \beta)$ is a separable extension of k, and so all the products, sums, differences, and quotients are also contained in the separable closure.

13.3 Finite fields

We want to review some basic properties of finite fields. To this end, let F be a finite field.

First, $\mathrm{char}(F) = p$, a prime, and $|F| = p^n$ for some n, and we view F as an extension of degree n of $\mathbb{F}_p$, the finite field of p elements. . Customarily we let $q = p^n$ and call $F = \mathbb{F}_q$.

The group of units of F, i.e., $(F^\times, \cdot)$, is a cyclic group. To see this, note first by the Fundamental theorem of finitely generated abelian groups,

$$F^\times \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \ldots \times \mathbb{Z}_{m_k}$$

Let $d = \mathrm{lcm}(m_1, m_2, \ldots, m_k)$. Then by definition $d \leq m_1 m_2 \cdots m_k = q - 1 = |F^\times|$. Now note how for $a \in F^\times$, $a^d = 1$, and so a is a root of $x^d - 1$. Now $x^d - 1$ has at most d distinct roots, and every $a \in F^\times$ is a root of it, so $|F^\times| \leq d \leq |F^\times|$. Hence $d = m_1 m_2 \cdots m_k$, implying that $(m_i, m_j) = 1$ for all $i \neq j$, and so finally

$$F^\times \cong \mathbb{Z}_{m_1 m_2 \cdots m_k}$$

is cyclic.

In other words, $F^\times \cong \mathbb{Z}_{q-1}$. Moreover all elements in $F^\times$ are roots of $x^{q-1} - 1$, so all elements in F (including 0) are roots of $x^q - x$. Hence F is the splitting field of $x^q - x$ over $\mathbb{F}_p$.

Theorem 13.3.1 (Existence)**.** *For every prime p and every $n \in \mathbb{N}$, there exists a field F such that $|F| = p^n$.*

Proof. Let $q = p^n$ and let $f(x) = x^q - x \in \mathbb{F}_p[x]$. Notice how $f'(x) = qx^{q-1} - 1 = -1 \neq 0$ since $\mathrm{char}\, \mathbb{F}_p = p$. Hence f has no repeated roots. Let F be the splitting field of $f(x)$ in $\overline{\mathbb{F}_p}$, and let F_1 be the set of all roots of $f(x)$ in $\overline{\mathbb{F}_p}$. Then $|F_1| = q$.

We claim that F_1 is a field. This is routine: for $\alpha, \beta \in F_1$, we have $\alpha^q = \alpha$ and $\beta^q = \beta$, and hence also $(\alpha\beta)^1 = \alpha^q \beta^q = \alpha\beta$, for $\beta \neq 0$ we have $\left(\frac{\alpha}{\beta}\right)^q = \frac{\alpha^q}{\beta^q} = \frac{\alpha}{\beta}$, and since we are in characteristic p, $(\alpha \pm \beta)^q = \alpha^q \pm \beta^q = \alpha \pm \beta$. Hence all of these are rots of $f(x)$, so belong to F_1, so F_1 is a field, and indeed $F_1 = F$. □

Theorem 13.3.2 (Uniqueness)**.** *All fields of order p^n are isomorphic. In particular, if $\overline{\mathbb{F}_p} \supset F_1, F_2 \supset \mathbb{F}_p$ and $|F_1| = |F_2|$, then $F_1 = F_2$.*

Proof. This follows directly from things we already know: if $|F_1| = |F_2| = p^n$, both are splitting fields of $x^{p^n} - x$, and splitting fields of the same polynomial are isomorphic. In particular if they are under the same algebraic closure, they are equal. □

We can classify the automorphisms of such fields:

Theorem 13.3.3. *If $|F| = p^n = q$, then $\mathrm{Aut}_{\mathbb{F}_p}(F) \cong \mathbb{Z}_n$ (hence cyclic), and in particular $\mathrm{Aut}_{\mathbb{F}_p}(F) = \langle\varphi\rangle$, where $\varphi \colon F \to F$, $\varphi(x) = x^p$ is the* **Frobenius automorphism**.

Proof. Note first how $\varphi^n(x) = x^{p^n} = x^q = x$, so $\varphi^n = \mathrm{Id}_F$, meaning that the order of φ is at most n.

Next let us show that it is at most n, and hence equal to n. Take $y \in F^\times$ such that $F^\times = \langle y \rangle$ (since we already showed this is cyclic). In other words, the

order of y is $q-1=p^n-1$, so $y^{q-1}=1$, and moreover $y^q=y$. Importantly this is the smallest positive power that works, i.e., $y^k\neq 1$ for any $0<k<q$. So $\varphi^n(y)=y^{p^n}=y$ is the smallest power of φ with this property, so $\varphi^m\neq \mathrm{Id}_F$ for all $0<m<n$, and hence the order of φ is at least m.

Hence $\mathrm{Aut}_{\mathbb{F}_p}(F)\supset\langle\varphi\rangle\cong\mathbb{Z}_n$.

Since $[F:\mathbb{F}_p]=n=[F:\mathbb{F}_p]_s$ (since finite extensions of finite fields are separable), there exists at most n distinct $\mathbb{F}_p$-embeddings of F into $\overline{\mathbb{F}_p}$, so $|\mathrm{Aut}_{\mathbb{F}_p}(F)|\leq n$. Thus $\mathrm{Aut}_{\mathbb{F}_p}(F)=\langle\varphi\rangle\cong\mathbb{Z}_n$, as desired. □

Lecture 14 Inseparable Extensions

14.1 Number of irreducible polynomials over finite fields

Theorem 14.1.1. *Let $k=\mathbb{F}_p$, where p is a prime. Let N_n denote the number of irreducible polynomials in $k[x]$ of degree n. Then*

$$N_n=\frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)p^d,$$

where $\mu\colon\mathbb{N}\to\{1,-1,0\}$ is the Möbius function ($\mu(1)=1$, and $\mu(n)=0$ is n is not square-free, and $(-1)^k$ if $n=p_1p_2\cdots p_k$, where p_i are distinct primes).

Proving is straight-forward if we first have the following lemma:

Lemma 14.1.2. *Let $f(x)\in\mathbb{F}_p[x]$ be an irreducible polynomial of degree d. Then $d\mid n$ if and only if $f(x)\mid x^{p^n}-x$.*

Proof. First, note how for $\ell,m\in\mathbb{N}$, $x^\ell-1\mid x^m-1$ if and only if $\ell\mid m$.

For the forward direction, $x^m-1=(x^\ell)^q-1$ can have a factor of $x^\ell-1$ taken out of it. For the reverse direction, write $m=\ell q+r$, with $0\leq r<\ell$. Then

$$\frac{x^m-1}{x^\ell-1}=\frac{x^{\ell q+r}-1}{x^\ell-1}=\frac{x^r(x^{q\ell}-1)}{x^\ell-1}+\frac{x^r-1}{x^\ell-1},$$

where the left-hand side is a polynomial, and so is the first term in the right-hand side, so $\frac{x^r-1}{x^\ell-1}$ must be a polynomial too. But $r<\ell$, so this cannot be a polynomial unless $r=0$. Hence $\ell\mid m$.

Similarly, let $a,\ell,m\in\mathbb{N}$, $a>1$. Then $a^\ell-\mid a^m-1$ if and only if $\ell\mid m$.

With this we can prove the lemma: For the forward direction, assume $d\mid n$. Then $p^d-1\mid p^n-1$ by the above (with $a=p$), and hence $x^{p^d-1}-1\mid x^{p^n-1}-1$. Multiplying by x, we get $x^{p^d}-x\mid x^{p^n}-x$.

Now $f(x)\in\mathbb{F}_p[x]$ is irreducible of degree d, so let $\alpha\in\overline{\mathbb{F}_p}$ be a root of $f(x)$, whence $[\mathbb{F}_p(\alpha):\mathbb{F}_p]=d$, so $|\mathbb{F}_p(\alpha)|=p^d$. Hence $\mathbb{F}_p(\alpha)$ is the splitting field of $x^{p^d}-x$ over $\mathbb{F}_p$, by the uniqueness of finite fields. Therefore α is a root of $x^{p^d}-x$, implying

$$f(x)\mid x^{p^d}-x\mid x^{p^n}-x.$$

For the converse direction, assume $f(x)\mid x^{p^n}0x$, with $f(x)$ irreducible of degree d. Let $\alpha\in\overline{\mathbb{F}_p}$ be a root of $f(x)$. Hence $f(x)\mid x^{p^n}-x$ implies $\mathbb{F}_p(\alpha)\subset\mathbb{F}_{p^n}$, the splitting field of $x^{p^n}-x$. Therefore

$$n=[\mathbb{F}_{p^n}:\mathbb{F}_p]=[\mathbb{F}_{p^n}:\mathbb{F}_p(\alpha)]\cdot[\mathbb{F}_p(\alpha):\mathbb{F}_p]=[\mathbb{F}_{p^n}:\mathbb{F}_p(\alpha)]\cdot d,$$

Date: October 3rd, 2019.

so $d \mid n$. □

14.2 Inseparable extensions

First we need two basic facts, essentially from calculus. Let k be a field, and let $f(x) \in k[x]$. Take $a \in \overline{k}$. Then a is a multiple root of $f(x)$ if and only if $f(a) = 0$ and $f'(a) = 0$.

To see this, write $f(x) = (x-a)^m g(x)$, and then

$$f'(x) = m(x-a)^{m-1}g(x) + (x-a)^m g'(x),$$

where m is the multiplicity of the root a. Then we can factor out $x - a$ from the derivative, so it is a root of $f'(x)$, if and only if $m > 1$.

Related to this: $f(x)$ has a multiple root in $\overline{k}$ if and only if $\gcd(f(x), f'(x)) \neq 1$ in $k[x]$.

Theorem 14.2.1. *Let $\overline{k} \supset k$ and $\alpha \in \overline{k}$. Let $f(x) = \mathrm{Irr}(\alpha; k, x)$.*

(*i*) *All roots of $f(x)$ in $\overline{k}$ have the same multiplicity.*

(*ii*) *If $\mathrm{char}(k) = 0$, then $f(x) = 0$ is multiplicity free (i.e., $f(x)$ has no repeated roots, so $f(x)$ is separable).*

(*iii*) *If $\mathrm{char}(k) = p > 0$, then the common multiplicity is of the form p^μ for some $\mu \in \mathbb{Z}$, $\mu \geq 0$.*

Moreover, $\beta = \alpha^{p^\mu}$ is separable and

$$[k(\alpha) : k] = p^\mu [k(\alpha) : k]_s = p^\mu [k(\beta) : k]_s = p^\mu [k(\beta) : k].$$

Proof. (*i*) Let $\alpha_1, \alpha_2, \ldots, \alpha_r$ be the set of all distinct roots of $f(x)$ in $\overline{k}$. For each α_i, there exists $\sigma_i \in \mathrm{Aut}_k(\overline{k})$ such that $\sigma_i(\alpha_i) = \alpha_1$. Note that since σ_i fixes k and $f(x) \in k[x]$, $f^{\sigma_i} = f$. Hence, if

$$f(x) = (x-\alpha_1)^{m_1}(x-\alpha_2)^{m_2}\cdots(x-\alpha_r)^{m_r},$$

then

$$f^{\sigma_i}(x) = (x-\sigma_i(\alpha_1))^{m_1}(x-\sigma_i(\alpha_2))^{m_2}\cdots(x-\sigma_i(\alpha_i))^{m_i}\cdots(x-\sigma_i(\alpha_r))^{m_r},$$

and since $\sigma_i(\alpha_i) = \alpha_1$, we see that $m_i = m_1$, for any i.

(*ii*) Let $f(x)$ be irreducible, say $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$, $a_i \in k$ and $a_n \neq 0$. Then

$$f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \ldots + a_1,$$

where $na_n \neq 0$. Hence $\gcd(f(x), f'(x)) = 1$ since $f(x)$ is irreducible and $\deg f' < \deg f$ and $f' \neq 0$. Thus $f(x)$ is separable.

(*iii*) If $\mathrm{char}(k) = p > 0$, let m be the common multiplicity of the roots of $f(x)$. If $m = 1$ then $\mu = 0$ and $f(x)$ is separable, so we are done.

Assume $m > 1$. Then, as above, if $\gcd(f(x), f'(x)) \neq 1$, we must have $f'(x) = 0$ since $\deg f' < \deg f$ and $f(x)$ is irreducible. Hence $f(x)$ must be

a polynomial in p^n, so that when taking the derivative we get multiples of p, which are zero in characteristic p. In other words, there exists some $g \in k[x]$ such that $f(x) = g(x^p)$. Since f is irreducible over k, so if g, and we can repeat this process for $g(x)$ if $g(x) = 0$ is not multiplicity free.

Hence there exists some $\mu \geq 1$ and $F(x) \in k[x]$ such that $F(x)$ is separable and $f(x) = F(x^{p^\mu})$.

Write $F(x) = (x - \beta_1)(x - \beta_2) \cdots (x - \beta_r)$, with $\beta_i \in \overline{k}$ distinct. Then

$$\begin{aligned} f(x) = F(x^{p^\mu}) &= (x^{p^\mu} - \beta_1)(x^{p^\mu} - \beta_2) \cdots (x^{p^\mu} - \beta_r) \\ &= (x - \delta_1)^{p^\mu}(x - \delta_2)^{p^\mu} \cdots (x - \delta_r)^{p^\mu} \end{aligned}$$

since $\mathrm{char}(k) = p$, where $\beta_i = \delta_i^{p^\mu}$. Note how δ_i are distinct since β_i are distinct, and they are all the distinct roots of $f(x)$, with multiplicity p^μ.

So $\alpha = \delta_1$, say, and we take $\beta = \beta_1 = \alpha^{p^\mu}$. Then $\mathrm{Irr}(\beta; k, x) = F(x)$, separable over k, so

$$[k(\alpha) : k] = p^\mu \cdot r,$$

since r is the number of distinct roots of $f(x)$, so

$$[k(\alpha) : k] = p^\mu [k(\alpha) : k]_s.$$

But r is also the degree of F, which is separable, so in turn

$$p^\mu \cdot r = p^\mu [k(\beta) : k] = p^\mu [k(\beta) : k]_s. \qquad \square$$

The situation, in a picture, is this:

$$\begin{array}{c} k(\alpha) \\ {\scriptstyle p^\mu}\,\big|\,{\scriptstyle \text{purely inseparable}} \\ k(\beta) \\ {\scriptstyle r}\,\big|\,{\scriptstyle \text{separable}} \\ k. \end{array}$$

We have $\mathrm{Irr}(\alpha; k(\beta), x) = x^{p^\mu} - \beta$, which in $\overline{k}[x]$ factors as $(x - \alpha)^{p^\mu}$, which is why we call the topmost extension ***purely inseparable***; it has only one root, with as large a multiplicity as possible.

In this setup we also call $[k(\alpha) : k]_i = p^\mu$ the ***inseparable degree*** of $k(\alpha)/k$.

More generally:

Definition 14.2.2. Let k be a field with $\mathrm{char}(k) = p > 0$. Let E/k be a finite algebraic extension. Then we define the ***inseparable degree*** of E/k by

$$[E : k]_i = \frac{[E : k]}{[E : k]_s}.$$

Note that if $p = 0$, then all finite extensions are separable, so the inseparable degree would be uninteresting. Note also how $[E : k]_i$ is always a power of p.

Proposition 14.2.3. *Let $E \supset F \supset k$ be a chain of field extensions, with E/k a finite extension. Then*

$$[E : k]_i = [E : F]_i [F : k]_i.$$

Proof. Both the degree and the separable degree have this multiplicative property, so the inseparable degree must too. □

Remark 14.2.4. Let E/k be an infinite algebraic extension. Then we define $[E:k]$ as the cardinality of the basis of E/k as a vector space, and we defined $[E:k]_s$ as the cardinality of the number of distinct embeddings of E into $\overline{k}$.

We don't define inseparable degrees for infinite extensions, and the reason is that they don't necessarily make a great deal of sense:

Example 14.2.5. Consider $k = \mathbb{Q}$ and $\overline{k} = \overline{\mathbb{Q}}$. Then $[\overline{\mathbb{Q}} : \mathbb{Q}] = |\mathbb{N}|$ is countable. However $[\overline{\mathbb{Q}} : \mathbb{Q}]_s = |\mathbb{R}|$ is uncountable, since, for instance, every $\sqrt{p}$, p prime, can be sent to two different images, so the cardinality is the power set of $\mathbb{N}$. ▲

Lecture 15 Purely Inseparable Extensions

15.1 Inseparable closures and purely inseparable extensions

Definition 15.1.1. Let E/k be a field extension, and let $\mathrm{char}(k) = p > 0$. Let $\alpha \in E$. Then α is called ***purely inseparable*** over k if $\alpha^{p^n} \in k$ for some n.

In this case, $f(x) = x^{p^n} - \alpha^{p^n} \in k[x]$, with $f(\alpha) = 0$. But $f(x) = (x-\alpha)^{p^n}$, meaning that $\mathrm{Irr}(\alpha; k, x) = (x-\alpha)^{p^m}$ for some m, whence $[k(\alpha) : k]_s = 1$.

Definition 15.1.2. Let $\mathrm{char}(k) = p$. An algebraic extension E/k is called ***purely inseparable*** if every element of E if purely inseparable over k.

In other words, $E_o = k$ where E_o is the separable closure of k in E (because $m = 0$, so $\alpha \in k$, in the above setup).

Proposition 15.1.3. *Let E/k be an algebraic extension with* $\mathrm{char}(k) = p$. *Let E_o be the separable closure of k in E. Then E/E_o is a purely inseparable extension.*

Proof. For $\alpha \in E$, there exists some $\mu \geq 0$ such that $\alpha^{p^\mu} = \beta$ is separable over k, so $\beta \in E_o$. Hence α is purely inseparable over E_o. □

Proposition 15.1.4. *Let K/k be a normal extension (hence also algebraic). Let K_o be the separable closure of k in K. Then K_o/k is also normal.*

Proof. Let σ be a k-embedding of K_o into $\overline{k}$. This means that σ can be lifted to an embedding τ of K, since K/k is algebraic.

Because K/k is normal, $\tau(K) = K$, meaning that $\sigma(K_o) \subset K$. But every element α in K_o is separable over k, so $\sigma(\alpha)$ is also separable over k, meaning that $\sigma(\alpha) \in K_o$. Thus $\sigma(K_o) \subset K_o$, which implies $\sigma(K_o) = K_o$ since K_o/k is a finite algebraic extension. Therefore K_o/k is normal. □

Proposition 15.1.5. *Let E/k be an algebraic extension,* $\mathrm{char}(k) = p$. *Then the following are equivalent:*

(*i*) $[E:k]_s = 1$;

(*ii*) *every element of E is purely inseparable over k;*

Date: October 8th, 2019.

