MATH 5055: ADVANCED ALGEBRA II (GALOIS THEORY)

HEESUNG YANG

1. September 6: Field Extensions (Section 5.1)

Definition 1.1. A field F is an *extension field* of a field K (or simply an *extension*) if $K \subseteq F$. We will often say that F/K is an *extension of fields*. Then F is a K-vector space. The dimension $\dim_K F$ will be denoted by $[F : K]$, which is also known as the *degree of an extension*. If F/E and E/K are both field extensions, we call E an *intermediate field* of F/K. Visually, the following diagram represents this *tower of fields*.

$$\begin{array}{c} F \\ | \\ E \\ | \\ K \end{array}$$

Theorem 1.1 (Multiplicativity of degrees in towers)**.** *Let F/E and E/K be field extensions. Then*

$$[F : K] = [F : E][E : K]$$

Proof (sketch). Let $\{u_1, \dots, u_m\} \subset E$ be a basis for E/K and $\{v_1, v_2, \dots v_n\}$ be a basis for F/E. All we need is to display a basis for F/K, and that there are mn elements. Namely, we claim that $\{u_i v_j \,|\, 1 \le i \le m, 1 \le j \le n\}$ is a basis for F/K. Proof of this claim will be left to the reader as an exercise. Finally, from the claim, we have $[F : K] = \#\{u_i v_j \,|\, 1 \le i \le m, 1 \le j \le n\} = mn = [F : E][E : K]$, as required. □

Definition 1.2. The *subfield* (resp. *subring*) of F generated by X is the intersection of all subfields (resp. subrings) of F that contain R, i.e., the <u>smallest</u> subfield (resp. subring) of F containing X. If F/K is an extension of fields, the *subfield generated by $X \subseteq F$ over K* (resp. *subring*) is the subfield (resp. subring) generated by $X \cup K$. This will be denoted by $K(X)$ (resp. $K[X]$).

Definition 1.3. For ease of notation, if $X = \{u_1, \dots, u_n\}$ is finite, we write $K(X) = K(u_1, \dots, u_n)$ and $K[X] = K[u_1, \dots, u_n]$. Then $K(X)$ and $K[X]$ are *finitely generated*. They are called *simple* if $n = 1$.

Lemma 1.1. *$K(u_1, \dots, u_n)$ and $K[u_1, \dots, u_n]$ do not depend on the order of the u_j. Furthermore, we have*

$$K[u_1, \dots, u_n] = (K[u_1, \dots, u_{n-1}])[u_n]$$
$$K(u_1, \dots, u_n) = (K(u_1, \dots, u_{n-1}))(u_n).$$

Date: 6 January 2019.

Theorem 1.2. *Let F/K be an extension of fields. Then we have:*

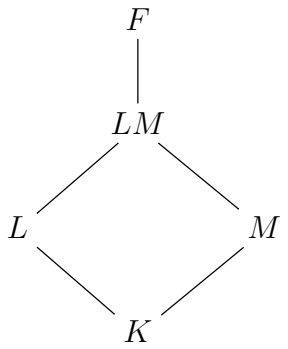
(a) $K[X] = \{f(u_1, \ldots, u_n) \,|\, n \in \mathbb{N}, u_1, \ldots, u_n \in X, f \in K[x_1, \ldots, x_n]\}$
(b) $K(X) = \{f(u_1, \ldots, u_n) \,|\, n \in \mathbb{N}, u_1, \ldots, u_n \in X, f \in K(x_1, \ldots, x_n)\}$
(c) For each $v \in K(X)$ there is a finite subset X' of X such that $v \in K(X)$. Similar claims hold for $K[X]$ and $K[X']$.

Proof (sketch). As for (a) and (b), we note that it is readily verified that our candidate sets have the required algebraic structure and sit inside F (hence, left as an exercise). Thus $K[X]$ is a subring of F containing K, and $K(X)$ is a subfield of F containing K. Finally, if R is any subring of F containing both X and K, then R would have to contain all polynomial expression in elements of X having coefficients in K. Similarly, if L is any subfield of F containing both X and K, then L must contain all rational function expressions in elements of X with coefficients in K.