(*iii*) *let* $\alpha \in E$. *Then* $\mathrm{Irr}(\alpha; k, x) = x^{p^n} - \alpha$ *for some* $a \in k$, $n \geq 0$; *and*

(*iv*) *there exists* $\left\{ \alpha_i \;\middle|\; i \in I \right\} \subset E$ *such that* $E = k(\alpha_i \mid i \in I)$, *where* α_i *are purely inseparable over* k.

Proof. For (*i*) implying (*ii*), take $\alpha \in E$. The separable degree has a multiplicative property, so $1 = [E : k]_s = [E : k(\alpha)]_s[k(\alpha) : k]_s$. Hence $[k(\alpha) : k]_s = 1$ as well, whence $\mathrm{Irr}(\alpha; k, x)$ has only one distinct root α, so $\mathrm{Irr}(\alpha; k, x) = (x-\alpha)^{p^\mu} = x^{p^\mu} - \alpha^{p^\mu}$. Thus α is inseparable over k.

For (*ii*) implying (*iii*), we are almost immediately done: $\alpha \in E$ being purely inseparable over k means $\alpha^{p^\mu} = a \in k$.

For (*iii*) implying (*iv*), we have $\alpha^{p^n} = a \in k$, so every $\alpha \in E$ works in (*iv*).

Finally, let us attack (*iv*) implying (*i*). If σ is a k-embedding of E, then σ is determined by $\sigma(\alpha_i)$. Since α_i is purely inseparable, $\sigma(\alpha_i) = \alpha_i$ for every $i \in I$,. Hence $\sigma = \mathrm{Id}_E$, so there is only one distinct embedding of E into $\overline{k}$, whence $[E : k]_s = 1$. □

Definition 15.1.6. Let E be a field of characteristic p. By E^p we mean the set of all p-powers of elements in E. That is, $E^p = \left\{ \alpha^p \;\middle|\; \alpha \in E \right\}$.

Note how E^p is a subfield of E. The only nontrivial part is to show that sums are in there, but in characteristic p, $\alpha^p \pm \beta^p = (\alpha \pm \beta)^p$.

Proposition 15.1.7. *Let* $\mathrm{char}(k) = p$, *and let* E/k *be a finite extension. Then* $E^p k = E$ *if and only if* E/k *is separable.*

Proof. First note that $E^p k = E$ if and only if $E^{p^n} k = E$ for every $n \geq 1$. The reverse direction is trivial—take $n = 1$. For the forward direction, note how $E^{p^2} k = (E^p)^p k = (E^p k)^p k$ since $k^p \subset E^p$. But $E^p k = E$ by assumption, so this is $(E^p k)^p k = E^p k = E$. Repeating this, we get the result.

For the forward direction of the proposition, let E_o be the separable closure of k in E. We want to show that $E_o = E$.

Being a finite extension of k, $E = k(\alpha_1, \alpha_2, \ldots, \alpha_n)$. For each i, there exists some μ_i such that $\alpha_i^{p^{\mu_i}} \in E_o$. Let $n = \max\left\{ \mu_1, \mu_2, \ldots, \mu_n \right\}$. Then $\alpha_i^{p^n} \in E_o$ for all i. Hence $\alpha^{p^n} \in E_o$ for all E, so $E^{p^n} \subset E_o$. By assumption, $E^{p^n} k = E$, so $E = E^{p^n} k \subset E_o k = E_o$, so $E = E_o$ since by construction $E_o \subset E$.

For the converse direction, assume E/k is separable. For $\alpha \in E$, $\alpha^p \in E^p \subset E^p k$. This implies $E/E^p k$ is purely inseparable. But E/k being separable implies $E/E^p k$ is separable, so $E/E^p k$ is both separable and purely inseparable, meaning that $E = E^p k$. □

Proposition 15.1.8. *Let* K/k *be a normal extension, and let* $\mathrm{char}(k) = p$. *Let* $G = \mathrm{Aut}_k(K)$. *Define* $K^G := \left\{ a \in K \;\middle|\; a^g = g \text{ for all } g \in G \right\}$ *be the set of all elements of* K *fixed by* G *(by* a^g *we mean* $g(a)$*). This is a subfield (since automorphism,s being homomorphisms, preserve the field operations). Let* K_o *be the separable closure of* k *in* K.

Then

(*i*) K^G *is the set of all purely inseparable elements of* K *over* k,

(*ii*) $K^G \cap K_o = k$,

(*iii*) K/K^G *is separable,*

(*iv*) $K = K_o K^G$.

Proof. (*i*) Let $\alpha \in K$ be purely inseparable over k. Then for $\sigma \in G$, $\sigma(\alpha) = \alpha$, meaning that $\alpha \in K^G$. Conversely, for $\beta \in K^G$, there exists some $\mu \geq 0$ such that $\beta^{p^\mu} = \gamma$ is separable over k. If we can show that $\gamma \in k$ we are done, since them β is both separable and purely inseparable over k.

To see this, suppose $\gamma \notin k$. Then there exists a k-embedding σ such that $\sigma(\gamma) = \gamma' \neq \gamma$. But σ can be lifted to $\sigma\colon K \to K$, where $\sigma(\beta) = \beta$, so $\sigma(\beta^{p^\mu}) = \beta^{p^\mu}$, meaning that $\sigma(\gamma) = \gamma$, a contradiction.

(*ii*) This part follows from (*i*). An element $\alpha \in K_o \cap K^G$ is both separable and purely inseparable over k, so $\alpha \in k$.

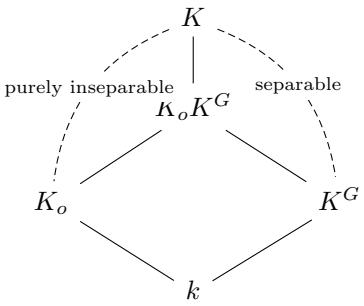
(*iii*) This proof is due to E. Artin. Let $\alpha \in K$, $[k(\alpha) : k] < \infty$. Let $\{ \sigma_1, \sigma_2, \ldots, \sigma_n \}$ be a maximal set of embeddings of K/k such that $\{ \sigma_1(\alpha), \sigma_2(\alpha), \ldots, \sigma_n(\alpha) \}$ are all distinct. In other words, this is the set of all distinct roots of $\mathrm{Irr}(\alpha; k, x)$.

Let $f(x) = \prod(x - \sigma_i(\alpha))$, and take $\sigma \in \mathrm{Aut}_k(K)$. Then

$$f^\sigma(x) = \prod(x - \sigma\sigma_i(\alpha)) = f(x),$$

so $f(x) \in K^G[x]$ since all $\sigma \in G$ fix the coefficients. Hence $f(x)$ is separable, and α is a root of $f(x)$, so α is separable over K^G.

(*iv*) Consider the diagram



Being purely inseparable over a smaller field means purely inseparable over a bigger field, so $K/K_o K^G$ is purely inseparable. Similarly, being separable over a smaller field means separable over a bigger one, so $K/K_o K^G$ is separable. Hence $K = K_o K^G$. □

Definition 15.1.9. A field k is ***perfect*** if every algebraic extension is separable.

Example 15.1.10. The rationals $\mathbb{Q}$ is a perfect field because $\mathrm{char}(\mathbb{Q}) = 0$. For the same reason, any field with characteristic 0 is perfect.

All finite fields are perfect because the elements are roots of $x^{p^n} - x$, which has no repeated roots. ▲

Lecture 16 Galois Theory

16.1 Galois extensions

Definition 16.1.1 (Galois extension)**.** A field extension K/k is ***Galois*** if it is normal (hence algebraic) and separable.

Let $G = \mathrm{Aut}_k(K)$ and let $K^G = \left\{ a \in K \,\middle|\, \sigma(a) = a \text{ for all } \sigma \in G \right\}$ be the subfield of K consisting of all elements fixed by G. Trivially, $k \subset K^G$.

Let $H < G$ be a subgroup. Then similarly define $K^H = \left\{ a \in K \,\middle|\, \sigma(a) = a \text{ for all } \sigma \in H \right\}$.

Theorem 16.1.2 (Fundamental theorem of Galois theory)**.** *Let K/k be a finite Galois extension and let $G = \mathrm{Aut}_k(K)$. Let $\mathcal{F}$ be the set of all subfields F such that $K \supset F \supset k$ and let $\mathcal{H}$ be the set of all subgroups of G.*

Then there is a one-to-one correspondence between $\mathcal{F}$ and $\mathcal{H}$.

Remark 16.1.3. Note that $|\mathcal{F}| < \infty$ by the Primitive element theorem, since K/k is both finite and separable.

Moreover, $|G| < \infty$ since there are only finitely many k-embeddings of K, and hence $|\mathcal{H}| < \infty$.

To demonstrate that the conditions are necessary, consider the following counterexamples.

Counterexample 16.1.4. Let k be a field of characteristic p, and let t and u be variables. Then $k(u,t) \supset k(u^p, t^p)$ is a normal but not separable extension. This is a finite extension—$[k(u,t) : k(u^p,t^p)] = p^2$, but there are infinitely many intermediate subfields. ▲

Counterexample 16.1.5. The extension $\overline{\mathbb{Q}}/\mathbb{Q}$ is normal and separable, and hence Galois. On the one hand $|\overline{\mathbb{Q}}|$ is countable, but $|G|$ is uncountable, where $G = \mathrm{Aut}_{\mathbb{Q}}(\overline{\mathbb{Q}})$.

But $|\mathcal{F}|$ and $|\mathcal{H}|$ are both uncountable, however there isn't a one-to-one correspondence.

As it happens, essentially the same theorem is still true, only for it to work in the infinite case we need a topology (namely the Krull topology) and the correspondence is with *closed* subgroups (and indeed all subgroups are closed in the finite case). ▲

We will spend a fair amount of time working our way up to this fundamental theorem, starting with

Proposition 16.1.6. *Let K/k be a Galois extension (possibly infinite), and let $G = \mathrm{Aut}_k(K)$. Then $K^G = k$.*

Proof. First, $k \subset K^G$ by definition.

Suppose there exists some $\alpha \in K^G \setminus k$. Then $k(\alpha)/k$ is a finite separable extension, so $[k(\alpha) : k]_s = [k(\alpha) : k] > 1$ since $\alpha \notin k$. This means there exists some $\sigma \neq \mathrm{Id}$ such that $\sigma \colon k(\alpha) \hookrightarrow \overline{k}$ is a k-embedding (so in particular $\sigma(\alpha) \neq \alpha$).

Date: October 15th, 2019.

Since $K/k(\alpha)$ is algebraic, we can lift σ to $\tau\colon K \hookrightarrow \overline{k}$, also a k-embedding, and since K/k is normal, $\tau(K) = k$, so $\tau \in G$.

But $\tau(\alpha) \neq \alpha$ since it restricts to σ, and this contradicts $\alpha \in K^G$. Hence $K^G = k$. □

Definition 16.1.7 (Galois group)**.** Let K/k be Galois. The ***Galois group*** of K/k is defined as $\mathrm{Gal}(K/k) \coloneqq \mathrm{Aut}_k(K)$.

Theorem 16.1.8. *Let K/k be a Galois extension. Let F, $k \subset F \subset K$ be an intermediate subfield. Then K/F is also Galois. Moreover, letting $H = \mathrm{Gal}(K/F)$, $K^H = F$.*

Proof. If $\sigma\colon K \hookrightarrow \overline{k}$ is an F-embedding, then it is also a k-embedding since $k \subset F$. Since K/k is normal, this means $\sigma(K) = K$, and so K/F is also normal.

Since the class of separable extensions is distinguished, K/k being separable implies K/F is separable. Hence K/F is Galois.

For the second part, simply use the previous proposition. □

The situation, so far, is this: if K/k is Galois and $G = \mathrm{Gal}(K/k)$, then starting with an intermediate subfield F, $k \subset F \subset K$, we have a subgroup $H = G_F = \mathrm{Gal}(K/F)$ of G, and by the above theorem we can pull this back to $K^H = F$.

Hence, in the Galois correspondence, we know that $\mathcal{F} \to \mathcal{H}$ is one-to-one, and the opposite direction $\mathcal{H} \to \mathcal{F}$ is onto.

The big question, then, is if we can go the other way: if we start with a subgroup $H < G$, move to K^H, and then pull back to $H' = \mathrm{Gal}(K/K^H)$ on the group side, we have $H' \supset H$, but are they equal?

In the finite case, the answer turns out to be yes. In the infinite case they need not be, but H' is the closure of H in the Krull topology.

There are some simple results we can establish about these objects that we will make use of shortly. Let K/k be Galois, and let $k \subset K_i \subset K$, $i = 1, 2$, and let $H_i = \mathrm{Aut}_{F_i}(K)$. Then

(*i*) $\mathrm{Aut}_{F_1F_2}(K) = H_1 \cap H_2$;

(*ii*) letting $H = \langle H_1, H_2 \rangle$, then $K^H = F_1 \cap F_2$; and

(*iii*) $F_1 \supset F_2$ if and only if $H_1 \subset H_2$.

Theorem 16.1.9 (Artin)**.** *Let K be a field. Let G be a* finite *subgroup of* $\mathrm{Aut}(K)$*. Then K/K^G is Galois, and $G = \mathrm{Gal}(K/K^G)$.*

To prove the second part of this theorem we will make use of the following lemma:

Lemma 16.1.10. *Let E/k be a separable extension. Suppose $[k(\alpha) : k] \leq n$ for all $\alpha \in E$. Then $[E : k] \leq n$.*

Proof. Take $\alpha \in E$ such that $[k(\alpha) : k] = m = \max_{\beta \in E}[k(\beta) : k]$.

We claim that $E = k(\alpha)$. To see this, suppose $E \neq k(\alpha)$, i.e., there exists some $\beta \in E \setminus k(\alpha)$. Then

$$[k(\alpha, \beta) : k] = [k(\alpha, \beta) : k(\alpha)][k(\alpha) : k] > m$$

since $\beta \notin k(\alpha)$ means $[k(\alpha,\beta) : k(\alpha)] > 1$ and $[k(\alpha) : k] = m$. But $k(\alpha,\beta)/k$ is a finite and separable extension, so by the Primitive element theorem it is simple, meaning that $k(\alpha,\beta) = k(\gamma)$ for some $\gamma \in E$. But this contradicts the maximality of $[k(\alpha) : k]$. □

Proof of Theorem 16.1.9. By definition $K^G = \left\{ a \in K \middle| g(a) = a \text{ for all } g \in G \right\}$. For any $\alpha \in K$, let $\left\{ \sigma_1(\alpha), \sigma_2(\alpha), \ldots, \sigma_r(\alpha) \right\}$ be a maximal set of distinct elements obtained by applying $\sigma \in G$.

Note that since $|G| = n$ is finite by assumption, $r \leq n$.

Take $\sigma_1(\alpha) = \alpha$, and let

$$f_\alpha(x) = \prod_{i=1}^{r} (x - \sigma_i(\alpha)).$$

Note that for $\sigma \in G$, $\left\{ \sigma\sigma_1(\alpha), \ldots, \sigma\sigma_r(\alpha) \right\} = \left\{ \sigma_1(\alpha), \ldots, \sigma_r(\alpha) \right\}$, so σ just permutes the roots. Hence $f_\alpha^\sigma = f_\alpha$, meaning that $f_\alpha \in K^G[x]$¿ Moreover f_α is separable by construction, so α is a root of a separable polynomial in $K^G[x]$, so α is separable over K^G. Hence K/K^G is separable.

Since K is the splitting field of a family $\left\{ f_\alpha(x) \in K^G[x] \;\middle|\; \alpha \in K \right\}$, K/K^G is normal.

Hence in all, K/K^G is Galois.

Secondly we wish to show that $G = \mathrm{Gal}(K/K^G)$. For $\alpha \in K$, $\mathrm{Irr}(\alpha; K^G, x) \mid f_\alpha(x)$. Now $\deg f_\alpha = r \leq n = |G|$, so $\deg \mathrm{Irr}(\alpha; K^G, x) \leq n$, meaning that $[K^G(\alpha) : K^G] \leq n$ for all $\alpha \in K$.

By the lemma, this means $[K : K^G] \leq n = |G|$, so

$$G \subset \mathrm{Gal}(K/K^G) = \mathrm{Aut}_{K^G}(G),$$

but

$$|\mathrm{Gal}(K/K^G)| = [K : K^G]_s = [K : K^G] = n,$$

since K/K^G is separable, and $n \leq |G|$, so G and $\mathrm{Gal}(K/K^G)$ have the same order, so they are equal. □

Lecture 17 Artin's Theorem

17.1 Examples

Definition 17.1.1. Let K be any field, and let k_o be the smallest subfield containing 1. Then k_o is called the ***prime field*** of K.

In particular, if $\mathrm{char}(K) = 0$, then $k_o \cong \mathbb{Q}$, and if $\mathrm{char}(K) = p$, then $k_o \cong \mathbb{F}_p$.

In this setting, $\mathrm{Aut}(K) = \mathrm{Aut}_{k_o}(K)$ by definition. In Artin's theorem, K/k_o may be transcendental.

Example 17.1.2. Let $k = \mathbb{C}$ and let $K = \mathbb{C}(x)$, where x is a variable. Then K/k is transcendental, and

$$\mathrm{Aut}_k(K) = \left\{ \sigma \colon x \mapsto \frac{ax+b}{cx+d} \;\middle|\; a,b,c,d \in \mathbb{C} \text{ and } ad - bc \neq 0 \right\} \cong \mathrm{PGL}_2(\mathbb{C}).$$

Date: October 17th, 2019.

If $G = \mathrm{Aut}_k(K)$, then $K^G = k$, and K/K^G is not Galois. This does not contradict Artin's theorem, because G is not finite.

If $G = \langle\sigma\rangle$, $\sigma\colon x \mapsto \sqrt{-1}x$, then $\sigma^4 = \mathrm{Id}$, so $|G| = 4$, and indeed $G \cong \mathbb{Z}_4$.

Then $K^G = \mathbb{C}(x^4)$, and $K/K^G = \mathbb{C}(x)/\mathbb{C}(x^4)$ is Galois. To see this, notice how

$$f(t) = \mathrm{Irr}(x; K^G, t) = t^4 - x^4 \in K^G[x],$$

and in $\mathbb{C}(x)$ this factors at $(t-x)(t+x)(t-\sqrt{-1}x)(t+\sqrt{-1}x)$. This splits in $\mathbb{C}(x)$ and is separable over $\mathbb{C}(x^4)$, so the extension is normal and separable. ▲

Lecture 18 Infinite Version of Artin's Theorem

18.1 Generalising Artin's theorem

Notice how in our proof of Artin's theorem, the only time we used the finiteness of $|G|$ was to establish that the maximal set $\{\,\sigma_1(\alpha), \ldots, \sigma_r(\alpha)\,\}$ is finite.

This immediately tells us we can generalise Artin's theorem to infinite groups G, provided we know this set is again finite. An easy way to do so is to just require K/k be algebraic, since then $\sigma(\alpha)$, $\sigma \in G$ are all roots of a certain irreducible polynomial, and that polynomial has only finitely many roots.