As for part (c), if $v \in K[X]$ then v can be written in the form $f(u_1, \ldots, u_n)$ for some $u_1, \ldots, u_n \in X$ and $f \in K[x_1, \ldots, x_n]$. But then $v \in K[u_1, \ldots, u_n]$, so $v \in K[X']$ for the finite subset $X' = \{u_1, \ldots, u_n\} \subseteq X$. Similarly, if $v \in K(X)$, then $v = f(u_1, \ldots, u_n)$ for some $u_1, \ldots, u_n \in X$, except that f this time is a rational function. Hence we obtain $v \in K(u_1, \ldots, u_n)$ by employing the similar type of argument. □

2. September 7: Composite fields, algebraic, and transcendental extension

Definition 2.1. Let L and M be subfields of F. Then the *composite field of L and M in F* is the field generated by $L \cup M$. It is denoted by LM. The tower of the fields will look like the below:



Definition 2.2. Let F/K be a field extension.

(a) $u \in F$ is *algebraic over K* if it satisfies a non-zero polynomial in $K[x]$. Otherwise u is *transcendental over K*.
(b) F/K is an *algebraic extension* if every element of F is algebraic over K. Otherwise it is a *transcendental extension*.

Remark.
- Every $u \in K$ is algebraic over K (because $x - u \in K[x]$).

- If $u \in F$ is algebraic over K, then u is automatically algebraic over intermediate fields of F/K. This is simply because $K[x] \subseteq E[x]$ for any intermediate fields E.

$$\begin{array}{ll} F & \ni u \\ | & \\ E & \\ | & \\ K & \end{array}$$

- $u \in F$ is algebraic over K if and only if it satisfies a monic polynomial (a polynomial with leading coefficient 1) in $K[x]$. In fact, the only algebraic elements in $K(x_1, \ldots, x_n)$ over K are those in K itself.

Example.
- $i \in \mathbb{C}$ is algebraic over $\mathbb{Q}$ (satisfies $x^2 + 1 \in \mathbb{Q}[x]$). Thus $i \in \mathbb{C}$ is algebraic over $\mathbb{R}$ also. In faxt, $\mathbb{R}(i) = \mathbb{C}$.
- $\pi, e \in \mathbb{R}$ are transcendental over $\mathbb{Q}$.
- Each of the variables x_j in the rational functions field $K(x_1, \ldots, x_n)$ is transcendental over K.

3. September 7: Simple extensions

Let F/K be a field extension where $F = K(u)$ for some $u \in F$, ie, F/K is a simple extension. Let $\varphi : K[x] \to K[u]$ be a homomorphism defined by $a_0 + a_1 x + \cdots + a_n x^n \mapsto a_0 + a_1 u + \cdots + a_n u^n$. Then by the first isomorphism theorem, we have $K[x]/\ker\varphi \cong K[u]$. If the kernel is trivial, then we have $K[x] \cong K[u]$. In this case, u is transcendental (in fact, $K[x] \cong K[u]$ iff u is transcendental). It thus follows that u is algebraic if and only if $\ker\varphi \neq (0)$. In particular, we have the following:

Theorem 3.1. *With the above notation, let $u \in F$ be transcendental over K. Then there is an isomorphism $K(u) \cong K(x)$ that is the identity on K.*

So, nothing much can be said about the transcendental case, as $K(u)$ is just isomorphic to the "boring" field of rational functions. But the algebraic cases are more interesting.

Recall that $\ker\varphi \neq (0)$ if u is algebraic. K is a field, so $K[x]$ is a principal ideal domain (PID). Thus $\ker\varphi = (f)$ for some $f \in K[x]$. There is a unique monic generator $f_u(x)$ for this ideal.

Definition 3.1. The polynomial $f_u(x)$ above is said to be the *minimal polynomial of u over K*.

The definition makes it clear that f_u is minimal with respect to divisibility amongst all the polynomials satisfied by u. That is, f_u divides every polynomial satisfied by u. Also, f_u is the polynomial of least degree satisfied by u.

Theorem 3.2. *f_u is the unique monic polynomial of least degree in $K[x]$ satisfied by u.*

Definition 3.2. Let D be an integral domain.

(a) $u \in D$ is a prime $\Leftrightarrow$ if $u \mid vw$ then $u \mid v$ or $u \mid w$ for all $v, w \in D$.
(b) $u \in D$ is irreducible $\Leftrightarrow$ if $u = vw$ then one of v, w is a unit (and the other is associate to u)t.

In any integral domain, primes are irreducible.

Remark. Every irreducible is a prime only when D is a unique factorization domain (UFD). Thus the same claim holds for PIDs, as every PID is a UFD. Thus any irreducible in $K[x]$ is also a prime.

Proposition 3.1. *Let D be an integral domain.*

(a) An element $u \in D$ is a prime if and only if (u) is a prime ideal of D.
(b) An element $u \in D$ is an irreducible if and only if (u) is maximal amongst principal ideals of D.
(c) In particular, if D is a PID, then $u \in D$ is irreducible if and only if (u) is maximal.

Proposition 3.2. *Let R be a commutative ring.*

(a) Let P be a prime ideal. Then R/P is an integral domain.
(b) Let M be a maximal ideal. Then R/M is a field.

Theorem 3.3. *Let F/K be a field extension, and let u be algebraic over K. Suppose that $f_u(x) \in K[x]$ is the minimal polynomial of u over K.*

(a) $K(u) = K[u]$
(b) $K(u) \cong K[x]/(f_u(x))$
(c) $[K(u) : K] = n$ where $n := \deg f_u$.
(d) $\{1, u, u^2, \ldots, u^{n-1}\}$ is a K-basis for $K(u)$.
(e) Every element in $v \in K(u)$ can be written uniquely in the form of $v = a_0 + a_1 u + \cdots + a_{n-1}u^{n-1}$ for $a_0, \ldots, a_{n-1} \in K$.

Proof. It follows from the first isomorphism theorem that $K[u] \cong K[x]/(f_u(x))$, which is an integral domain. Thus, $f_u(x)$ is a prime ideal of $K[x]$. This means that $f_u(x)$ is prime hence irreducible also. Therefore $(f_u(x))$ is maximal, so $K[x]/(f_u(x)) \cong K[u]$ is a field. But note that $K[u] \subseteq K(u)$. But $K(u)$ is the smallest subfield of F containing K and u and $K[u] \subseteq K(u)$. This completes parts (a) and (b). □

4. September 11

Proposition 4.1. *Let F/K be a field extension, and $u \in F$ algebraic over K. Let $f(x) \in K[x]$ be the monic polynomial satisfied by f. Then the following are equivalent:*

(a) f is the minimal polynomial of u over K.
(b) f is of least degree amongst monic polynomials in $K[x]$ satisfied by u
(c) f divides all such polynomials.
(d) f is irreducible over K.

Definition 4.1. The *degree of $u \in F$ over K* is the degree of f_u. It equals the dimension $[K(u) : K]$ of $K(u)$ over K.

Example. Let u be a real root of $f(x) = x^3 - 3x - 1 \in \mathbb{Q}[x]$.

(a) Show that $[\mathbb{Q}(u) : \mathbb{Q}] = 3$ and $\{1, u, u^2\}$ is a $\mathbb{Q}$-basis for $\mathbb{Q}(u)$.
Solution: We show that f is irreducible over $\mathbb{Q}$. Suppose not. Then f would have a rational root, say $a \in \mathbb{Q}$. The rational root theorem limits us to two possibilities: ± 1. But then we see that $1^3 - 3 - 1 \neq 0$ and $(-1)^3 - 3(-1) - 1 \neq 0$. Thus $x^3 - 3x - 1$ is irreducible over $\mathbb{Q}$. f is thus f_u, the minimal polynomial of u, hence $[\mathbb{Q}(u) : \mathbb{Q}] = 3 = \deg f_u$. It is a standard exercise to check that $\{1, u, u^2\}$ is a basis.

(b) Express $v = u^4 + 2u^3 + 3 \in \mathbb{Q}[(u)$ as a $\mathbb{Q}$-linear combination of $1, u, u^2$.
Solution: $f(u) = 0$, so $u^3 = 3u + 1$. Thus

$$\begin{aligned} v &= u \cdot u^3 + 2u^3 + 3 \\ &= u(3u+1) + 2(3u+1) + 3 \\ &= 5 + 7u + 3u^2. \end{aligned}$$

(c) Do the same for v^{-1}.
Solution: Let $v^{-1} = a + bu + cu^2$ where $a, b, c \in \mathbb{Q}$. Thus we have $(5+7u+3u^2)(a+bu+cu^2) = 1 = vv^{-1}$.

$$\begin{aligned} (5+7u+3u^2)(a+bu+cu^2) &= 1 \\ 5a + (5b+7a)u + (5c+3a+7b)u^2 + (7c+3b)u^3 + 3cu^4 &= 1 \\ 5a + (5b+7a)u + (5c+3a+7b)u^2 + (7c+3b)(3u+1) + 3cu(3u+1) &= 1 \\ (5a+3b+7c) + (7a+14b+24c)u + (3a+7b+14c)u^2 &= 1. \end{aligned}$$

Equate coefficients, and make the computer solve the system for you. Then you get $a = \frac{28}{111}, b = -\frac{26}{111}, c = \frac{7}{111}$. Therefore $v^{-1} = \frac{28}{111} - \frac{26}{111} + \frac{7}{111}u^2$.