Theorem 18.1.1. *Assume K/k is algebraic. Let $G \leq \mathrm{Aut}_k(K)$ (possibly infinite). Then K/K^G is Galois.*

Proof. For any $\alpha \in K$, the set $\{\,\sigma(\alpha) \mid \sigma \in G\,\}$ is finite, since all $\sigma(\alpha)$ are roots of $\mathrm{Irr}(\alpha; k, x)$ because K/k is algebraic.

Take $\{\,\sigma_1(\alpha), \sigma_2(\alpha), \ldots, \sigma_r(\alpha)\,\}$ to be a maximal set of distinct elements and consider $f_\alpha(x) = (x - \sigma_1(\alpha)) \cdots (x - \sigma_r(\alpha))$. Notice how $f_\alpha^\sigma(x) = f_\alpha(x)$ for all $\sigma \in G$, meaning that $f_\alpha(x) \in K^G[x]$. Now as in the proof of the finite version of Artin's theorem, this means K/K^G is Galois. □

Remark 18.1.2. Notice how $\sup\limits_{\alpha \in K} \deg f_\alpha$ may be infinite, so K/K^G may be infinite Galois.

Similarly, we do get $G \leq \mathrm{Gal}(K/K^G)$. In the finite case, we compared the order of these groups to conclude that they are equal. In the infinite case we cannot do that, and indeed the groups need not be equal.

The situation, as we have discussed at some point in the past, is this: Let K/k be Galois and let $\mathcal{F}$ be the set of all intermediate subfields and let $\mathcal{H}$ be the set of all subgroups of $G = \mathrm{Gal}(K/k)$.

Define $\Gamma\colon \mathcal{F} \to \mathcal{H}$ by $F \mapsto \mathrm{Gal}(K/F)$ and define $\Phi\colon \mathcal{H} \to \mathcal{F}$ by $H \mapsto K^H$.

Then we have already showed $\Phi \circ \Gamma = \mathrm{Id}_{\mathcal{F}}$.

For the reverse direction, we have to consider two cases.

First: K/k is finite Galois. Then $H \leq G$ is a finite subgroup. Standard Artin then tells us K/K^H is Galois and $H = \mathrm{Gal}(K/K^H)$, so in this case $\Gamma \circ \Phi = \mathrm{Id}_{\mathcal{H}}$.

In other words, in this case Γ and Φ are one-to-one and onto correspondences.

Second: K/k is infinite Galois. In this case, by infinite Artin, we know K/K^H is Galois and $H \leq \mathrm{Gal}(K/K^H) = H'$. Since H and H' are not necessarily the same, $\Gamma \circ \Phi \neq \mathrm{Id}_{\mathcal{H}}$.

Date: October 22nd, 2019.

That said, if $H \leq G$ is a finite subgroup, then we do have $\Gamma \circ \Phi(H) = H$, and K/K^H is a finite Galois extension (with $[K : K^H] = |H|$).

This gives us a modified version of Galois' theorem:

Theorem 18.1.3. *Let $\mathcal{F}_o$ be the set of all intermediate subfields F such that $[K : F] < \infty$. Let $\mathcal{H}_o$ be the set of all finite subgroups of G. Then $\mathcal{F}_o \leftrightarrow \mathcal{H}_o$ is a one-to-one and onto correspondence.*

18.2 Conjugation

Definition 18.2.1 (Conjugatation)**.** Let $\| \supset E \supset k$ and let $\sigma \in \mathrm{Aut}_k(\overline{k})$. The field $\sigma(E)$ is called a ***conjugation*** of E and for $\alpha \in E$, $\sigma(\alpha)$ is called a ***conjugate*** of α.

Proposition 18.2.2. *Let K/k be Galois and let $G = \mathrm{Gal}(K/k)$. Let $\sigma \in G$. Let $k \subset F \subset K$, and take $H = \mathrm{Gal}(K/F)$. Then $\mathrm{Gal}(K/\sigma(F)) = \sigma H \sigma^{-1}$.*

In other words, conjugate fields have conjugate Galois groups.

Proof. Let $\tau \in \mathrm{Gal}(K/\sigma(F))$. For all $a \in F$, $\tau(\sigma(a)) = \sigma(a)$, so $\sigma^{-1} \circ \tau \circ \sigma(a) = a$, meaning that $\sigma^{-1} \circ \tau \circ \sigma \in H$, so $\tau \in \sigma H \sigma^{-1}$.

On the other hand, for $h \in H$, $a \in F$, we have $\sigma h \sigma^{-1}(\sigma(a)) = \sigma h(a) = \sigma(a)$, so $\sigma h \sigma^{-1} \in \mathrm{Gal}(K/\sigma(F))$, so $\sigma H \sigma^{-1} \subset \mathrm{Gal}(K/\sigma(F))$. □

Proposition 18.2.3. *Let K/k be Galois. Let $G = \mathrm{Gal}(K/k)$ and let $K \supset F \supset k$. Then F/k is Galois if and only if $H = \mathrm{Gal}(K/F)$ is a normal subgroup of G.*

Moreover, $\mathrm{Gal}(F/k) \cong G/H$.

Proof. The extension F/k is Galois if and only if F/k is normal (separability is always true since K/k is separable) if and only if $\sigma(F) = F$ for every $\sigma \in G$, if and only if $\sigma H \sigma^{-1} = H$ for every $\sigma \in G$, if and only if H is normal in G.

For the isomorphism, consider $\varphi \colon G \to \mathrm{Gal}(F/k)$ defined by $\rho \mapsto \rho\big|_F$. This is well-defined since $\rho(F) = F$ because F/k is normal. It is clear that φ is a group homomorphism.

Suppose $\rho \in \ker \varphi$. This means $\rho\big|_F = \mathrm{Id}_F$, i.e., ρ fixes F, meaning that $\rho \in \mathrm{Gal}(K/F) = H$. So $\ker \varphi = H$.

Since K/F is Galois, every $\sigma \in \mathrm{Gal}(F/k)$ can be lifted to $\mathrm{Gal}(K/k)$, so φ is also onto.

Hence by the isomorphism theorem, $G/\ker \varphi \cong \mathrm{Im}\, \varphi$, or in other words $G/H \cong \mathrm{Gal}(F/k)$. □

18.3 Lifts and Galois extensions

Proposition 18.3.1. *Let K/k be Galois. Let F/k be any extension. Then*

(*i*) *$K/(K \cap F)$ is Galois,*

(*ii*) *KF/F is Galois, and*

(*iii*) $\mathrm{Gal}(KF/F) \cong \mathrm{Gal}(K/(K \cap F))$.

Proof. (*i*) This is trivial: being Galois over a small field implies Galois over a bigger field.

(*ii*) Both normality and separability are preserved by lifting, so this, too, is clear.

(*iii*) Let $G = \mathrm{Gal}(KF/F)$ and $H = \mathrm{Gal}(K/(K \cap F))$. Define $\varphi\colon G \to H$ by $\rho \mapsto \rho\big|_K$. This fixes $K \cap F$ since it fixes F, which is bigger. This is a homomorphism, and if $\rho \in \ker\varphi$, then $\rho\big|_K = \mathrm{Id}_K$, but $\rho\big|_F = \mathrm{Id}_F$. Hence $\rho = \mathrm{Id}_{KF}$, so $\ker\varphi = \{\,\mathrm{Id}\,\}$, so φ is one-to-one.

We claim that φ is onto.

First, consider the case where K/k is a finite Galois extension. Then $\mathrm{Im}\,\varphi = \{\,\sigma\big|_K \mid \sigma \in G\,\} = H' \leq H$. We want to show that $H' = H$. If we can show that $K^{H'}$, then $H = \mathrm{Gal}(K/(K \cap F)) = H'$, so the claim follows.

Note that clearly $K \cap H \subset K^{H'}$. Suppose there exists some $\alpha \in K^{H'} \setminus (K \cap F)$. Then $F(\alpha) \supsetneq F$, but $\sigma(\alpha) = \alpha$ for every $\sigma \in H'$, so $\sigma(\alpha) = \alpha$ for every $\sigma \in G$. Hence $\alpha \in (KF)^G = F$, which is a contradiction.

Second, consider the case where K/k is an infinite Galois extension. Let $\{\,K_\lambda \mid \lambda \in \Lambda\,\}$ be the set of all intermediate fields K_λ such that $K \supset K_\lambda \supset k$ and $[K_\lambda : k] < \infty$ and K_λ/k is Galois.

Note that $K = \bigcup\limits_{\lambda\in\Lambda} K_\lambda$, and by the first case $\mathrm{Gal}(K_\lambda/(K_\lambda \cap F)) \cong \mathrm{Gal}(K_\lambda F/F)$.

We want to show that any $\rho \in \mathrm{Gal}(K/(K \cap F))$ can be lifted to $\mathrm{Gal}(KF/F)$. Given $\rho \in \mathrm{Gal}(K/(K \cap F))$, define $\rho_\lambda = \rho\big|_{K_\lambda} \in \mathrm{Gal}(K_\lambda/(K_\lambda \cap F))$ for $\lambda \in \Lambda$.

By the finite case, we can lift ρ_λ to $\sigma_\lambda \in \mathrm{Gal}(K_\lambda F/F)$. For $\alpha \in KF$, we must have $\alpha \in FK_\lambda$ for some λ, and so define $\sigma(\alpha) = \sigma_\lambda(\alpha)$.

We claim that $\sigma \in \mathrm{Gal}(KF/F)$. First of all, it is well-defined—if we have another $K_{\lambda'}$, then K_λ and $K_{\lambda'}$, with their corresponding ρ_λ and $\rho_{\lambda'}$, may have an intersection. So do the lifts σ_λ and $\sigma_{\lambda'}$ have the same image on α? The answer is yes—look at $K_\lambda K_{\lambda'} = K_\beta$, and consider the lift σ_β of λ_β. Then restricted to K_λ this becomes σ_λ, and restricted to $K_{\lambda'}$ it becomes $\sigma_{\lambda'}$. □

Lecture 19 Special Kinds of Galois Extensions

19.1 Cyclic, abelian, nilpotent, and solvable extensions

Definition 19.1.1. Let K/k be Galois and let $G = \mathrm{Gal}(K/k)$. If G is cyclic (abelian, nilpotent, solvable) then we say that the extension K/k is ***cyclic*** (***abelian***, ***nilpotent***, ***solvable***).

Let us recall what the latter of these two mean:

Definition 19.1.2. Let G be a group and let

$$Z(G) = \{\, z \in G \mid gz = zg \text{ for all } g \in G\,\}$$

be the ***centre*** of G. This is a normal subgroup. Consider the map $\varphi_1\colon G \to G/Z(G)$, and consider the pullback $Z_2(G) = \varphi_1^{-1}(Z(G/Z(G)))$, which, being the pullback of a normal subgroup, is normal. Repeat, i.e., consider $\varphi_2\colon G \to G/Z_2(G)$, define $Z_3(G) = \varphi_2^{-1}(Z(G/Z_2(G)))$, and so on.

Date: October 24th, 2019.

Then we have a sequence of normal subgroups

$$\{ 1 \} < Z(G) < Z_2(G) < \ldots < Z_n(G) < \ldots < G.$$

We say that G is ***nilpotent*** if $G = Z_n(G)$ for some n.

Definition 19.1.3. A group G is ***solvable*** if there exists a sequence

$$G = G_0 > G_1 > G_2 > \ldots > G_s = \{ 1 \}$$

of subgroups such that G_i is normal in G_{i-1} and G_{i-1}/G_i is abelian.

Exercise 19.1.4. If G is nilpotent (solvable), then every subgroup of G is nilpotent (solvable).

(The same is true, but very trivial, for cyclic and abelian, of course.)

Proposition 19.1.5. *If K/k is cyclic (abelian, nilpotent, solvable) and $k \subset F \subset K$ is an intermediate subfield, then K/F is cyclic (abelian, nilpotent, solvable).*

Proof. Because $\mathrm{Gal}(K/F) < \mathrm{Gal}(K/k)$, all of this is immediate. □

Proposition 19.1.6. *If K/k is cyclic (abelian) and F is an intermediate subfield. Then F/k is cyclic (abelian).*

Proof. This follows from noting that $\mathrm{Gal}(K/F)$ is normal in $\mathrm{Gal}(K/k)$ is K/k is cyclic (abelian), and then $\mathrm{Gal}(F/k) \cong \mathrm{Gal}(K/k)/\mathrm{Gal}(K/F)$. □

Theorem 19.1.7. *Let K_1/k and K_2/k be Galois extensions and let $G_i = \mathrm{Gal}(K_i/k)$, $i = 1, 2$. Then K_1K_2/k is Galois and $\mathrm{Gal}(K_1K_2/k)$ is isomorphic to a subgroup of $G_1 \times G_2$.*

Moreover if $K_1 \cap K_2 = k$, then $\mathrm{Gal}(K_1K_2/k) \cong G_1 \times G_2$.

Proof. Normality and separability are preserved by composition, so K_1K_2/k being Galois is trivial.

Define $\varphi\colon \mathrm{Gal}(K_1K_2/k) \to G_1 \times G_2$ by $\rho \mapsto (\rho\big|_{K_1}, \rho\big|_{K_2})$.

Suppose $\rho \in \ker\varphi$. Then $\rho\big|_{K_1} = \mathrm{Id}_{K_1}$ and $\rho\big|_{K_2} = \mathrm{Id}_{K_2}$, meaning that $\rho\big|_{K_1K_2}$. Hence φ is one-to-one. This means $\mathrm{Gal}(K_1K_2/k)$ is a subgroup of $G_1 \times G_2$.

Now assume $K_1 \cap K_2 = k$. By the lifting property,

$$\mathrm{Gal}(K_1/k) \cong \mathrm{Gal}(K_1K_2/K_2) \subset \mathrm{Gal}(K_1K_2/k).$$

Since $\mathrm{Gal}(K_1/k)$ embeds into $G_1 \times G_2$ by $g \mapsto (g, \mathrm{Id}_{K_2})$, meaning that $G_1 \times \{ \mathrm{Id}_{K_2} \} \subset \mathrm{Im}(\varphi)$, and similarly $\{ \mathrm{Id}_{K_1} \} \times G_2 \subset \mathrm{Im}(\varphi)$. Hence $G_1 \times G_2 \subset \mathrm{Im}(\varphi)$, so φ is onto in this case, meaning that $\mathrm{Gal}(K_1K_2/k) \cong G_1 \times G_2$. □

Theorem 19.1.8. *Let K_i/k be Galois and $G_i = \mathrm{Gal}(K_i/k)$, $i = 1, 2, \ldots, n$. Assume $K_i \cap (K_1K_2 \cdots K_{i-1}) = k$, $i = 1, 2, \ldots, n$. Then*

$$\mathrm{Gal}(K_1K_2 \cdots K_n/k) \cong G_1 \times G_2 \times \ldots \times G_n.$$

Proof. Let $E = K_1K_2 \cdots K_{n-1}$. Then $E \cap K_n = k$, so

$$\mathrm{Gal}(EK_n/k) \cong \mathrm{Gal}(E/k) \times G_n$$

by the previous theorem. Now repeat on E. □

Theorem 19.1.9. *Let K/k and L/k be abelian. Then KL/k is abelian.*

Proof. Since $\mathrm{Gal}(KL/k) \hookrightarrow \mathrm{Gal}(K/k) \times \mathrm{Gal}(L/k)$, and the two factors on the left are abelian, the product is abelian, and so is any subgroup of it. □

Definition 19.1.10. Let $\overline{k} \supset k$. We define the ***abelian closure*** k^{ab} as the largest abelian extension of k in $\overline{k}$. (This exists because, by the theorem, any composition of abelian groups is abelian, and there is at least one abelian extension (namely k itself), so there is a maximal one by Zorn.) In fact, k^{ab} is the composition of all abelian extensions E/k.

That is to say, let $\left\{ E_\lambda \,\middle|\, \overline{k} \supset E_\lambda \supset k,\ E_\lambda/k \text{ abelian} \right\}$. Then

$$k^{ab} = \prod_\lambda E_\lambda$$

and

$$\mathrm{Gal}(k^{ab}/k) \hookrightarrow \prod_\lambda \mathrm{Gal}(E_\lambda/k),$$

where the right-hand side is abelian.

Example 19.1.11. Consider $\overline{\mathbb{Q}} \supset \mathbb{Q}$. There is almost nothing known about $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, but we do know something about $\mathbb{Q}^{ab}/\mathbb{Q}$. In particular,

$$\mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) \cong \prod_p \mathbb{Z}_p^\times,$$

where $\mathbb{Z}_p$ is the p-adic integers. ▲

19.2 Examples and applications

In the proceeding discussion, we will always let k denote a base field and $\overline{k}$ an algebraic closure of k.

Let $f(x) \in k[x]$ be monic and separable, $\deg f = n$. Then

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

for $\alpha_i \in \overline{k}$.

Let $K = k(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Then K/k is Galois, and let $G = \mathrm{Gal}(K/k)$.

The group G permutes $\left\{ \alpha_1, \alpha_2, \ldots, \alpha_n \right\}$, and any $\sigma \in G$ is determined by its image on this set. So G is a permutation of n elements, meaning that $G \hookrightarrow S_n$, the symmetric group of n elements. In particular this means $|G| \leq n!$.

Example 19.2.1. Let $\deg f = 2$, the quadratic case. Assume that $\mathrm{char}(k) \neq 2$, so that we can complete the square,

$$f(x) = x^2 + \alpha x + \beta = \left(x - \frac{\alpha}{2}\right)^2 + \beta - \frac{\alpha^2}{4}.$$

Then we may assume $f(x) = x^2 + a \in k[x]$ by a change of variables.

Note how $f(x)$ is irreducible if and only if $\sqrt{a} \notin k$, i.e., a isn't the square of any element in k, so f has no root in k. Then $f(x) = (x - \sqrt{a})(x + \sqrt{a})$ in $\overline{k}[x]$, and $G \hookrightarrow S_2 \cong \mathbb{Z}_2$. So either $|G| = 1$ or $|G| = 2$. If $|G| = 1$, then both roots of f in $\overline{k}$ are equal, so f is not separable, which is a contradiction. Hence $|G| = 2$, so $G \cong S_2 \cong \mathbb{Z}_2$.

In the $\mathrm{char}(k) = 2$ case, note that in $\mathbb{F}_2$, the only irreducible quadratic polynomial if $x^2 + x + 1$. ▲

Example 19.2.2. Now consider the cubic case, $\deg f = 3$, and for the same reason assume $\operatorname{char}(k) \neq 2, 3$. We may assume $f(x) = x^3 + ax + b \in k[x]$ by a change of variables, and $f(x)$ is irreducible. Then

$$f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$$

for $\alpha_i \in \overline{k}$, and $G \hookrightarrow S_3$. Now $|S_3| = 3! = 6$, and $[K : k] = |G|$, but $[k(\alpha_1) : k] = 3$, so $3 \mid |G|$, implying that $G \cong A_3$ or $G \cong S_3$, since either $|G| = 3$ or $|G| = 6$.