Let $\sigma : R \to S$ be a ring isomorphism. Then σ naturally extends to a ring isomorphism between $R[x]$ and $S[x]$, by applying σ to the coefficients of polynomials in $R[x]$, i.e.,

$$\sigma : \sum_j u_j x^j \mapsto \sum_j \sigma(u_j) x^j.$$

Theorem 4.1. *Let $\sigma : K \to L$ be a field isomorphism, u an element in some extension of K and v an element in some extension of L. If either:*

(i) u is transcendental over K, and v is transcendental over L; or
(ii) u is algebraic over K (with the minimal polynomial f_u, and v is algebraic over L (with the minimal polynomial f_v), and $\sigma f_u = f_v$ holds,

then σ extends to an isomorphism $K(u) \to K(v)$ that maps u onto v.

$$\begin{array}{ccc} K(u) & \xrightarrow[\sigma]{} & K(v) \\ \Big| & & \Big| \\ K & \xrightarrow[\sigma]{} & L \end{array}$$

Proof. Suppose that (i) holds. Then σ extends further to a field isomorphism $K(x) \to L(x)$ (just apply σ to the numerators and denominators). If u is transcendental over K and v transcendental over L, then we have isomorphisms between

$$\begin{aligned} K(u) \to K(x) \to L(x) \to L(v) \\ f(u) \mapsto f(x) \mapsto (\sigma f)(x) \mapsto (\sigma f)(v), \end{aligned}$$

the composite of which is an isomorphism from $K(u)$ to $L(v)$, extending σ and mapping u onto v.

Now suppose that (ii) holds. Then we have the field isomorphism $\sigma : K[x] \to L[x]$. Under this map, we have $\sigma((f_u)) = (\sigma f_u) = (f_v)$. We therefore obtain an induced isomorphism

$$K[x]/(f_u) \to L[x]/(f_v)$$
$$x + (f_u) \mapsto x + (f_v).$$

All in all, we get isomorphisms $K(u) = K[u] \to K[x]/(f_u) \to L[x]/(f_v) \to L[u] = L(v)$, the composite of which is an isomorphism. Now take $K = L$ and $\sigma = \mathrm{id}_K$, then the result follows. □

Corollary 4.1. *Let u and v be elements in some extension of K. Suppose also that u and v are algebraic over K. Then the following are equivalent:*

(i) $f_u = f_v$ (i.e, u and v have the same minimal polynomial over K)
(ii) There exists an isomorphism from $K(u)$ to $K(v)$ that maps u onto v and is the identity on K.

Proof. ((ii) ⇒ (i)) Let $f_u(x) = \sum_j a_j x^j$. Then clearly we have $0 = f_u(u) = \sum_j a_j u^j$. Applying $\sigma : K(u) \to K(v)$ gives

$$\begin{aligned} 0 = \sigma(0) &= \sigma\left(\sum_j a_j u^j\right) \\ &= \sum_j \sigma(a_j)\sigma(u)^j \\ &= \sigma_j a_j v^j, \end{aligned}$$

since σ fixes $a_j \in K$ and $\sigma : u \mapsto v$. Thus v is a root of f_u. The result follows upon observing that f_u is irreducible over K.

((i) ⇒ (ii)) This is a direct consequence of Theorem 4.1. □

5. September 13

Theorem 5.1. *Let $f \in K[x]$ be a degree n polynomial. Then there exists a simple extension $K(u)$ over K such that:*

(i) u is a root of f
(ii) $[K(u) : K] \leq n$ with equality holding if and only if f is irreducible over K
(iii) whenever f is irreducible, $K(u)$ is unique up to an isomorphism fixing K.

Proof (sketch). Let g be an irreducible factor of f. Then (g) is maximal in $K[x]$. Therefore $K[x]/(g)$ is a field. Then the inclusion map $K \hookrightarrow K[x]/(g)$ defined by $a \mapsto a + (g)$ is a monomorphism, so we can view K as a subfield of $K[x]/(g)$. For $u := x + (g)$ is a root of g (and therefore of f), it follows $K[x]/(g) = K(u)$. So it follows that $[K(u) : K] = \deg g \leq \deg f = n$. If f is irreducible, then $g = f$, so equality holds in this case. □

Theorem 5.2. *Every finite extension is algebraic and is finitely generated.*

Proof. Let F/K be a finite extension, say of degree n. Let $u \in F$. The elements $1, u, u^2, \ldots, u^n \in F$ must be K-linearly dependent. Thus there are constants $a_0, a_1, \ldots, a_n \in K$ not all zero such that $a_0 + a_1 u + a_2 u^2 + \cdots + a_n u^n = 0$. Therefore u is algebraic as desired. F/K is thus

algebraic as u was arbitrary. Finally, observe that any chosen K-basis for F generates F as a field, so F is indeed finitely generated. $\square$

Theorem 5.3. *If $F = K(X)$ for some subset X of F consisting entirely of elements that are algebraic over K then F/K is algebraic.*

Proof. Let $u \in F$. Then $u \in K(u_1 \ldots, u_n)$ for finitely many $u_j \in X$. Consider the following tower of fields:

$$\begin{array}{c} K(u_1, \ldots, u_n) \\ | \\ K(u_1, \ldots, u_{n-1}) \\ | \\ \vdots \\ | \\ K(u_1, u_2) \\ | \\ K(u_1) \\ | \\ K \end{array}$$

Each u_j is algebraic over K (because $u_j \in X$), so each u_j is algebraic over $K(u_1, \ldots, u_{j-1})$. For all j, we see that $[K(u_1, \ldots, u_j) : K(u_1, \ldots, u_{j-1})] < \infty$. So we have that

$$[K(u_1, \ldots, u_n) : K] = \prod_j [K(u_1, \ldots, u_j) : K(u_1, \ldots, u_{j-1})]$$

is finite. Hence $K(u_1, \ldots, u_n)/K$ is algebraic, so u is algebraic over K. Hence F/K is algebraic. $\square$

Remark. If X happened to be finite, then $K(X)/K$ is not just algebraic, but finite as well.

Theorem 5.4. *If F/E and E/K are algebraic extensions, then F/K is an algebraic extension.*

Proof. Let $u \in F$. Then u is algebraic over E.Therefore there exist $b_0, \ldots b_j \in E$ and $b_n \neq 0$ such that $b_0 + b_1 u + \cdots + b_n u^n = 0$. Hence u is algebraic over $K(b_0, \ldots, b_n)$. But $K(b_0, \ldots, b_n)$ is a finite extension of k. Finally, we see that we have the tower

$$\begin{array}{c} K(b_0, \ldots, b_n)(u) \\ | \\ K(b_0, \ldots, b_n) \\ | \\ K \end{array}$$

such that each of the extension is finite. Therefore $K(b_0, \ldots, b_n)(u)/K$ is finite, hence algebraic. So u is algebraic over K as required. □

Theorem 5.5. *The set E of all elements of F that are algebraic over K is a field. It is the maximal algebraic subextension of F/K.*

Proof. The second statement is immediate from the first statement, so it suffices to prove the first statement. Let $u, v \in E$ with $v \neq 0$. We need to show that $u - v, uv^{-1} \in E$ in order to show that E is a field. Consider the tower

$$\begin{array}{c} E \\ | \\ K(u,v) \\ | \\ K \end{array}$$

Clearly $K(u, v)$ is a field, so $K(u, v) \ni u - v, uv^{-1}$. Therefore $u - v, uv^{-1} \in E$. Thus E is a field as required. □

6. September 13 & 14: Fundamental Theorem of Galois Theory

Let E/K and F/K be field extensions, and let $\sigma : E \to F$ a non-zero field homomorphism. We are mostly interested in σ that also preserves the linear structure of E/K and F/K. The following result shows that the maps of interest are those that fix K element-wise.

Lemma 6.1. *Let E/K and F/K be fields extensions, and $\sigma : E \to F$ a non-zero field homomorphism. Then σ is a K-linear transformation (or a K-module homomorphism) if and only if $\sigma|_K = \mathrm{id}_K$ (i.e., σ fixes K element-wise).*

Proof. Suppose first that σ is K-linear, and let $a \in K$. Then $\sigma(a) = \sigma(a \cdot 1) = a\sigma(1) = a$. Thus σ fixes K element-wise. Conversely, if σ fixes K element-wise, and if u, v *inE* and $a \in K$, then we have $\sigma(u + av) = \sigma(u) + \sigma(a)\sigma(v) = \sigma(u) + a\sigma(v)$. Thus σ is K-linear. □

Definition 6.1. A *K-homomorphism* a non-zero homomorphism from E to F that fixes K element-wise. Similarly, we can define a *K-monomorphism, K-epimorphism, K-isomorphism*, and *K-automorphism*.