To determine which of the two is the case, let $\delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)$, and set

$$\Delta = \delta^2 = \prod_{1 \leq i < j \leq 3} (\alpha_i - \alpha_j)^2.$$

Recall how G permutes $\{\alpha_1, \alpha_2, \alpha_3\}$. Suppose $\sigma \in G$ is a transposition, i.e., it switches two of them and keeps the third fixed. Then $\sigma(\delta) = -\delta$.

Hence in general, if σ is an odd permutation, $\sigma(\delta) = -\delta$, and if σ is an even permutation, then $\sigma(\delta) = \delta$.

In either case, this means $\sigma(\Delta) = \Delta$ for all $\sigma \in G$. But that means G fixes Δ, so $\Delta \in k$.

There are two cases to consider. If Δ is a square in k, i.e., $\Delta = \varepsilon^2$ for some $\varepsilon \in k$, then $\Delta = \varepsilon^2 = \delta^2$, so $\delta = \pm\varepsilon \in k$. Hence for $\sigma \in G$, $\sigma(\delta) = \delta$, so G does not contain an odd permutation, meaning that $G \cong A_3$.

On the other hand, if Δ is not a square in k, then $\delta \notin k$, so there exists a $\sigma \in G$ with $\sigma(\delta) \neq \delta$, whence $\sigma(\delta) = -\delta$. Therefore G contains an odd permutation, so $G \cong S_3$.

In conclusion, for $f(x) = x^3 + ax + b \in k[x]$ with $\operatorname{char}(k) \neq 2, 3$, let

$$\Delta = \prod_{1 \leq i < j \leq 3} (\alpha_i - \alpha_j)^2,$$

the ***discriminant*** of f.

If Δ is a square in k, then $G \cong A_3$, and if Δ is not a square in k, then $G \cong S_3$.

This is easy to check, because as it happens $\Delta = -4a^3 - 27b^2$. This comes from comparing $x^3 + ax + b = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$.

Hence for example, consider $f(x) = x^3 - x + 1 \in \mathbb{Q}[x]$. Then $\Delta = -4(-1)^3 - 27(1)^2 = -23$, which is not a square in $\mathbb{Q}$, so $G \cong S_3$.

On the other hand, if $f(x) = x^3 - 3x + 1 \in \mathbb{Q}[x]$, $\Delta = -4(-3)^3 - 27(1)^2 = 81 = 9^2$, so $G \cong A_3$. ▲

Lecture 20 Galois Group of a Polynomial

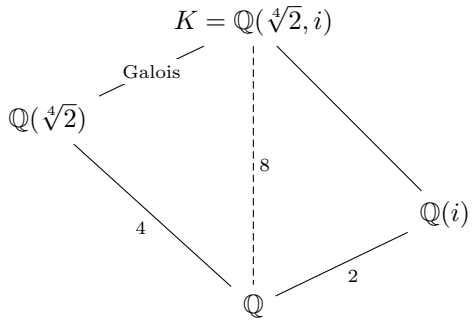
20.1 Galois group of polynomials

Let $f(x) \in k[x]$ be separable, and let K be the split field of f. Then K/k is Galois, and we write $\operatorname{Gal}(f) = \operatorname{Gal}(K/k)$.

Example 20.1.1. Consider $f(x) = x^4 - 2$ $in\mathbb{Q}[x]$. By Eisenstein's criterion this is irreducible. We want to figure out what $\operatorname{Gal}(f)$ is.

Date: October 29th, 2019.

In the splitting field, $f(x) = (x - \sqrt[4]{2})(x - \sqrt[4]{2}i)(x + \sqrt[4]{2})(x + \sqrt[4]{2}i)$, so the situation looks like



where $K/Q(\sqrt[4]{2})$ is Galois because $\mathbb{Q}(i)/\mathbb{Q}$ is Galois, and it lifts. We also have $\mathbb{Q} = \mathbb{Q}(\sqrt[4]{2}) \cap \mathbb{Q}(i)$, since the former is real and the latter is complex.

Hence $|\mathrm{Gal}(f)| = 8$. Thus to identify what group $\mathrm{Gal}(f)$ is, note how the groups of order 8 are $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ (all abelian) and D_4 (the dihedral group) and Q_8 (the quaternion group), the latter two being nonabelian.

Now G contains an automorphism τ sending i to $-i$ and $\sqrt[4]{2}$ to itself, whence $\tau^2 = \mathrm{Id}$ is of order two, and an automorphism σ sending i to i and $\sqrt[4]{2}$ to $i\sqrt[4]{2}$, so $\sigma^4 = \mathrm{Id}$ is of order 4.

Hence $G \supset \langle \tau, \sigma \rangle \cong D_4$, meaning that $G = D_4$. ▲

Lecture 21 Examples of Galois Groups

21.1 More examples

Example 21.1.1. Let k be a field and let $t_1, t_2, \ldots, t_n$ be variables. Let $K = k(t_1, t_2, \ldots, t_n)$.

The symmetric group S_n acts on K/k by permuting $\{t_1, t_2, \ldots, t_n\}$, so $G = S_n \subset \mathrm{Aut}_k(K)$, and $|S_n| = n!$, so $G = S_n$ is finite. Let $F = K^G$. By Artin's theorem, K/F is Galois, and $\mathrm{Gal}(K/F) = G$.

So, aside from $F = K^G$, how might we describe F?

Elements in $K^G \subset K$ are rational functions in $t_1, t_2, \ldots, t_n$, and they have to be fixed by all $\sigma \in G$, so they must be symmetric polynomials.

The simplest symmetric polynomials are the ***elementary symmetric polynomials*** of $t_1, t_2, \ldots, t_n$,

$$\begin{aligned} s_1 &= t_1 + t_2 + \ldots + t_n \\ s_2 &= t_1t_2 + t_1t_3 + \ldots + t_1t_n + t_2t_3 + \ldots + t_2t_n + \ldots + t_{n-1}t_n, \\ &\vdots \\ s_n &= t_1t_2 \cdots t_n. \end{aligned}$$

All of these are fixed by G. Hence, letting $E \coloneqq k(s_1, s_2, \ldots, s_n)$, since $s_i^\sigma = s_i$ for every $\sigma \in G$, $E \subset F$.

Date: October 31st, 2019.

We claim $E = F$. One way to see this is to note that $[K : F] = n!$, so if we can show that $[K : E] \leq n!$, then $E = F$. Consider

$$f(x) = (x-t_1)(x-t_2)\cdots(x-t_n) = x^n - s_1x^{n-1} + s_2x^{n-2} - s_3x^{n-3} + \ldots + (-1)^n s_n.$$

Therefore $f(x) \in E[x]$, so $K = E(t_1, t_2, \ldots, t_n)$ is the splitting field of $f(x)$ over E, and $\deg f(x) = n$, so $[K : E] \leq n!$ (and in fact it divides $n!$). ▲

Remark 21.1.2. Every symmetric polynomial can be expressed as a polynomial of elementary symmetric polynomials. Hence if $f_1, f_2, \ldots, f_m$ are symmetric polynomials.

Remark 21.1.3. A large reason we care about this is this: Every finite group H is a subgroup of S_n for some n. Hence there exists a Galois extension K/F such that $\mathrm{Gal}(K/F) = H$.

Let $f(x) \in k[x]$ be separable, and write $f(x) = (x - \alpha_1)\cdots(x - \alpha_n)$ in some algebraic closure. Define

$$\delta = \delta(f) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)$$

and

$$\Delta = \Delta(f) = \delta^2 = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2,$$

the ***discriminant*** if f.

The degree three discussion we had previously generalises in one case, and not quite in the other:

Theorem 21.1.4. *Let $f(x) \in k[x]$ be separable. Let K be the splitting field of f over k, and $G = \mathrm{Gal}(K/k)$. Let $n = \deg f$.*

Then $G \hookrightarrow A_n$ if and only of Δ is a square in k.

Proof. Note that $G \hookrightarrow S_n$, and $\Delta = \delta^2 \in k$ since $\Delta \in K^G$.

For the forward direction, suppose $G \hookrightarrow A_n$. This means $\sigma(\delta) = \delta$ for all $\sigma \in G$, whence $\delta \in k$, so $\Delta = \delta^2$ is a square in k.

For the converse direction, suppose $\Delta = \varepsilon^2$ for $\varepsilon \in k$. But $\Delta = \delta^2$, whence $\delta = \pm\varepsilon \in k$, so $\sigma(\delta) = \delta$ for all $\sigma \in G$. Thus σ is even for all $\sigma \in G$, else it switches sign. □

Theorem 21.1.5. *Let p be a prime and $f(x) \in \mathbb{Q}[x]$ be irreducible of degree p. Suppose $f(x)$ has exactly 2 nonreal roots. Then $\mathrm{Gal}(f) \cong S_p$.*

Proof. Recall how S_p is generated by one transposition and one p-cycle, and also note how $\mathrm{Gal}(f) \hookrightarrow S_p$.

Let $\{\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_p\}$ be the roots of $f(x)$, and suppose α_1, α_2 are the nonreal roots.

Let τ be the complex conjugate. Then $\tau(\alpha_1) = \alpha_2$, $\tau(\alpha_2) = \alpha_1$, since complex roots of real polynomials come in complex conjugate pairs, and $\tau(\alpha_i) = \alpha_i$ for all $i \geq 3$. Hence $\tau = (1\ 2)$ in S_p.

Second, $\mathrm{Gal}(f)$ acts transitively on the roots $\{\alpha_1, \alpha_2, \ldots, \alpha_p\}$, so the permutation

$$\sigma\colon \alpha_1 \mapsto \alpha_2 \mapsto \alpha_3 \mapsto \ldots \mapsto \alpha_p \mapsto \alpha_1,$$

i.e., $\sigma = (1\ 2\ \cdots\ p) \in \mathrm{Gal}(f)$. Hence $S_p = \langle \tau, \sigma \rangle \hookrightarrow \mathrm{Gal}(f)$, and $\mathrm{Gal}(f) \hookrightarrow S_p$, so $\mathrm{Gal}(f) \cong S_p$. □

Example 21.1.6. Let $f(x) = x^3 - 2 \in \mathbb{Q}[x]$. This has two nonreal roots, so $\mathrm{Gal}(f) \cong S_3$. ▲

Example 21.1.7. Consider $f(x) = x^5 - 4x + 2 \in \mathbb{Q}[x]$. This is irreducible by Eisenstein's criterion, and has two nonreal roots. Its degree is prime, so $\mathrm{Gal}(f) = \cong S_5$. ▲

21.2 Roots of unity

Let k be a field. The roots of $x^n - 1$ are called the ***nth roots of unity***.

Suppose $\mathrm{char}(k) = 0$. Then $f(x) = x^n - 1$ is trivially separable over k.

Suppose $\mathrm{char}(k) = p$. If $p \mid n$, then $n = pm$ and $x^n - 1 = (x^m)^p - 1 = (x^m - 1)^p$. So $x^n - 1 = 0$ if and only if $x^m - 1 = 0$, hence we should assume $p \nmid n$.

In that case, if $p \nmid n$, $f(x) = x^n - 1$ and $f'(x) = nx^{n-1}$ have no common factors (the latter has only 0 as roots, and the former doesn't have 0 as a root), so $\gcd(f(x), f'(x)) = 1$ and $f(x)$ is separable.

From now on, we will therefore assume we are in one of those separable situations.

We will denote by $\mu_n = \mu[n]$ the set of all the nth roots of unity. This is an abelian group of order n, and in fact μ_n is a cyclic group (because it is a finite subgroup of $\overline{k}^\times$).

Let $k_n = k(\mu_n)$ be the splitting field of $x^n - 1$. Then k_n/k is Galois.

Since μ_n is cyclic, let ξ be a primitive nth roots of unity, so that $\mu_n = \langle \xi \rangle$, and $\mathrm{ord}(\xi) = n$. Then $k_n = k(\xi)$.

This raises a natural question: what is $G = \mathrm{Gal}(K_n/k)$?

Certainly $\sigma \in G$ is determined by $\sigma(\xi) = \xi^i$ (since all elements in μ_n look like ξ^i for some i). But we must have $\langle \xi^i \rangle = \langle \xi \rangle = \mu_n$, so we need $\gcd(i, n) = 1$. Hence we have $G \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ by $\sigma \mapsto i$, where $\sigma(\xi) = \xi^i$.

Theorem 21.2.1. *We have* $[\mathbb{Q}(\mu_n) : \mathbb{Q}] = \varphi(n)$ *and* $\mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

Proof. Write $\mu_n = \langle \xi \rangle$. Let $f(x) = \mathrm{Irr}(\xi; \mathbb{Q}, x)$. We can clear the denominator to get $f(x) \in \mathbb{Z}[x]$ (strictly speaking a different f, but redefine it to be so). We claim that $\deg f = \varphi(n)$.

Note how $f(x) \mid x^n - 1$, implying that $x^n - 1 = f(x)h(x)$ for some $h(x) \in \mathbb{Q}[x]$. In fact, by Gauss lemma we can guarantee $h(x) \in \mathbb{Z}[x]$.

Note that since $f(\xi) = 0$, for any prime $p \nmid n$, $f(x^p) = 0$. Otherwise, if $f(x^p) \neq 0$, then

$$0 = (\xi^p)^n - 1 = f(\xi^p)h(\xi^p),$$

where $f(\xi^p) \neq 0$, so $h(\xi^p) = 0$. Hence ξ is a root of $h(x^p)$, meaning that $f(x) \mid h(x^p)$, because $f = \mathrm{Irr}(\xi; \mathbb{Q}, x)$.

Now consider this modulo p, say $\overline{x^n - 1} = \overline{f(x)h(x)}$ in $\mathbb{F}_p$. Now modulo p, $\overline{h(x^p)} = \overline{h(x)}^p$, so $\overline{f(x)} \mid \overline{h(x)}^p$. Thus every root of $\overline{f(x)}$ is a root of $\overline{h(x)}$, so whilst the left-hand side of $\overline{x^n - 1} = \overline{f(x)h(x)}$ is separable (since $p \nmid n$), so it has no repeated roots, the right-hand side does have repeated roots. □

Lecture 22 Cyclotomic Fields

22.1 Proof finished

Proof continued. Similarly, for another prime $q \nmid n$, $(\xi^p)^q = \xi^{pq}$ is a zero of $f(z)$. Hence $\xi^{n'}$ is a zero of $f(x)$ for any n' coprime to n, meaning that $\deg f(x) \geq \varphi(n)$.

On the other hand, $[\mathbb{Q}(\mu_n) : \mathbb{Q}] \leq \varphi(n)$, so together $\deg f(x) = \varphi(n) = [\mathbb{Q}(\mu_n) \colon \mathbb{Q}]$, and so $\mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. (The left-hand side embeds into the right-hand side, and they are of the same order.) □

There is good reason we specified $k = \mathbb{Q}$ in this theorem:

Counterexample 22.1.1. Let $k = \mathbb{R}$, and let ξ be a primitive 5th root of unity, i.e., a root of $x^5 - 1$. Then $\mathrm{Gal}(\mathbb{R}(\xi)/\mathbb{R}) \hookrightarrow (\mathbb{Z}/5\mathbb{Z})^\times$, and $|(\mathbb{Z}/5\mathbb{Z})^\times| = 5$.

However

$$x^5-1 = (x-1)(x^4+x^3+x^2+x+1) = (z-1)\Big(x^2+\frac{1+\sqrt{5}}{2}x+1\Big)\Big(x^2+\frac{1-\sqrt{5}}{2}x+1\Big)$$

over $\mathbb{R}$, so $[\mathbb{R}(\xi) : \mathbb{R}] = |\mathrm{Gal}(\mathbb{R}(\xi)/\mathbb{R})| = 2$. ▲

Counterexample 22.1.2. Let $k = \mathbb{F}_q$, where $q = p^m$ is a prime power. Let ξ be a primitive nth root of unity. Then $K = k(\xi)$ is the splitting field of $x^n - 1$, and $\mathrm{Gal}(K/k) = \langle\sigma\rangle$ where $\sigma \colon a \mapsto a^q$ is the Frobenius automorphism.

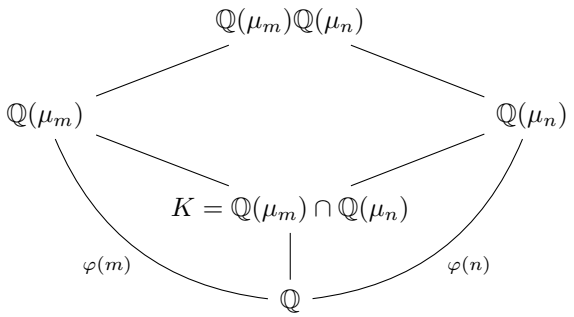
Then $\mathrm{Gal}(K/k) = \langle\sigma\rangle \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ by $\sigma \mapsto q$, so the order of σ is the order of q in $(\mathbb{Z}/n\mathbb{Z})^\times$. But q may or may not be a generator in $(\mathbb{Z}/m\mathbb{Z})^\times$. ▲

Definition 22.1.3. A splitting field K of $x^n - 1 \in k[x]$ is called a ***cyclotomic extension*** of order n, or just a ***cyclotomic field*** if we don't specify the order.

Let us recall some properties of the Euler ϕ function. First, $\varphi(p^n) = p^n - p^{n-1}$ for p prime. Second, if $(m, n) = 1$, then $\varphi(mn) = \varphi(m)\varphi(n)$, i.e., ϕ is multiplicative.

Proposition 22.1.4. *Suppose* $(m, n) = 1$. *Then* $\mathbb{Q}(\mu_m) \cap \mathbb{Q}(\mu_n) = \mathbb{Q}$.

Proof. We have the following situation:



First, notice how $\mathbb{Q}(\mu_m)\mathbb{Q}(\mu_n) = \mathbb{Q}(\mu_m\mu_n) - \mathbb{Q}(\mu_{mn})$. The last step is a consequence of the fact that

$$(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/mn\mathbb{Z})^\times$$

Date: November 5th, 2019.

if $(m,n)=1$. Second, since $\mathbb{Q}(\mu_n)/\mathbb{Q}$ is Galois, so is $\mathbb{Q}(\mu_n)/K$, and we can lift this to $\mathbb{Q}(\mu_{mn})/\mathbb{Q}(\mu_m)$, and $\mathrm{Gal}(\mathbb{Q}(\mu_m)/K) \cong \mathrm{Gal}(\mathbb{Q}(\mu_{mn})/\mathbb{Q}(\mu_n))$. Now

$$|\mathrm{Gal}(\mathbb{Q}(\mu_{mn})/K)| = \frac{\varphi(mn)}{\varphi(n)} = \varphi(m)$$

since $(m,n)=1$. Hence $K=Q$. □

22.2 Quadratic reciprocity

Let p be an odd prime, and let $v \in \mathbb{Z}$ with $(v,p)=1$. Define

$$\left(\frac{v}{p}\right) = \begin{cases} 1, & \text{if there exists } x \in \mathbb{Z} \text{ such that } x^2 \equiv v \pmod p, \\ -1, & \text{otherwise.} \end{cases}$$

If $\left(\frac{v}{p}\right)=1$, then v is called a ***quadratic residue*** modulo p, and if $\left(\frac{v}{p}\right)=-1$, then v is called a ***quadratic nonresidue*** modulo p.

Note how, since $x^2 = (-x)^2$, squaring the numbers $\{1,2,\dots,p-1\} = (\mathbb{Z}/p\mathbb{Z})^\times$, we get exactly half of them back, i.e., exactly $\frac{p-1}{2}$ of them are quadratic residues.

This quadratic symbol has a couple of basic properties:

(*i*) $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$, called the law of quadratic reciprocity;

(*ii*) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$;

(*iii*) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$;

(*iv*) $\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right)$, so it is completely multiplicative; and

(*v*) $\left(\frac{a^2}{p}\right) = \left(\frac{a}{p}\right)^2 = 1$.

22.3 Gauss sums

Let p be an odd prime and let ξ be a primitive pth root of unity (e.g., $\xi = e^{\frac{2\pi i}{p}}$). We define the ***Gauss sum***

$$S \coloneqq \sum_{1 \le v \le p-1} \left(\frac{v}{p}\right)\xi^v.$$

Proposition 22.3.1. *$S^2 = \left(\frac{-1}{p}\right)p$, and hence $S = \pm\sqrt{p}$ or $S = \pm\sqrt{-p}$.*

Proof. The proof is essentially a change of variables. We have

$$\begin{aligned} S^2 &= \Big(\sum_{1\le v\le p-1}\left(\frac{v}{p}\right)\xi^v\Big)\Big(\sum_{1\le u\le p-1}\left(\frac{u}{p}\right)\xi^v\Big) = \sum_{v,u}\left(\frac{uv}{p}\right)\xi^{v+u} \\ &= \sum_u\Big(\sum_v\left(\frac{uv}{p}\right)\xi^{v+u}\Big). \end{aligned}$$

Notice how, since $u \neq 0$, uv just permutes v modulo p, so making the change of variables $v \mapsto uv$ we don't change the sum, so

$$S^2 = \sum_u \Big(\sum_v \left(\frac{u^2 v}{p}\right) \xi^{vu+u} \Big) = \sum_u \Big(\sum_v \left(\frac{v}{p}\right) \xi^{(v+1)u} \Big).$$

We split this sum into two parts, one where $v = -1 = p-1$, and one where $v \neq -1$. So

$$S^2 = \left(\frac{-1}{p}\right)(p-1) + \sum_u \sum_{v \neq -1} \left(\frac{v}{p}\right) \xi^{(v+1)u}.$$

Let us focus on the second sum for a moment. Changing the order of summation,

$$\sum_u \sum_{v \neq -1} \left(\frac{v}{p}\right) \xi^{(v+1)u} = \sum_{v \neq -1} \left(\frac{v}{p}\right) \sum_{1 \leq u \leq p-1} \xi^{(v+1)u},$$

where again $v+1 \neq 0$ on the inside, so the inside sum is just

$$\sum_u \xi^u = \xi + \xi^2 + \ldots + \xi^{p-1} = -1,$$

whence, putting this back,

$$S^2 = \left(\frac{-1}{p}\right)(p-1) - \sum_{v \neq -1} \left(\frac{v}{p}\right) = \left(\frac{-1}{p}\right) p - \sum_v \left(\frac{v}{p}\right) = \left(\frac{-1}{p}\right) p. \qquad \square$$

Remark 22.3.2. Gauss proved that

$$S = \begin{cases} \sqrt{p}, & \text{if } p \equiv 1 \pmod 4 \\ \sqrt{-p}, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

We will not prove that here, because we don't need it.

Example 22.3.3. We have, for instance, for $p = 3$

$$S = \xi - \xi^2,$$

where $\xi = e^{\frac{2\pi i}{3}}$, and if $p = 7$, take $\xi = e^{\frac{2\pi i}{7}}$ and we have

$$S = \xi + \xi^2 - \xi^3 + \xi^4 - \xi^5 - \xi^6. \qquad \blacktriangle$$

Theorem 22.3.4. *Let K be a field such that $[K : \mathbb{Q}] = 2$ (i.e., K is a quadratic extension of $\mathbb{Q}$). Then there exists some m such that $K \subset \mathbb{Q}(\mu_m) = \mathbb{Q}(e^{\frac{2\pi i}{m}})$.*

In other words, every quadratic extension of $\mathbb{Q}$ is contained in a cyclotomic extension.

Something more general, but much harder to prove, is true:

Theorem 22.3.5 (Kronecker–Weber)**.** *Let $K/\mathbb{Q}$ be an abelian extension. Then there exists an m such that $K \subset \mathbb{Q}(\mu_m)$.*

Lecture 23 Characters

23.1 Cyclotomic extensions

Let us start by proving Theorem 22.3.4 from last lecture.

Proof. We have a degree two extension $K/\mathbb{Q}$, which, being finite and since $\mathrm{char}(\mathbb{Q}) = 0$, must be simple according to the Primitive element theorem. Ergo, $K = \mathbb{Q}(\alpha)$ for some α, and α is the root of a second degree polynomial.

By completing the square we can make a change of variable and assume the polynomial looks like $x^2 + 1$, and by clearing denominators we can moreover assume $a \in \mathbb{Z}$. Therefore $\mathbb{Q}(\sqrt{a})$.

We can also assume a is square free, since otherwise we would just factor them out, so $a = p_1 p_2 \cdots p_r$ or $a = -p_1 p_2 \cdots p_r$, where p_i are distinct primes.

Consequently $\sqrt{a} = \sqrt{p_1}\sqrt{p_2}\cdots\sqrt{p_r}$ or $\sqrt{a} = \sqrt{-1}\sqrt{p_1}\sqrt{p_2}\cdots\sqrt{p_r}$.

Recall how if p is an odd prime,

$$S = \sum_{v=1}^{p-1} \left(\frac{v}{p}\right) \xi^v,$$

with $\xi = e^{\frac{2\pi i}{p}} \in \mathbb{Q}(\mu_p)$, then $S = \pm\sqrt{p} \in \mathbb{Q}(\mu_p)$ or $S = \pm\sqrt{-1}\sqrt{p} \in \mathbb{Q}(\mu_p)$.

Also, $\mathbb{Q}(\mu_4) = \mathbb{Q}(e^{\frac{2\pi i}{4}}) = \mathbb{Q}(\sqrt{-1})$, so $\sqrt{-1} \in \mathbb{Q}(\mu_4)$.

Moreover, for the prime $p = 2$, we have $\mathbb{Q}(\mu_8) = \mathbb{Q}(e^{\frac{2\pi i}{8}})$, whence $e^{\frac{2\pi i}{8}} = \frac{(1+i)\sqrt{2}}{2} \in \mathbb{Q}(\mu_8)$, and by the reflexive property $\frac{(1-i)\sqrt{2}}{2} \in \mathbb{Q}(\mu_8)$. Hence their sum is in $\mathbb{Q}(\mu_8)$, so $\sqrt{2} \in \mathbb{Q}(\mu_8)$.

Now remember that, if $(m, n) = 1$, then $\mathbb{Q}(\mu_m \mu_n) = \mathbb{Q}(\mu_{mn})$.

So if all p_i in a are odd, then

$$K \subset \mathbb{Q}(\mu_4 \mu_{p_1} \cdots \mu_{p_r}) = \mathbb{Q}(\mu_{4|a|}),$$

and if $p_1 = 2$, then

$$K \subset \mathbb{Q}(\mu_8 \mu_{p_2} \cdots \mu_{p_r}) = \mathbb{Q}(\mu_{4|a|}),$$

so in both cases $K \subset \mathbb{Q}(\mu_{4|a|})$. □

We will not prove the more general Kronecker–Weber theorem here, for it requires local class field theory, which we will not discuss.

Definition 23.1.1. Let

$$\Phi_n(x) = \prod_{i=1}^{\varphi(n)} (x - \xi_i),$$

where $\{\, \xi_i \mid i = 1, 2, \ldots, \varphi(n) \,\}$ is the set of all primitive nth roots of unity. Then by our proof of the fact that $\mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ it follows that $\Phi_n(x) \in \mathbb{Q}[x]$ is irreducible, and clearly $\deg \Phi_n = \varphi(n)$.

This polynomial $\Phi_n(x)$ is called the nth ***cyclotomic polynomial***.

Date: November 7th, 2019.

Since $x^n - 1$ has as its roots all nth roots of unity, not just the primitive ones, we must have

$$x^n - 1 = \prod_{d|n} \Phi_d(x),$$

and consequently

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{\substack{d|n \\ d \neq n}} \Phi_d(x)}$$

For instance, $\Phi_1(x) = x - 1$ and $\Phi_2(x) = x + 1$. Next

$$\Phi_3(x) = \frac{x^3 - 1}{x - 1} = x^2 + x + 1,$$

and

$$\Phi_4(x) = \frac{x^4 - 1}{(x - 1)(x + 1)} = x^2 + 1.$$

Since $p = 5$ is a prime, we see simply how

$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1,$$

but more interestingly, for instance,

$$\Phi_6(x) = x^2 - x + 1$$

and

$$\Phi_{12}(x) = x^4 - x^2 + 1.$$

23.2 Classical Galois results

A classical question in Galois theory is this: can we find a Galois extension of $\mathbb{Q}$ with corresponding Galois group S_n?

Below are two answers.

First, by Schur, let

$$E_n(x) = 1 + x + \frac{x^2}{2!} + \cdots + \frac{x^n}{n!} \in \mathbb{Q}[x].$$

Then $\deg E_n = n$ and

$$\mathrm{Gal}(E_n) = \begin{cases} A_n, & \text{if } n \equiv 0 \pmod 4, \\ S_n, & \text{otherwise.} \end{cases}$$

Another answer: let

$$H_m(x) = (-1)^m e^{\frac{x^2}{2}} \frac{d^m}{dx^m}\left(e^{-\frac{x^2}{2}}\right) \in \mathbb{Q}[x]$$

be the mth ***Hermite polynomial***. Then $H_m(x)$ is even if m is even, and odd if m is odd, and therefore we can write

$$H_{2n}(x) = K_n^{(0)}(x^2)$$

and

$$H_{2n+1}(x) = xK_n^{(1)}(x^2).$$

Then $\mathrm{Gal}(K_n^{(i)}) \cong S_n$ for $i = 0, 1$ and all $n > 12$.

23.3 Characters

Definition 23.3.1. Let G be a monoid[1] and let K be a field. A homomorphism $\varphi\colon G \to K^\times$ is called a ***character*** of G to K.

Very often we will just take G to be a group.

Theorem 23.3.2 (Artin)**.** *Let G be a monoid and K a field. Let $\chi_1, \chi_2, \ldots, \chi_n$ be distinct characters of G to K. Then $\{ \chi_1, \chi_2, \ldots, \chi_n \}$ is linearly independent over K.*

Proof. Suppose the set $\{ \chi_1, \chi_2, \ldots, \chi_n \}$ is linearly dependent. Then

$$a_1\chi_1 + a_2\chi_2 + \cdots + a_m\chi_m = 0$$

for some $a_i \in K$, $a_i \neq 0$. In particular, take m to be the smallest such number, i.e., we have the smallest nontrivial set of linearly dependent characters.

Since $\chi_1 \neq \chi_2$, there exists some $z \in G$ so that $\chi_1(z) \neq \chi_2(z)$, and consequently consider the system

$$\begin{aligned} a_1\chi_1 + a_2\chi_2 + \cdots + a_m\chi_m &= 0 \\ a_1\chi_1(z)\chi_1 + a_2\chi_2(z)\chi_2 + \cdots + a_m\chi_m(z)\chi_m &= 0. \end{aligned}$$

Taking $\chi_1(z)$ times the first equation and subtracting the second, we get

$$a_2(\chi_1(z) - \chi_2(z))\chi_2 + \cdots + a_m(\chi_1(z) - \chi_m(z))\chi_m = 0,$$

but $\chi_1(z) - \chi_2(z) \neq 0$, so we have produced a smaller linearly dependent set, which contradicts the minimality of m. □

Lecture 24 Norms and Traces

First let us state a simple consequence of Artin's theorem from last time:

Corollary 24.0.1. *Let E/k be separable of degree n. Let $\{ \sigma_1, \sigma_2, \ldots, \sigma_n \}$ be distinct k-embeddings of E into $\overline{k}$. Then $\{ \sigma_1, \sigma_2, \ldots, \sigma_n \}$ is a linearly independent set.*

Proof. Just consider $\sigma_i\colon E^\times \to \overline{k}^\times$, which is a character. □

24.1 Field norms and field traces

Definition 24.1.1. Let E/k be a separable extension of degree n. Let $\{ \sigma_1, \sigma_2, \ldots, \sigma_n \}$ be the set of all k-embeddings of E into $\overline{k}$.

For $\alpha \in E$, we define the ***(field) normnorm*** of α as

$$\mathrm{N}_{E/k}(\alpha) = \sigma_1(\alpha)\sigma_2(\alpha)\cdots\sigma_n(\alpha)$$

and the ***(field) trace***

$$\mathrm{Tr}_{E/k}(\alpha) = \sigma_1(\alpha) + \sigma_2(\alpha) + \cdots + \sigma_n(\alpha).$$

When there is no risk of ambiguity we will omit the subscript and just write N and Tr.

[1] Meaning a semigroup with identity, i.e., a group but elements do not necessarily have inverses.

Date: November 12th, 2019.

Remark 24.1.2. Both $\mathrm{N}_{E/k}(\alpha)$ and $\mathrm{Tr}_{E/k}(\alpha)$ are in k. To see this, notice how applying any σ to either of them just permutes the terms, so they are fixed by all σ.

Now suppose there exists some $\alpha \in E$, fixed by all σ, but not in k. Then σ must send α to another root of $\mathrm{Irr}(\alpha; k, x)$, but $\sigma(\alpha) = \alpha$, so $k(\alpha)$ would be purely inseparable, which is a contradiction to E/k being separable.

Remark 24.1.3. Suppose $E \supset F \supset k$. Then we can compute norms over the large extension piecewise,

$$\mathrm{N}_{E/k}(\alpha) = \mathrm{N}_{F/k}(\mathrm{N}_{E/F}(\alpha)),$$

and likewise

$$\mathrm{Tr}_{E/k}(\alpha) = \mathrm{Tr}_{F/k}(\mathrm{Tr}_{E/F}(\alpha)).$$

Example 24.1.4. Suppose $E = k(\alpha)$ is a simple extension of k. Write

$$f(x) = \mathrm{Irr}(\alpha; k, x) = x^n + a_1 x^{n-1} + \cdots + a_n,$$

which in $\overline{k}[x]$ factors as

$$f(x) = (x - \sigma_1(\alpha))(x - \sigma_2(\alpha)) \cdots (x - \sigma_n(\alpha)).$$

Hence $\mathrm{N}_{E/k}(\alpha) = (-1)^n a_n$ and $\mathrm{Tr}_{E/k}(\alpha) = -a_1$. ▲

Example 24.1.5. Let E be a separable extension of k and let $\beta \in E$. Then there is a subfield $F = k(\beta)$ between k and E, and by the above example we understand the norm of β on F/k. Specifically, let

$$f(x) = \mathrm{Irr}(\beta; k, x) = x^m + a_1 x^{m-1} + \cdots + a_m,$$

and so $\mathrm{N}_{F/k}(\beta) = (-1)^m a_m$. Then

$$\mathrm{N}_{E/k}(\beta) = \mathrm{N}_{F/k}(\mathrm{N}_{E/F}(\beta)),$$

but $\beta \in F$, so all F-embeddings fix is, meaning that $\mathrm{N}_{E/F}(\beta) = \beta^{[E:F]}$. Hence

$$\mathrm{N}_{E/k}(\beta) = \mathrm{N}_{F/k}(\beta^{[E:F]}) = \mathrm{N}_{F/k}(\beta)^{[E:F]} = ((-1)^m a_m)^{[E:F]}.$$

Similarly,

$$\begin{aligned} \mathrm{Tr}_{E/k}(\beta) &= \mathrm{Tr}_{F/k}(\mathrm{Tr}_{E/F}(\beta)) = \mathrm{Tr}_{F/k}([E:F] \cdot \beta) \\ &= [E:F] \,\mathrm{Tr}_{F/k}(\beta) = -[E:F] a_1. \end{aligned}$$ ▲

Remark 24.1.6. In the above we have used the following properties:

(*i*) $\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\,\mathrm{N}(\beta)$, i.e., the norm is multiplicative, since the σ involved are homomorphisms, and hence also multiplicative.

Similarly, $\mathrm{Tr}(\alpha + \beta) = \mathrm{Tr}(\alpha) + \mathrm{Tr}(\beta)$ is additive, for the same reason.

(*ii*) In particular, $\mathrm{N}_{E/k}(a \cdot \alpha) = a^n \,\mathrm{N}_{E/k}(\alpha)$ for $a \in k$, if $[E:k] = n$.

Similarly, $\mathrm{Tr}_{E/k}(a \cdot \alpha) = a \,\mathrm{Tr}_{E/k}(\alpha)$. Hence trace is a k-linear map.

Theorem 24.1.7. *Define a k-bilinear form $\langle \cdot, \cdot \rangle \colon E \times E \to k$ by $\langle x, y \rangle = \mathrm{Tr}_{E/k}(xy)$. Then this bilinear form is* **non-degenerate**[2]*. Hence E and its dual space $E^* = \mathrm{Hom}_k(E, k)$ are identified.*

Proof. Suppose $\langle \cdot, \cdot \rangle$ is degenerate, i.e., there exists some $x \neq 0$ such that $\langle x, y \rangle = 0$ for all $y \in E$. That is, $\mathrm{Tr}_{E/k}(xy) = 0$ for all $y \in E$, so $\mathrm{Tr}_{E/k}(xE) = 0$, meaning that $\mathrm{Tr}_{E/k}(E) = 0$.

This means that we have

$$\sigma_1(x) + \sigma_2(x) + \cdots + \sigma_n(x) = 0$$

for all $x \in E$, but this implies $\left\{ \sigma_1, \sigma_2, \ldots, \sigma_n \right\}$ is a linearly dependent set, which contradicts Artin's theorem.

Hence $\langle \cdot, \cdot \rangle$ is non-degenerate, and therefore the map $E \to E^*$ defined by $x \mapsto \phi_x$, with $\phi_x(y) = \langle x, y \rangle = \mathrm{Tr}_{E/k}(xy)$ is one-to-one.

But these are finite dimensional vector spaces (over k), so one-to-one implies onto, so this is an isomorphism. □

Definition 24.1.8. Let E/k be separable of degree n. Let $\left\{ w_1, w_2, \ldots, w_n \right\}$ be a basis of E/k (as a vector space). Then $\left\{ w_1', w_2', \ldots, w_n' \right\}$ is called the ***dual basis*** of $\left\{ w_1, w_2, \ldots, w_n \right\}$ if $(w_i', w_j) = \delta_{ij}$, where

$$\delta_{ij} = \begin{cases} 1, & \text{if } i = j, \\ 0, & \text{if } i \neq j. \end{cases}$$

Here we use w_i' to also correspond to an element $\langle w_i', \cdot \rangle$ in the dual space.