Definition 6.2. The *Galois group* of F/K, denoted $\mathrm{Aut}_K F$ is the set of all K-automorphisms of F.

Example. Let $F := K(x)$ be the rational function field over the infinite field K. Show that the Galois group $\mathrm{Aut}_K K(x)$ is an infinite, non-abelian group.

Proof. For $a \in K \setminus \{0\}$, the dilation map defined as

$$\sigma_a \left(\frac{f(x)}{g(x)} \right) = \frac{f(ax)}{g(ax)},$$

for $f, g \in K[x]$, is a K-automorphism of $K(x)$. Further, for $b \in K$ we have the K-automorphism

$$\tau_b \left(\frac{f(x)}{g(x)} \right) = \frac{f(x+b)}{g(x+b)},$$

for $f, g \in K[x]$, given by translation by b. Therefore $\mathrm{Aut}_K\, K(x)$ is infinite. Also, $\mathrm{Aut}_K\, K(x)$ is indeed not abelian because σ_a and τ_b cannot commute as long as $a \neq 1, b \neq 0$. Note that $\sigma_a\tau_b(x) = a(x+b) = ax + ab$ whereas $\tau_b\sigma_a(x) = \tau_b(ax) = ax + b$. □

Theorem 6.1. *Let $\sigma \in \mathrm{Aut}_K\, F$ and $f \in K[x]$. If u is a root of f, then so is $\sigma(u)$.*

Proof. Let $f(x) := \sum_j a_j x^j$ with $a_j \in K$. Then it follows that

$$\begin{aligned} 0 = \sigma(0) &= \sigma\left(\sum_j a_j u^j\right) \\ &= \sum_j \sigma(a_j)\sigma(u)^j \\ &= \sum_j a_j \sigma(u)^j = f(\sigma(u)), \end{aligned}$$

as desired. □

Our primary focus will be extensions of the form $F = K(u)$ where u is algebraic over K.

- Each element in $\mathrm{Aut}_K\, K(u)$ is uniquely determined by its value at u.
- Each element of $\mathrm{Aut}_K\, F$ must send u to a root of the minimal polynomial of u over K.

From these facts, we see that $\#\,\mathrm{Aut}_K\, K(u)$ does not exceed the number of *distinct* roots of the minimal polynomial of u over K, so cannot exceed the degree of the minimal polynomial of u over K either. Therefore, we have $\#\,\mathrm{Aut}_K\, K(u) \leq [K(u) : K]$.

Proposition 6.1. $\#\,\mathrm{Aut}_K\, K(u) \leq [K(u) : K]$.

Recall that if $\sigma : K \to L$ is a field isomorphism, u is algebraic over K, and v algebraic over L, then σ extends to an isomorphism from $K(u)$ to $L(v)$ if and only if σ maps the minimal polynomial of u over K onto that of v over L.

Example. Find the Galois group of the given extension:

(a) K/K
Solution: $\mathrm{Aut}_K\, K = \{\mathrm{id}\}$, since $[K : K] = 1$. If K/K, then indeed the Galois group is trivial. However, the converse is *false*, as we will see in part (b).

(b) $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$
Solution: We note that $f(x) = x^3 - 2$ is irreducible over $\mathbb{Q}$ (by the rational root theorem), so f is the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$. There are three roots of f: $\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$, with ω being the primitive cube root of unity. Thus we get three isomorphisms:

$$\begin{aligned} \sigma_1 = \mathrm{id} &: \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ \sigma_2 &: \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega \\ \sigma_3 &: \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega^2. \end{aligned}$$

But note that $\sqrt[3]{2}\omega \in \mathbb{Q}(\sqrt[3]{2}\omega)$, and $\mathbb{Q}(\sqrt[3]{2})$ contains the real numbers only. Therefore $\sigma_2 \notin \mathrm{Aut}_{\mathbb{Q}}\,\mathbb{Q}(\sqrt[3]{2})$. Similarly, $\sigma_3 \notin \mathrm{Aut}_{\mathbb{Q}}\,\mathbb{Q}(\sqrt[3]{2})$, since $\sqrt[3]{2}\omega^2 \in \mathbb{Q}(\sqrt[3]{2}\omega^2)$. Thus σ_1 is the only automorphism of $\mathbb{Q}(\sqrt[3]{2})$. Thus $\mathrm{Aut}_{\mathbb{Q}}\,\mathbb{Q}(\sqrt[3]{2}) = \{\mathrm{id}\}$.