Theorem 24.1.9. *Let E/k be separable of degree n. Let $\alpha \in E$ so that $E = k(\alpha)$ (note how E/k is finite and separable, so by the Primitive element theorem this is possible). Let $f(x) = \mathrm{Irr}(\alpha; k, x)$, and let $\left\{ \alpha_1, \alpha_2, \ldots, \alpha_n \right\}$ be the distinct roots of $f(x)$.*

Then $\left\{ 1, \alpha, \alpha^2, \ldots, \alpha^{n-1} \right\}$ is a basis of E/k and its dual basis is given by $\left\{ \delta_0, \delta_1, \ldots, \delta_{n-1} \right\}$ where

$$\delta_i = \frac{\beta_i}{f'(\alpha)}$$

for $i = 0, 1, 2, \ldots, n-1$, and β_i are the coefficients of

$$\frac{f(x)}{x - \alpha} = \beta_{n-1} x^{n-1} + \beta_{n-2} x^{n-2} + \cdots + \beta_0 \in E[x].$$

To prove this we need the following lemma:

Lemma 24.1.10 (Lagrange interpolation theorem)**.** *With the same assumptions as in the previous theorem, we have for any $0 \leq r \leq n-1$*

$$\sum_{i=1}^{n} \frac{f(x)}{x - \alpha_i} \frac{\alpha_i^r}{f'(\alpha_i)} = x^r.$$

[2]That is, for $x \in E$, $\langle x, y \rangle = 0$ for all $y \in E$ if and only if $x = 0$.

Proof. We have $f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$. Then by the product rule

$$f'(\alpha_i) = \prod_{j\neq i}(\alpha_i - \alpha_j).$$

Consider

$$g(x) = x^r - \sum_{i=1}^{n} \frac{f(x)}{x-\alpha_i}\frac{\alpha_i^r}{f'(\alpha_i)}.$$

This is a polynomial of degree at most $n-1$.

But on the other hand, if we plug α_k into g, only the $i=k$ term in the sum survives, and

$$g(\alpha_k) = \alpha_k^r - \prod_{j\neq k}(\alpha_k - \alpha_j)\frac{\alpha_k^r}{f'(\alpha_k)} = 0$$

for $k = 1, 2, \ldots, n$. So it has more zeros than its degree, meaning that $g = 0$. □

With this we are ready to prove the theorem:

Proof of Theorem 24.1.9. Notice first how the terms

$$\frac{f(x)}{x-\alpha_i}\frac{\alpha_i^r}{f'(\alpha_i)}$$

for $i = 1, 2, \ldots, n$ are all conjugates of one another, since our embeddings send α_i to other α_j. Hence the sum in the previous lemma is

$$\mathrm{Tr}_{E/k}\Big(\frac{f(x)}{x-\alpha}\frac{\alpha^r}{f'(\alpha)}\Big) = x^r,$$

where by taking the trace of a polynomial we mean apply the trace to the coefficients.

Hence, since $\frac{f(x)}{x-\alpha} = \beta_{n-1}x^{n-1} + \cdots + \beta_0$, we have

$$\mathrm{Tr}_{E/k}\Big((\beta_{n-1}x^{n-1} + \cdots + \beta_0)\frac{\alpha^r}{f'(\alpha)}\Big) = x^r.$$

Comparing coefficients here, we see that the x^ith coefficient of the left-hand side is

$$\mathrm{Tr}_{E/k}\Big(\beta_i\frac{\alpha^r}{f'(\alpha)}\Big) = \mathrm{Tr}_{E/k}(\delta_i\alpha^r) = \delta_{ir},$$

so $\mathrm{Tr}_{E/k}(\delta_i\alpha^r) = \langle\delta_i, \alpha^r, =\rangle\delta_{ir}$, so we have a dual basis $\langle\delta_i, \cdot\rangle$. □

24.2 Galois theory of solvability of algebraic equations

Theorem 24.2.1 (Hilbert's theorem 90)**.** *Let K/k be a cyclic extension of degree n. Let $\beta \in K$. Then $\mathrm{N}(\beta) = 1$ if and only if there exists some $\alpha \in K$ such that $\beta = \frac{\alpha}{\sigma(\alpha)}$, where $\mathrm{Gal}(K/k) = \langle\sigma\rangle$.*

Proof. The converse direction is trivial. Suppose $\beta = \frac{\alpha}{\sigma(\alpha)}$. Then

$$\mathrm{N}(\beta) = \mathrm{N}\Big(\frac{\alpha}{\sigma(\alpha)}\Big) = \frac{\mathrm{N}(\alpha)}{\mathrm{N}(\sigma(\alpha)} = \frac{\mathrm{N}(\alpha)}{\mathrm{N}(\alpha)} = 1$$

since $\sigma(\alpha)$ just permutes the terms in the norm of α.

For the forward direction we need to be much more careful. We will use the notation $\sigma(\alpha) = \alpha^\sigma$. By Artin's theorem, $\left\{ 1 = \sigma^0, \sigma, \sigma^2, \dots, \sigma^{n-1} \right\}$ is a linearly independent set. Therefore

$$\beta^0\sigma^0 + \beta\sigma + \beta^{1+\sigma}\sigma^2 + \beta^{1+\sigma+\sigma^2}\sigma^3 + \cdots + \beta^{1+\sigma+\sigma^2+\cdots+\sigma^{n-2}}\sigma^{n-1}$$

is a non-zero map. In the $\sigma(\beta) = \beta^\sigma$ notation, note how this means, for example,

$$\beta^{1+\sigma} = \beta^1\beta^\sigma = \beta\sigma(\beta)$$

and

$$\beta^{1+\sigma+\sigma^2} = \beta^1\beta^\sigma\beta^{\sigma^2} = \beta\sigma(\beta)\sigma^2(\beta).$$

This being a non-zero map, there must exists some $\theta \in K$ such that, when evaluating at θ, we get

$$\alpha \coloneqq \theta + \beta\theta^\sigma + \beta^{1+\sigma}\theta^{\sigma^2} + \cdots + \beta^{1+\sigma+\cdots+\sigma^{n-2}}\theta^{\sigma^{n-1}} \neq 0.$$

Apply σ and multiply by β and we get

$$\beta\alpha^\sigma = \beta\left(\theta^\sigma + \beta^\sigma\theta^{\sigma^2} + \beta^{\sigma+\sigma^2}\theta^{\sigma^3} + \cdots + \beta^{\sigma+\sigma^2+\cdots+\sigma^{n-1}}\theta^{\sigma^n}\right).$$

Note two things: first, $\sigma^n = \mathrm{Id}$, so $\theta^{\sigma^n} = \theta$. Second, multiplying through by β the last term becomes

$$\beta\beta^{\sigma+\sigma^2+\cdots+\sigma^{n-1}} = \beta^{1+\sigma+\sigma^2+\cdots+\sigma^{n-1}} = \mathrm{N}(\beta) = 1.$$

Hence the above is nothing but

$$\theta + \beta\theta^\sigma + \beta^{1+\sigma}\theta^{\sigma^2} + \cdots + \beta^{1+\sigma+\cdots+\sigma^{n-2}}\theta^{\sigma^{n-1}} = \alpha,$$

so $\beta\alpha^\sigma = \alpha$, and we are done. □

Lecture 25 Radical Extensions

25.1 Kummer extensions

From now on out, until the end of these notes, we will assume extensions are separable unless otherwise stated.

Theorem 25.1.1 (Kummer extensions)**.** *Assume k contains a primitive nth root of unity.*

(*i*) *Let K/k be a cyclic extension of degree n. Then there exists some $\alpha \in K$ such that $K = k(\alpha)$ and $\mathrm{Irr}(\alpha; k, x) = x^n - a \in k[x]$. In particular, $\alpha^n = a \in k$.*

(*ii*) *Let α be a root of $f(x) = x^n - a \in k[x]$. Then $k(\alpha)/k$ is a cyclic extension of degree d with $d \mid n$, and $\alpha^d = b \in k$, with $\mathrm{Irr}(\alpha; k, x) = x^d - b$.*

Date: November 14th, 2019.

This theorem therefore classifies cyclic extensions of degree n if the base field k contains a primitive nth root of unity.

Proof. (i) Let ξ be a primitive nth root of unity, which is in k by assumption. Then

$$\mathrm{N}_{K/k}(\xi^{-1}) = (\xi^{-1})^n = \frac{1}{\xi^n} = 1$$

since $\xi \in k$, and hence $\xi^{-1} \in k$, means its norm is just itself to the power $n = [K : k]$. By Hilbert 90 this means that there exists some $\alpha \in K$ so that

$$\frac{1}{\xi} = \frac{\alpha}{\sigma(\alpha)}$$

where $\mathrm{Gal}(K/k) = \langle\sigma\rangle$, which is cyclic by assumption. Therefore $\sigma(\alpha) = \alpha\xi$.

Notice how $\sigma^2(\alpha) = \sigma(\alpha\xi) = \sigma(\alpha)\xi = \alpha\xi^2$, and in general $\sigma^i(\alpha) = \alpha\xi^i$ for $i = 0, 1, \ldots, n-1$, which are all distinct since ξ is a primitive nth root of unity.

Hence

$$f(x) = \mathrm{Irr}(\alpha; k, x) = (x - \alpha)(x - \sigma(\alpha)) \cdots (x - \sigma^{n-1}(\alpha)),$$

which is of degree n, and therefore $K = k(\alpha)$ since $K \supset k(\alpha)$ and both are degree n extensions of k.

To show that $f(x) = \mathrm{Irr}(\alpha; k, x) = x^n - 1$, we will show that $\alpha^n = a \in k$, so that $f(x) \mid x^n - a$. Since they are of the same degree, this means they are equal.

So let $a = \alpha^n$. To show $a \in k$ is suffices to show that $\sigma(a) = a$, since this means it is fixed by the entire Galois group. Now

$$\sigma(a) = \sigma(\alpha^n) = (\alpha\xi)^n = \alpha^n\xi^n = \alpha^n = a$$

where $\xi^n = 1$ since it is a (primitive) nth root of unity. Hence $f(x) = x^n - a$.

(ii) Since α is a root of $x^n - a$, we know that $\mathrm{Irr}(\alpha; k, x) \mid x^n - a$. Moreover, we know that

$$x^n - a = \prod_{i=0}^{n-1} (x - \alpha\xi^i).$$

Since $\xi \in k$ means $\xi^i \in k$, the field $k(\alpha)$ is a splitting field of both $\mathrm{Irr}(\alpha; k, x)$ and $x^n - a$. Hence $k(\alpha)/k$ is Galois, and so let $H = \mathrm{Gal}(k(\alpha)/k)$.

For $\tau \in H$, we we have $\tau(\alpha) = \alpha\omega_\tau$, where

$$\omega_\tau \in \langle\xi\rangle = Set1, \xi, \xi^2, \ldots, \xi^{n-1} \cong \mathbb{Z}/n\mathbb{Z}.$$

Define $\phi\colon H \to \langle\xi\rangle \cong \mathbb{Z}/n\mathbb{Z}$ by $\phi\colon \tau \mapsto \omega_\tau$. Then ϕ is one-to-one, so H is a subgroup of $\mathbb{Z}/n\mathbb{Z}$, and consequently H is cyclic, making $k(\alpha)/k$ a cyclic extension. Moreover if $|H| = d$, we must have $d \mid n$ because H is a subgroup of $\mathbb{Z}/n\mathbb{Z}$, which is of order n.

Finally, $\mathrm{Irr}(\alpha; k, x)$ has degree d. Let $b = \alpha^d$. Then

$$\tau(b) = \tau(\alpha^d) = \tau(\alpha)^d = (\alpha\omega_\tau)^d = \alpha^d\omega_\tau^d = \alpha^d = b,$$

so $b \in k$. Hence, as above, $\mathrm{Irr}(\alpha; k, x) = x^d - b$. □

To study the same question—that of classifying cyclic extensions of degree n—when the base field k does not contain any primitive nth roots of unity is much harder, and to do this we need Galois cohomology to do Kummer theory.

25.2 Radical extensions

Definition 25.2.1. We call E/k a ***radical extension (of height** 1**)*** if

(*i*) $E = k(\alpha)$ for some $\alpha \in E$ and $\alpha^p \in k$ with p prime; and

(*ii*) $\alpha^p \neq \beta^p$ for all $\beta \in k$. In particular, $\alpha \notin k$, so E is a proper extension.

Example 25.2.2. Let $k = \mathbb{Q}$, $\alpha = e^{\frac{2\pi i}{p}}$, a primitive pth root of unity, and consider $E = \mathbb{Q}(\alpha)$. Notice how $\alpha^p = 1 = 1^p \in \mathbb{Q}$, and $1 \in \mathbb{Q}$. Does this mean E is not a radical extension? We can't tell—there is not sufficient information here. It is possible that $E = \mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$ for some other generator β which does satisfy the conditions.

For example, take $p = 3$ and $\omega = \frac{-1+\sqrt{-3}}{2}$, and consider $\mathbb{Q}(\omega)/\mathbb{Q}$. Here $\omega^3 = 1 \in \mathbb{Q}$, so we are in the above situation. However $\mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{-3})$, so taking $\alpha = \sqrt{-3}$ we have $\omega^2 = -3 \neq \beta^2$ for any $\beta \in \mathbb{Q}$. So $\mathbb{Q}(\omega)/\mathbb{Q}$ is a radical extension. ▲

All by way of saying: it is difficult to determine if an extension is radical. In particular, note that the first part of the definition is generally not too hard to check—if $\alpha^p \in k$—but the second part is. That is, checking whether α^p is a pth power of something in the base field k.

There are special situations where we don't have to check this:

Example 25.2.3. Let p be a prime. Then $x^p - a \in k[x]$ is irreducible if $a \notin k^p$. Hence assume it is irreducible.

Let $\alpha \in \overline{k}$ so that $\alpha^p = a$, i.e., α is a root of $x^p - a$. Let $E = k(\alpha)$. Then $[E : k] = p$ (which, for the record, means there are no intermediate subfields, the degree being prime).

Let θ be a primitive pth root of unity in $\overline{k}$. Then

$$x^p - a = (x - \alpha)(x - \alpha\theta) \cdots (x - \alpha\theta^{p-1}).$$

Note how $\alpha\theta^i \notin k$ for $i = 0, 1, \ldots, p-1$ since $x^p - a$ is irreducible.

Assume $\theta \in k$. Then if $\alpha^p = \beta^p$ for some $\beta \in k$, we must have $(\alpha\beta^{-1})^p = 1$, so $\alpha\beta^{-1}$ is a pth root of unity. Hence $\alpha\beta^{-1} = \theta^i$ for some i, meaning that $\alpha = \beta\theta^i \in k$, contradicting $\alpha \notin k$. ▲

So if the base field contains a primitive pth root of unity, then we don't have to check the harder part—we have $\alpha^p \neq \beta^p$ for all $\beta \in k$ automatically.

Remark 25.2.4. If the prime p is replaced by an integer n, then $x^n - a$, $a \notin k^n$, need not be irreducible, so we cannot apply this argument.

Definition 25.2.5. We say that E/k is a ***radical extension (of height** s**)*** if there exists a chain

$$k = E_0 \subset E_1 \subset R_2 \subset \cdots \subset E_s = E$$

such that each E_i/E_{i-1}, for $i = 1, 2, \ldots, s$, is a radical extension fo height 1 with respect to some prime p_i. So $[E : k] = p_1 p_2 \cdots p_s$.

The situation looks like

$$\begin{array}{c} E = E_s = E_{s-1}(\alpha_s) \\ \Big| \\ \vdots \\ \Big| \\ E_2 = E_1(\alpha_2) \\ \Big| p_2 \\ E_1 = E_0(\alpha_1) \\ \Big| p_1 \\ k = E_0 \end{array}$$

where at each step there are no intermediate subfields, though it is possible there are other subfields between E and k not in the tower.

Example 25.2.6. Consider $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$. This is a rational extension, but of height 2. Consider $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$.

The first extension is radical, since $\sqrt{2}^2 = 2 \in \mathbb{Q}$ and $\mathbb{Q}$ contains a primitive 2nd root of unity (namely -1), and $\sqrt{2} \notin \mathbb{Q}$. For the same reason, the second extension is radical since $\sqrt[4]{2}^2 = \sqrt{2}$. ▲

Remark 25.2.7. Let E/k be a radical extension and let F be an intermediate subfield, i.e., $E \supset F \supset k$. Then E/F is radical, but in general F/k need not be.

To see that E/F is radical, consider the tower for E/k above, where at each stage we adjoin an α_i.

Now adjoining the same elements to form a tower over F, so $F \subset F(\alpha_1) \subset F(\alpha_1, \alpha_2) \subset \cdots \subset E$, we see that E/F is radical.

On the other hand, if both E/F and F/k are radical, then E/k is radical—just combine the two chains.

Remark 25.2.8. Composites of radical extensions are not radical in general.

For example, consider $k = \mathbb{Q}$, $E_1 = \mathbb{Q}(\sqrt[7]{2})$, and $E_2 = \mathbb{Q}(\sqrt{7}2e^{\frac{2\pi i}{7}})$. Then $E_1/\mathbb{Q}$ and $E_2/\mathbb{Q}$ are both radical, but $E_1E_2/\mathbb{Q}$ is not.

Lecture 26 Solvability by Radicals

26.1 Solvable groups

Definition 26.1.1. Let $f(x) \in k[x]$. We say that f is ***solvable by radicals*** if there exists a radical extension E/k such that f splits in $E[x]$.

(So in other words, f splits in $E[x]$ and everything in E, hence including the roots of f, can be written as radical expressions of things in k.)

Remark 26.1.2. A polynomial f being solvable by radicals does *not* mean the splitting field of f over k is radical—its splitting field is just contained in some radical extension of k.

Date: November 19th, 2019.

Remark 26.1.3. In fact, every root of $f(x)$ is contained in a radical extension of k if and only if f is solvable by radicals, i.e., all roots are contained in one radical extension of k.

Theorem 26.1.4. *Let E/k be an extension such that there exists $u \in E$ with $u^n \in k$ and $E = k(u)$ for some n. Assume k contains a primitive nth root of unity. Then E/k is a radical extension (of some height).*

Remark 26.1.5. For convenience, we say k/k is radical of height 0.

Proof. We use induction on n. If $n = 1$, then $E = k$ and we are done.

Suppose $n > 1$, and write $n = p_1 p_2 \cdots p_r$ where p_i are primes, not necessarily distinct. Write $n = p_1 \cdot n_1$ and set $u_1 = u^{p_1}$. So $u_1^{n_1} = u^{p_1 n_1} = u^n \in k$, and k contains a primitive n_1th root of unity since $n_1 \mid n$.