(c) $\mathbb{C}/\mathbb{R}$

Solution: Note that $\mathbb{C} = \mathbb{R}(i)$, and that $f(x) = x^2 + 1$ is the minimal polynomial of i over R. So we get two isomorphisms: σ_1 which sends i to i (i.e., the identity), and σ_2 which sends i to $-i$. It's clear that $\mathbb{R}(i) = \mathbb{R}(-i)$, so both σ_1 and σ_2 are $\mathbb{R}$-automorphisms of $\mathbb{C}$. In conclusion, $\mathrm{Aut}_{\mathbb{R}}\,\mathbb{C} \cong \mathbb{Z}/2\mathbb{Z}$.

(d) $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$

Solution: Clearly $f(x) = x^2 - 2$ is the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$. So there are two isomorphisms (namely $\sqrt{2} \mapsto \pm\sqrt{2}$). Thus $\mathrm{Aut}_{\mathbb{Q}}\,\mathbb{Q}(\sqrt{2}) \cong \mathbb{Z}/2\mathbb{Z}$.

(e) $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$

Solution: We need to split up the extension into two pieces, specifically:

$$\begin{array}{c} \mathbb{Q}(\sqrt{2},\sqrt{3}) \\ | \\ \mathbb{Q}(\sqrt{2}) \\ | \\ \mathbb{Q} \end{array}$$

We claim that the minimal polynomial of $\sqrt{3}$ over $\mathbb{Q}(\sqrt{2})$ is indeed $f_{\sqrt{3}}(x) := x^2 - 3$ since $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ (not that hard to see – just prove this by contradiction).

We have isomorphisms

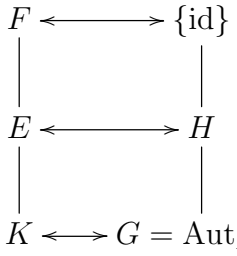
$$\begin{aligned} \sigma_1 : \mathbb{Q}(\sqrt{2}) &\to \mathbb{Q}(\sqrt{2}) \\ \sqrt{2} &\mapsto \sqrt{2} \\ \sigma_2 : \mathbb{Q}(\sqrt{2}) &\to \mathbb{Q}(-\sqrt{2}) = \mathbb{Q}(\sqrt{2}) \\ \sqrt{2} &\mapsto -\sqrt{2}. \end{aligned}$$

Each extends to two maps on $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, Thus $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 2 \cdot 2 = 4$. one sending $\sqrt{3} \mapsto \sqrt{3}$ and the other $\sqrt{3} \mapsto -\sqrt{3}$. So we end up with the four isomorphism maps $\tau_1, \ldots, \tau_4$ such that

$$\begin{array}{llll} \tau_1 : \sqrt{2} \mapsto \sqrt{2} & \tau_2 : \sqrt{2} \mapsto \sqrt{2} & \tau_3 : \sqrt{2} \mapsto -\sqrt{2} & \tau_4 : \sqrt{2} \mapsto -\sqrt{2} \\ \quad \sqrt{3} \mapsto \sqrt{3} & \quad \sqrt{3} \mapsto -\sqrt{3} & \quad \sqrt{3} \mapsto \sqrt{3} & \quad \sqrt{3} \mapsto -\sqrt{3}. \end{array}$$

So $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is the standard basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})\mathbb{Q}$. Note that there are only two groups of order 4 up to isomorphism: $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ (also known as the Klein-four group.) In this case, we see that $\mathrm{ord}\,(\tau_1) = 1$, and $\mathrm{ord}\,(\tau_j) = 2$ for $j = 2, 3, 4$. This means that $\mathrm{Aut}_{\mathbb{Q}}\,\mathbb{Q}(\sqrt{2}.\sqrt{3})$ is not cyclic, so is isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

7. September 18: Galois correspondence



Theorem 7.1. *The following statements hold, regarding the towers of fields and groups above:*

(i) $H' := \{u \in F \mid \sigma(u) = u \text{ for all } \sigma \in H\}$ *is an intermediate subfield of* F/K.
(ii) $E' := \mathrm{Aut}_E F = \{\sigma \in G \mid \sigma(u) = u \text{ for all } u \in E\}$ *is a subgroup of* G.

Proof (sketch). It is clear that H' is a subset of F that contains K and E' is a subset of G. Just verify closure under the appropriate operations. □

So we have $F' = \{\mathrm{id}\}$ and $\{\mathrm{id}\}' = F$. Similarly $K' = G$. However, $G' \supseteq K$ but could be strictly larger.