By the induction hypothesis, $E_1 = k(u_1)/k$ is radical. Now $u^{p_1} = u_1 \in E_1$, E_1 contains a primitive p_1th root of unity, and $p_1 < n$ so $E = E_1(u)/E_1$ is radical by the induction hypothesis.

Putting these together, E/k is radical as well. □

Recall how, in general, compositions of radical extensions are not radical. In special cases, they might be:

Proposition 26.1.6. *Suppose E_1/k and E_2/k are radical. Assume k contains sufficiently many roots of unity. Then E_1E_2/k is radical.*

Proof. By assumption E_1/k is radical. If we can show that E_1E_2/E_1 is radical, we are done. Since E_2/k is radical, there exists a chain $k \subset k(u_1) \subset k(u_1, u_2) \subset \cdots \subset k(u_1, u_2, \ldots, u_n) = E_2$, where each step is radical for some prime p_i.

Then certainly we have a chain

$$E_1 \subset E_1(u_1) \subset E_1(u_1, u_2) \subset \cdots \subset E_1(u_1, u_2, \ldots, u_n) = E_1E_2.$$

We need to show that each step in this new chain is radical. This is the case if, at each step, E_i contains an p_ith root of unity, by the last theorem. Hence if k itself contains all those p_ith roots of unity, the composition is indeed radical. □

Recall that a group G is ***solvable*** if there exists

$$G = G_0 > G_1 > G_2 > \cdots > G_s = \{ 1 \}$$

such that G_i is normal in G_{i-1} and G_{i-1}/G_i is abelian.

Note how if G is a finite group, we can refine the sequence $\{ G_i \}$ such that G_{i-1}/G_i is cyclic (by the Fundamental theorem of finitely abelian groups, essentially).

Proposition 26.1.7. (*i*) *Every homomorphic image and subgroup of a solvable group is solvable (because homomorphisms send normal subgroups to normal subgroups, and abelian subgroups to abelian subgroups).*

(*ii*) *G is solvable if and only if G/N and N are solvable for some normal subgroup $N \subset G$.*

Consider a tower of extensions $E \supset F \supset k$, where E/F and F/k are solvable. We don't know if E/k is solvable—we don't even know if E/k is Galois.

However if E/k *is* Galois, then ley $G = \mathrm{Gal}(E/k)$ and $N = \mathrm{Gal}(E/F)$, so that $G/N = \mathrm{Gal}(F/k)$. So E/k is Galois.

In the first lecture we mentioned how Gauss proved that $x^m - 1$ is solvable by radicals. We are finally ready to prove this:

Theorem 26.1.8 (Gauss)**.** *Let* $\mathrm{char}(k) = 0$*. Let* F *be any intermediate field such that* $\overline{k} \supset F \supset k$ *(i.e.,* F/k *is algebraic). Let* η *be a primitive* m*th root of unity. Then there exists a radical extension* M/F *such that* $M \supset F(\eta)$*.*

Proof. We use induction on m. If $m = 1$, then $M = F = k$ and we are done.

Assume the lemma holds for all $\ell < m$. Let $1 \neq \ell_1 < m$, and take η_1 to be a primitive ℓ_1st root of unity. By the induction hypothesis, there exists $F_1 \supset F(\eta_1)$ such that F_1/F is radical.

Now use F_1 as the new base field, letting $\ell_2 \neq 1, \ell_1$, $\ell_2 < m$, and taking η_2 to be a primitive ℓ_2nd root of unity. Then by the induction hypothesis there exists $F_2 \supset F_1(\eta_2)$ and F_2/F_1 is radical, whence F_2/F is radical.

Repeat this argument and we get some F'/F that is radical, and F' contains all ℓth roots of unity for $\ell < m$. Write

$$m = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r},$$

with p_i distinct primes. There are two cases to consider: if $r \geq 2$, then F' contains $\eta_{p_1^{e_1}}$ and $\eta_{p_2^{e_2} \cdots p_r^{e_r}}$. Since those two orders are coprime, F' contains a primitive mth root of unity, namely their product.

Second, if $r = 1$, i.e., $m = p_1^{e_1}$, then consider $G = \mathrm{Gal}(F'(\eta_m)/F') \hookrightarrow (\mathbb{Z}/m\mathbb{Z})^\times$, so $|G| \leq \varphi(m) < m$. So $\eta_m^{\varphi(m)} \in F'$, but F' contains a primitive $\varphi(m)$th root of unity, hence by the previous theorem $F'(\eta_m)/F'$ is radical.

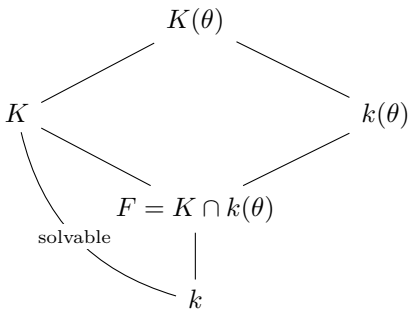
Hence $F'(\eta_m)/F$ is radical, and we are done. □

26.2 Galois' theorem

Theorem 26.2.1 (Galois)**.** *Assume* $\mathrm{char}(k) = 0$*. Let* $f(x) \in k[x]$*. Let* K *be a splitting field of* $f(x)$*, and let* $G = \mathrm{Gal}(K/k)$*. Then every root of* $f(x)$ *is contained in a radical extension of* k *if and only if* G *is solvable.*

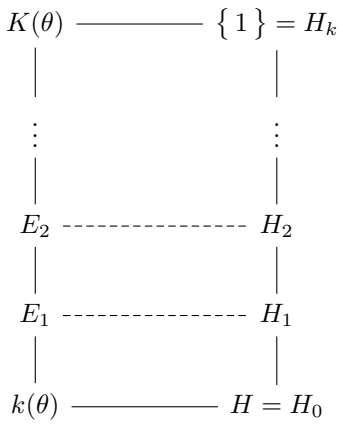
Proof. We prove the converse first. Suppose G is solvable, and let θ be a primitive nth root of unity with n sufficiently large (more on this in a moment).

We have the following situation:



Here, $K(\theta)/k(\theta)$ is Galois and solvable, since $\mathrm{Gal}(K/F)$ is a subgroup of $\mathrm{Gal}(K/k)$, which is solvable, and $H = \mathrm{Gal}(K(\theta)/k(\theta)) = \mathrm{Gal}(K/F)$ by Galois lifting.

Since $K(\theta)/k(\theta)$ is solvable, we have



meaning there exists a sequence

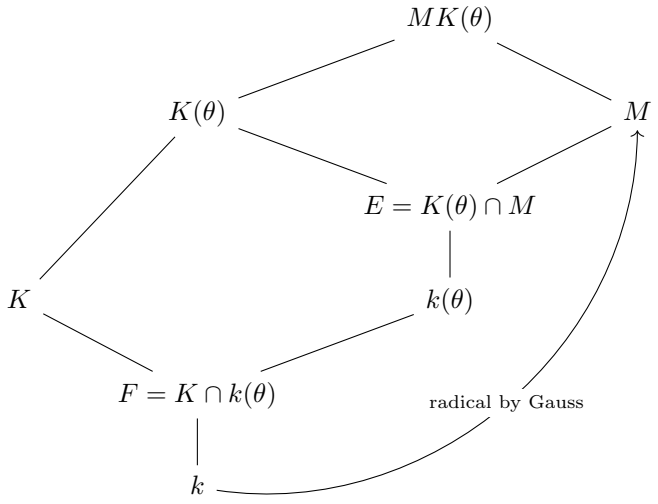
$$H = H_0 \supset H_1 \supset \cdots \supset H_k = \{1\}$$

such that H_{i-1}/H_i is cyclic (since the original extension is finite). For n sufficiently large, we can assume $k(\theta)$ contains all primitive $|H_{i-1}/H_i|$th roots of unity.

Hence E_i/E_{i-1} is cyclic with Galois group $\mathrm{Gal}(E_i/E_{i-1}) \cong H_i/H_{i-1}$. By Kummer's theorem and our previous theorem, E_i/E_{i-1} is therefore radical.

Hence $K(\theta)/k(\theta)$ is radical. So it $K(\theta)/k$ were radical we would be done, but in general that is not the case.

The trick now is to invoke Gauss lemma. By Gauss lemma there exists some M/k, which is radical, with $k(\theta) \subset M$. This extends our diagram to



and by Galois lifting and repeating the argument we used to show $K(\theta)/k(\theta)$ is radical we can show, in the same way, that $MK(\theta)/M$ is radical. Hence $MK(\theta)/k$ is radical, and the converse direction is done.

Lecture 27 Topological Groups

27.1 Galois theorem

Proof, continued. For the forward direction, assume $f(x)$ is irreducible in $k[x]$. (If not, suppose $f(x) = f_1(x)f_2(x)$ with the two factors irreducible. Then if K_1 is the splitting field of f_1 over k and K_2 is the splitting field of f_2 over k, we have that K_1/k is Galois and solvable, and so is K_1K_2/K_1 since it is the splitting field of f_2 over K_1. Now the large extension K_1K_2/k will be solvable if it is Galois, which is the case: it is the splitting field of f.)

Let α be a root of $f(x)$. Then there exist

$$k = E_0 \subset E_1 \subset E_2 \subset \cdots \subset E_s,$$

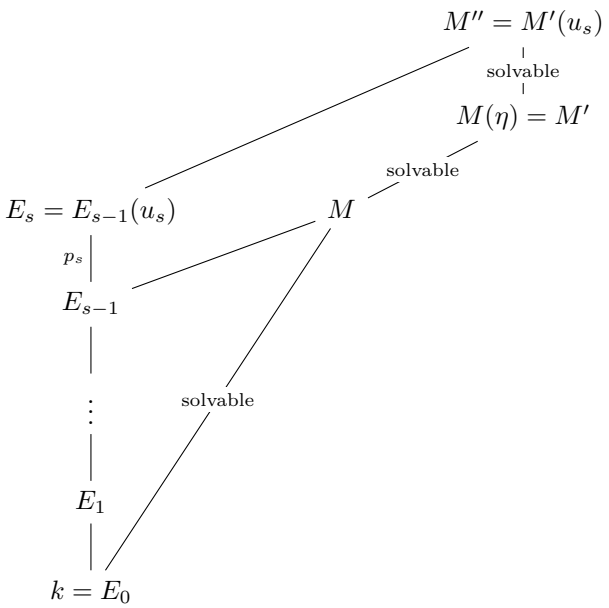
with each extension being radical of height 1 and $\alpha \in E_s$ (by which we mean the chain depends on α). We claim there exists a solvable extension M/k such that $M \supset E_s$ for all α. Hence M contains all roots of $f(x)$, meaning that $K \subset M$, so G is solvable.

We prove this by induction on s. In other words, suppose such M exist for $s-1$.

By definition of E_s/E_{s-1} being radical there exists some $u_s \in E_s$ such that $u_s^{p_s} \in E_{s-1}$. By the induction hypothesis there exists some M/k such that $M \supset E_{s-1}$ and M/k is solvable.

Let η be a primitive p_sth root of unity, and let $M' = M(\eta)$, and let $M'' = M'(u_s)$. Then $u_s^{p_s} \in E_{s-1} \subset M'$, so by Kummer's theorem M''/M' is a cyclic Galois extension, so in particular it is solvable (cyclic implies abelian implies solvable). In the same way, M'/M is solvable.

The situation is as follows:



Date: November 21st, 2019.

Hence if M''/k is Galois we would be done, since then M''/k is solvable, but in general this is not the case.

Instead we enlarge slightly by letting $\widehat{M''}$ be the Galois closure of M''/k. Then, by the Lemma below, $\mathrm{Gal}(\widehat{M''}/k)$ is solvable, and we are done. □

The lemma we need is this:

Lemma 27.1.1. *Let $k \subset F \subset D \subset \widehat{D}$, where $\widehat{D}$ is the Galois closure of D/k (i.e., the smallest Galois extension $\widehat{D}/k$ such that $D \subset \widehat{D} \subset \overline{k}$.) Assume D/F and F/k are solvable Galois extensions. Then $\mathrm{Gal}(\widehat{D}/k)$ is solvable.*

Proof. Let $G = \mathrm{Gal}(\widehat{D}/k)$ and $N = \mathrm{Gal}(\widehat{D}/F)$. Since $\mathrm{Gal}(F/k) \cong G/N$, G/N is solvable.

Similarly, since $\mathrm{Gal}(D/F) \cong N/H$, N/G is solvable.

Set

$$V = \bigcap_{g \in G} H^g,$$

where $H^g = gHg^{-1}$ is the conjugate.

Then $V \subset H$ is a normal subgroup in G, so fixed field E of V is Galois over k.

We have the following Galois correspondence:

$$\begin{array}{ccc}
\widehat{D} & \text{———} & \{1\} \\
| & & | \\
E & \text{———} & V \\
| & & | \\
D & \text{———} & H \\
| & & | \\
F & \text{———} & N = \mathrm{Gal}(\widehat{D}/F) \\
| & & | \\
k & \text{———} & G = \mathrm{Gal}(\widehat{D}/k)
\end{array}$$

But $\widehat{D}$ is the smallest Galois extension of k containing D, so by minimality $E = \widehat{D}$, and $V = \{1\}$. Hence $\widehat{D}/k$ is Galois.

Exercise 27.1.2. Suppose A and B are normal subgroups of a group G. Assume G/A and G/B are solvable. Then G/AB is also solvable.

Now H is normal in N, so $H^g \cap N$ is normal in N, and N/H is solvable. Hence $N/N \cap H^g$ is solvable. Repeat this for all $g \in HG$, and we conclude

$$N/\bigcap_{g \in G} H^g$$

is solvable, i.e., $N/V = N/\{1\} = N$ is solvable. Hence since G/N and N are solvable, G is solvable. □

This immediately gives:

Theorem 27.1.3 (Abel)**.** *Let k be a field with* $\operatorname{char}(k) = 0$*. For a general $f(x) \in k[x]$ with* $\deg f = n$*, $f(x)$ is solvable by radicals if and only if $n \leq 4$.*

(By this we mean, all polynomials of degree at most 4 *are solvable by radicals, but for higher degree this is not true.)*

Proof. This follows from the fact that S_n is solvable if and only if $n \leq 4$. □

Theorem 27.1.4. *Let $k \subset \mathbb{R}$. Let $f(x) = x^3 + ax^2 + bx + c \in k[x]$ be irreducible. Suppose all three roots of $f(x)$ are real. Then any root of $f(x)$ cannot be expressed using only real radicals.*

Proof. Write $f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$, so $K = k(\alpha_1, \alpha_2, \alpha_3)$ is the splitting field of $f(x)$ over k.

Suppose

$$k = E_0 \subset E_1 \subset E_2 \subset \cdots \subset E_s$$

are radical extensions with $\alpha_1 \in E_2$, and suppose that this chain is minimal in length for α_1 specifically (if not, just relabel).

So we have $\alpha_1 \in E_s$, but $\alpha_1 \notin E_{s-1}$, and indeed $\alpha_2, \alpha_3 \notin E_{s-1}$ either.

Since E_{s-1} don't contain the roots of $f(x)$, it is irreducible in there, so $[E_{s-1}(\alpha_1) : E_{s-1}] = \deg f = 3$. On the other hand, we can write $E_s = E_{s-1}(u_s)$ for some u_s, where $u_s^{p_s} \in E_{s-1}$ and $[E_s : E_{s-1}] = p_s$ is prime. Hence $p_s = 3$, and $E_s = E_{s-1}(\alpha_1)$.

Now let E be the Galois closure of E_s/E_{s-1}. Since E contains E_s, which contains α_1, and E/E_{s-1} is Galois, E contains all roots $\alpha_1, \alpha_2, \alpha_3$.

Hence E contains the splitting field of $f(x)$ over E_{s-1}. Let $u_s^3 = a \in E_{s-1}$, and let $g(x) = x^3 - a \in E_{s-1}[x]$.

Then $u_s \in E_s \subset E$, so $g(x) = (x - u_s)(x - u_s\omega)(x - u_s\omega^2)$ in E, where

$$\omega = \frac{-1 + \sqrt{-3}}{2}$$

is a primitive 3rd root of unity. In particular, $\omega = \frac{u_s\omega}{u_s} \in E$, so $E \not\subset \mathbb{R}$. Hence the radical extension containing the splitting field of $f(x)$ is not real. □

27.2 Infinite Galois

We will finally revisit something hinted at long ago: what happens when Galois groups are infinite?

Let K/k be Galois (possibly infinite). Let $G = \operatorname{Gal}(K/k)$. Let $\mathcal{F} = \left\{ F \,\middle|\, k \subset F \subset K \right\}$ be the set of all intermediate subfields and let $\mathcal{H} = \left\{ H \,\middle|\, H < G \right\}$ be the set of all subgroups.

Let $\Gamma\colon \mathcal{F} \to \mathcal{H}$ be defined by $\Gamma(F) = \operatorname{Gal}(K/F)$, and let $\Phi\colon \mathcal{H} \to \mathcal{F}$ be defined by $\Phi(H) = K^H$, the fixed field of H.

We know already that $\Phi(\Gamma(F)) = F$, i.e., $\Phi \circ F = \mathrm{Id}_{\mathcal{F}}$.

However $\Gamma \circ \Phi \neq \mathrm{Id}_{\mathcal{H}}$ in general, though if G is finite, then $\Gamma \circ \Phi = \mathrm{Id}_{\mathcal{H}}$.

To fix this, we will define a topology on G, and in that topology let $\mathcal{H}^o = \left\{ H \,\middle|\, H < G \text{ closed subgroup} \right\}$. We will show that $\Gamma \circ \Phi\Big|_{\mathcal{H}^o} = \mathrm{Id}_{\mathcal{H}^o}$.

Definition 27.2.1. A group G is said to be a ***topological group*** if

(*i*) G is a topological space and

(*ii*) $G \times G \to G$ defined by $(x, y) \mapsto xy$ and $G \to G$ defined by $x \mapsto x^{-1}$ are both continuous (i.e., the group actions are compatible with the topology).

Remark 27.2.2. If G is a topological group and $\mathcal{U}(1)$ is the system of neighbourhoods of 1, then $\mathcal{U}(1)$ satisfies

(*i*) $u \in \mathcal{U}(1)$ implies $1 \in u$;

(*ii*) $u_1, u_2 \in \mathcal{U}(1)$ implies $u_1 \cap u_2 \in \mathcal{U}(1)$;

(*iii*) $u \in \mathcal{U}(1)$ and $u \subset v$, v open, implies $v \in \mathcal{U}(1)$;

(*iv*) for all $u \in \mathcal{U}(1)$ there exists $w \in \mathcal{U}(1)$ such that $w \cdot w \subset u$;

(*v*) for all $u \in \mathcal{U}(1)$, $u^{-1} \in \mathcal{U}(1)$; and

(*vi*) for all $u \in \mathcal{U}(1)$ and all $g \in G$, $gug^{-1} \in \mathcal{U}(1)$.

Conversely, if a group G possesses a set $\mathcal{U}$ of subsets of G satisfying (*i*)–(*vi*), then G can be given the structure of a topological group with its ***fundamental system*** of neighbourhoods of 1 given by $\mathcal{U}$.

Lecture 28 Topological Groups

28.1 Review of topological spaces

Definition 28.1.1. A ***topology*** on a set X is a collection $\mathcal{F}$ of subsets of X satisfying

(*i*) $\varnothing, X \in \mathcal{F}$;

(*ii*) if $A_\alpha \in \mathcal{F}$, $\alpha \in \Lambda$, then $\bigcup_{\alpha\in\Lambda} A_\alpha \in \mathcal{F}$; and

(*iii*) if $A_1, A_2, \ldots, A_n \in \mathcal{F}$, then $A_1 \cap A_2 \cap \cdots \cap A_n \in \mathcal{F}$.

The tuple $(X, \mathcal{F})$ is called a ***topological space***. The elements in $\mathcal{F}$ are called ***open sets***.

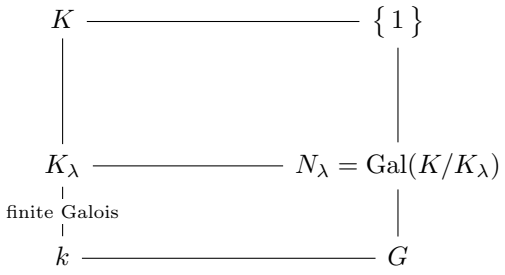
Note that *arbitrary* unions of open sets are open, but only *finite* intersections of open sets are open.

Definition 28.1.2. Let $(X, \mathcal{F}_X)$ and $(Y, \mathcal{F}_Y)$ be topological spaces. A function $f\colon X \to Y$ is ***continuous*** if $f^{-1}(A) \in \mathcal{F}_X$ for every $A \in \mathcal{F}_Y$.

Let K/k be Galois, and let $G = \mathrm{Gal}(K/k)$. Let

$$\mathcal{F} = \left\{ K_\lambda \;\middle|\; K \supset K_\lambda \supset k,\ K_\lambda/k \text{ is finite Galois} \right\} = \left\{ K_\lambda \;\middle|\; \lambda \in \Lambda \right\}.$$

We then have the following correspondence



Date: December 3rd, 2019.

Now since K_λ/k is finite Galois, N_λ is normal in G, and so $\mathrm{Gal}(K_\lambda/k) = G/N_\lambda$ is a finite group, since the K_λ/k is finite. Let $\mathcal{N} = \{ N_\lambda \mid \lambda \in \Lambda \}$.

Our goal is to use $\mathcal{N}$ to generate a topology on G.

Lemma 28.1.3. (*i*) $\bigcap_{\lambda\in\Lambda} N_\lambda = \{ 1 \}$.

(*ii*) *For $N_\lambda, N_\mu \in \mathcal{N}$, there exists some $N_\nu \in \mathcal{N}$ such that $N_\nu = N_\lambda \cap N_\mu$.*

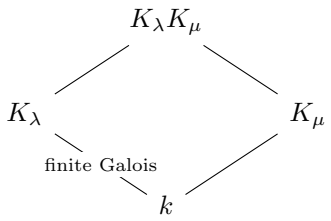
(*iii*) *For $N_\lambda \in \mathcal{N}$, there exists some $N_\mu \in \mathcal{N}$ such that $N_\mu^{-1} \subset N_\lambda$.*

(*iv*) *For $N_\lambda \in \mathcal{N}$, there exists $N_\nu \in \mathcal{N}$ such that $N_\mu N_\mu \subset N_\lambda$.*

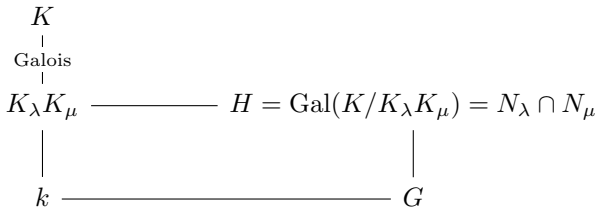
(*v*) *For $N_\lambda \in \mathcal{N}$ and $g \in G$, there exists $N_\mu \in \mathcal{N}$ such that $gN_\mu g^{-1} \subset N_\lambda$.*

Proof. (*i*) It suffices to show for $\sigma \neq 1$ there exists some N_λ such that $\sigma \notin N_\lambda$. Since $1 \neq \sigma\colon K \to K$, there must exist some $\alpha \in K$ such that $\sigma(\alpha) \neq \alpha$. Now $k(\alpha)/k$ might not be Galois, but if not we simply take its Galois closure $\widehat{k(\alpha)}$. Hence $\widehat{k(\alpha)}/k$ is finite Galois, so it is equal to K_λ for some λ, meaning it corresponds to $N_\lambda = \mathrm{Gal}(K/K_\lambda)$. Then $\sigma(\alpha) \neq \alpha \in K_\lambda$ implies $\sigma \notin N_\lambda$ since anything in N_λ must fix K_λ.

(*ii*) We have $N_\lambda = \mathrm{Gal}(K/K_\lambda)$ and $N_\mu = \mathrm{Gal}(K/K_\mu)$. Then $N_\lambda \cap N_\mu = \mathrm{Gal}(K/K_\lambda K_\mu)$. Considering the diagram



we can lift to see that $K_\lambda K_\mu/K_\mu$ is also finite Galois. This gives us a new graph



Here since H is the intersection of two normal subgroups in G, it is itself normal, so $K_\lambda K_\mu/k$ is finite Galois, meaning it K_ν for some ν, and we are done.

For the last three parts, using $N_\lambda = N_\mu$ suffices. □

We use $\mathcal{N} = \{ N_\lambda \mid \lambda \in \Lambda \}$ as a ***basis*** of the system of neighbourhoods of 1. Let $\mathcal{N}(1)$ denote this system of neighbourhoods of 1.

For $x \in G$, let $\mathcal{N}(x) = \{ xN \mid N \in \mathcal{N}(1) \}$.

In particular, if $G = \mathrm{Gal}(K/k)$, then this endows G with the structure of a topological group.

Proposition 28.1.4. *G is a T_0-topological space.*[3]

[3]Meaning for any two distinct points, we can find a neighbourhood of one not containing the other.

Proof. For $g_1, g_2 \in G$, $g_1 \neq g_2$, we can shift to $1, g_1^{-1}g_2$. Recall how

$$\bigcap_{\lambda\in\Lambda} N_\lambda = \{\, 1 \,\}$$

so there exists some N_λ such that $1 \in N_\lambda$ but $g_1^{-1}g_2 \notin N_\lambda$. Shifting back, $g_1 \in g_1 N_\lambda$ and $g_2 \notin g_1 N_\lambda$. □

Topological groups in general, not specifically Galois groups, have remarkable structure:

Proposition 28.1.5. *Let G be a general topological group.*

(*i*) *Any T_0-topological group is a T_2-space.*[4]

(*ii*) *Any T_2-topological group is* **regular**[5]

(*iii*) *Any open subgroup of a topological group is closed.*

(*iv*) *Any closed subgroup of finite index is open.*

(*v*) *Any subgroup that contains an open subgroup is open.*

Proof. We prove some of these.

(*i*) Without loss of generality, take $1, g \in G$. There exists an open set U such that $1 \in U$ and $g \notin U$ since by hypothesis the space is T_0. Now take an open neighbourhood V of 1 such that $VV^{-1} \subset U$ (this is always possible, since we could take for instance $V = U \cap U^{-1}$). Then gV is an open neighbourhood of g. We claim $gV \cap V = \varnothing$.

If not, then there exist $v, u \in V$ such that $gv = u$, meaning that $g = uv^{-1} \in VV^{-1} \subset U$, contradicting $g \notin U$.

(*iii*) Let $H < G$ be an open subgroup. We can decompose G into cosets, say

$$H = \bigsqcup_{g\in G/H} gH$$

where by $\sqcup$ we mean a disjoint union. Since H is open, so are gH, and we can rearrange this into

$$H = G \setminus \Big(\bigsqcup_{g\neq 1} gH\Big),$$

so H is the complement of some arbitrary union of open sets, so it is is the complement of an open set, so it is closed.

(*iv*) As above, but this time we need finite index to ensure we get a finite intersection.

[4]Also known as a ***Hausdorff space***, meaning that for any two distinct points we can find neighbourhoods of both that do not intersect.

[5]Meaning we can separable not only two distinct points by neighbourhoods, but any point and any closed set.

(v) The idea is similar: if $G \supset H \supset J$, with J open, then we can write

$$H = \bigcup_{h \in H} hJ$$

with hJ open, so H is a union of open sets, so open. □

Back to Galois groups $G = \mathrm{Gal}(K/k)$ in particular.

Proposition 28.1.6. *The subgroup $\{1\}$ is closed. Hence any single point in G is closed.*

Proof. Recall

$$\{1\} = \bigcap_{\lambda \in \Lambda} N_\lambda.$$

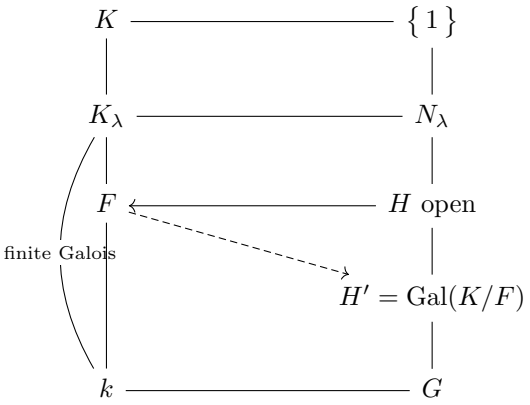
where N_λ is open. Open subgroups are closed, as discussed above, so N_λ is closed. Hence $\{1\}$ is an arbitrary intersection of closed sets, so is closed. □

In the special case where K/k is finite Galois, $G = \mathrm{Gal}(K/k)$ is a finite group. This means that for any $g \in G$, $\{g\}^c = G \setminus \{g\}$ is closed, because it is finite, so $\{g\}$ is also open. Hence G is a ***discrete group*** (i.e., its topology is discrete—every set is open and closed.).

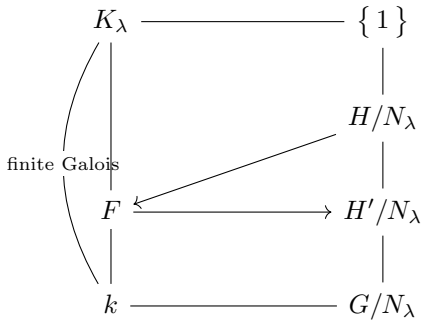
Theorem 28.1.7. *Let K/k be infinite Galois, with $G = \mathrm{Gal}(K/k)$. Then we have*

- (i) *A subgroup $H < G$ is open if and only if there exists $K \supset F \supset k$, $[F : k] < \infty$, with $H = \mathrm{Gal}(K/k)$.*
- (ii) *A subgroup $H < G$ is closed if and only if $H = \bigcap_\alpha U_\alpha$ where U_α are open subgroups.*

Proof. (i) For the forward direction, there exists N_λ such that $N_\lambda \subset H$ since H is open. We have the situation

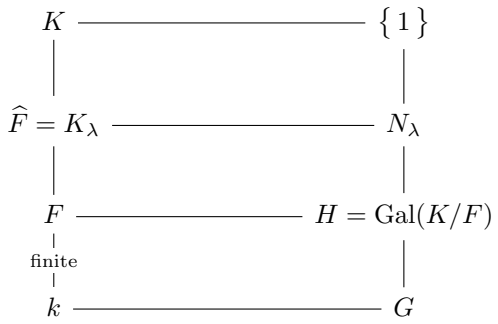


If we focus on the lower part of this, we can reframe it as



Then $H = H'$ because $H/N_\lambda = H'/N_\lambda$, since both come from finite Galois extensions, where the correspondence is one-to-one always.

For the converse direction, things fall out pretty much immediately. We have



so H contains an open subgroup, meaning that H is open.

(*ii*) For the forward direction we use the following lemma, to be proved momentarily:

Lemma 28.1.8. *Let H be asubgroup of G. Then $\overline{H} = \bigcap_{\lambda\in\Lambda} HN_\lambda$.*

With this, it follows immediately that if H is closed,

$$H = \overline{H} = \bigcap_{\lambda\in\Lambda} HN_\lambda,$$

where HN_λ is open.

For the converse,

$$H = \bigcap_{\alpha} U_\alpha,$$

where U_α are open subgroups, meaning they're closed, so H is an arbitrary intersection of closed sets, so it is closed. □

We now prove the above lemma:

Proof of lemma. We have $\sigma \in \overline{H}$ if and only if for all $\lambda \in \Lambda$, $\sigma N_\lambda \cap H \neq \varnothing$, if and only if for all $\lambda \in \Lambda$, there exists $n_\lambda \in N_\lambda$ and $h_\lambda \in H$ such that $\sigma n_\lambda = h_\lambda$. This is equivalent to $\sigma \in HN_\lambda$ (using the inverse property) for all $\lambda \in \Lambda$, which is true if and only if $\sigma \in \bigcap_{\lambda\in\Lambda} HN_\lambda$. □

Lecture 29 Infinite Galois Correspondence

29.1 Infinite Galois extensions

In the last theorem, note how the intermediate field F/k is finite Galois, meaning that it is finite and separable. The Primitive element theorem tells us this is simple, so $F = k(\alpha)$ for some $\alpha \in K$. In other words, if $H < G$ is a subgroup, then H is open if and only if there exists some $\alpha \in K$ such that $H = \mathrm{Gal}(K/k(\alpha))$.

Consequently:

Proposition 29.1.1. *Let K/k be infinite Galois. Let $G = \mathrm{Gal}(K/k)$. Let $K \supset F \supset k$ by any intermediate field. Then*

$$\Gamma(F) = \mathrm{Gal}(K/F) = \bigcap_{\alpha \in F} \Gamma(k(\alpha))$$

is closed.

Proof. It is clear: $\Gamma(k(\alpha))$ is open, but open subgroups are closed, so this is an arbitrary intersection of closed sets, and so closed. □

Let $\mathcal{H}^o$ be the set of all closed subgroups of G. Let $\mathcal{F}$ be the set of all intermediate fields. Then as before we have a map $\Gamma\colon \mathcal{F} \to \mathcal{H}^o$ taking the Galois group and a map back $\Phi\colon \mathcal{H}^o \to \mathcal{F}$ taking the fixed field.

Theorem 29.1.2 (Krull)**.** *Let K/K be (infinite) Galois, and $G = \mathrm{Gal}(K/k)$. Let $H < G$ be a subgroup. Then*

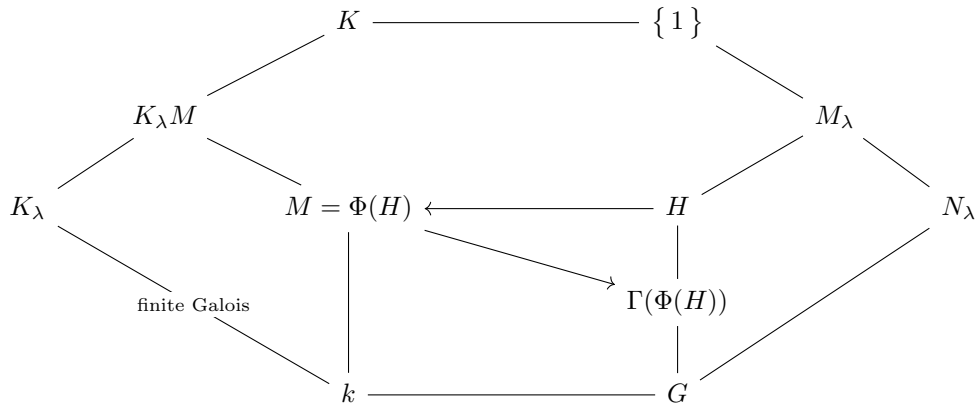
(*i*) *H is dense in $\Gamma(\Phi(H))$ (i.e., $\overline{H} = \Gamma(\Phi(H))$).*

(*ii*) *H is closed if and only if $H = \Gamma(\Phi(H))$.*

Proof. First note how (*ii*) follows immediately from (*i*), so let us focus on the first one.

It suffices to show that, for any $\sigma \in \Gamma(\Phi(H))$, and any neighbourhood σN_λ of σ, σN_λ contains an element of H (so $\sigma N_\lambda \cap H \neq \varnothing$).

We have the following, quite complicated, diagram:



Date: December 5th, 2019.

There are some comments to be made here. Any neighbourhood of 1 looks like N_λ, so shifting it σN_λ is a neighbourhood of σ. On the other hand, N_λ corresponds to an extension K_λ/k that is finite Galois.

Moreover, we can lift this to $K_\lambda M/M$, whence this is also finite Galois, and so this corresponds to some $M_\lambda \subset N_\lambda$.

Now consider a map $\varphi\colon \Gamma(\Phi(H)) \to \mathrm{Gal}(K_\lambda M/M)$ defined by $\rho \mapsto \rho\big|_{K_\lambda M}$ (note how $\Gamma(\Phi(H)) = \mathrm{Gal}(K/M)$, so this makes sense). Then φ is a surjective homomorphism, since automorphisms can be lifted to K, being an algebraic extension.

The fixed field of $\varphi(H)$ is M, so $\varphi(H) = \mathrm{Gal}(K_\lambda M/M)$. To see this, consider the Galois correspondence

and restrict the correspondence to the lower half of the diagram.

Consequently $\varphi(\sigma) = \sigma\big|_{K_\lambda M} = \varphi(h) \in \mathrm{Gal}(K_\lambda M/M)$ for some $h \in H$. So we have $h\colon K \to K$, and we can lift $\sigma\colon K \to K$, and hence $\sigma^{-1} \circ h \in \mathrm{Gal}(K/k)$.

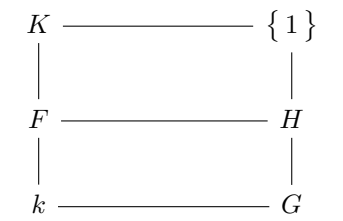
On the other hand, $\sigma^{-1} \circ h\big|_{K_\lambda M} = \mathrm{Id}_{K_\lambda M}$, so $\sigma^{-1} \circ h \in \mathrm{Gal}(K/K_\lambda M) = M_\lambda \subset N_\lambda$.

Hence $h \in \sigma N_\lambda$, but $h \in H$, so $H \cap \sigma N_\lambda \neq \varnothing$. □

This finishes our Galois correspondence:

Theorem 29.1.3 (Galois correspondence)**.** *Let K/k be (infinite) Galois and let $G = \mathrm{Gal}(K/k)$. Let $\mathcal{F}$ be the set of all intermediate fields and let $\mathcal{H}^o$ be the set of all closed subgroups of G. Then $\Gamma\colon \mathcal{F} \to \mathcal{H}^o$ and $\Phi\colon \mathcal{H}^o \to \mathcal{F}$ are one-to-one and onto correspondences.*

In particular, if we have the diagram



then F/k is Galois if and only if H is a closed normal subgroup of G.

Index