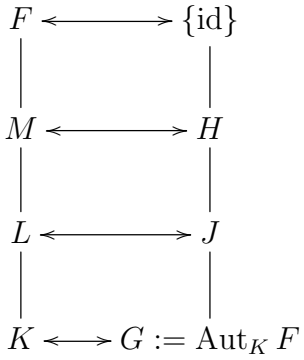
Definition 7.1. F/K is called *Galois* if $G' = K$.

Remark. For any field extension F/K, one can find a subfield $K \subseteq K_0 \subseteq F$ such that F/K_0 is Galois (i.e., $K_0 = G' = \mathrm{Aut}_K F$).

Example. $\mathbb{C}/\mathbb{R}$ is Galois. Previously, we sound that $\mathrm{Aut}_{\mathbb{R}} \mathbb{C} = \{\sigma_1, \sigma_2\}$ where σ_1 is identity on $\mathbb{C}$ and σ_2 is the complex conjugation. If $u \in \mathbb{C} \setminus \mathbb{R}$ then $\sigma_2(u) \neq u$. So no elements outside of $\mathbb{R}$ is fixed by $\mathrm{Aut}_R \mathbb{C}$. Therefore $\mathbb{C}/\mathbb{R}$ is Galois.

Example. $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$ is Galois. If $u = a + b\sqrt{3} \in \mathbb{Q}(\sqrt{3}) \setminus \mathbb{Q}$, then u is *not* fixed by $\mathrm{Aut}_{\mathbb{Q}} \mathbb{Q}(\sqrt{3})$ since $\mathrm{Aut}_{\mathbb{Q}} \mathbb{Q}(\sqrt{3}) = \{\sigma_1, \sigma_2\}$, where σ_1 is the identity and σ_2 sends $a + b\sqrt{3}$ to its conjugate. If $u \notin \mathbb{Q}$ then $b \neq 0$. Therefore $\sigma_2(u) \neq u$, implying that $G' = \mathbb{Q}$. So $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$ is indeed Galois.

Definition 7.2. The dimension $[M : L]$ in the tower of fields below is called the *relative dimension of* L *in* M (or *relative dimension of* M *over* L).



Then the index $[J : H]$ is said to be the *relative index of* H *in* J (or *relative index of* J *over* H).

Theorem 7.2 (Fundamental theorem of Galois theory)**.** *Let F/K be a* finite *Galois extension. Then the maps $E \mapsto E'$ and $H \mapsto H'$ induce a one-to-one, inclusion-reversing correspondence between the set of all intermediate fields of F/K and the set of all subgroups of $G = \mathrm{Aut}_K F$ such that:*

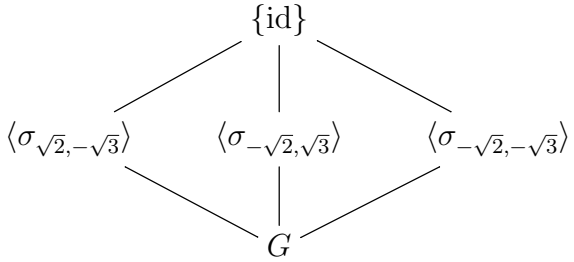
(i) The relative dimension of intermediate fields is equal to the corresponding relative index of subgroups, i.e., $[M : L] = [L' : M']$. In particular, we have $\#G = [G : \{\mathrm{id}\}] = [F : K]$.
(ii) F is automatically Galois over intermediate fields E.
(iii) However, E/K is Galois if and only if E' is a normal subgroup *of G; and in this case, $\mathrm{Aut}_K E \cong G/E'$.*

The proof of this theorem will involve a lot of technicalities, so we will go over some examples first to illustrate this theorem.

Example. We want to show that $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ is Galois, and want to find the lattices of intermediate fields and subgroups that illustrate the fundamental theorem.
Solution: We've already seen that

$$G := \mathrm{Aut}_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{\mathrm{id} = \sigma_{\sqrt{2},\sqrt{3}}, \sigma_{\sqrt{2},-\sqrt{3}}, \sigma_{-\sqrt{2},\sqrt{3}}, \sigma_{-\sqrt{2},\sqrt{3}}\}.$$

So there is one subgroup of order 4, namely G itself. There are three subgroups of order 2, each of which is generated by the remaining three elements of order 2 (besides the identity): $\langle\sigma_{\sqrt{2},-\sqrt{3}}\rangle, \langle\sigma_{-\sqrt{2},\sqrt{3}}\rangle, \langle\sigma_{-\sqrt{2},\sqrt{3}}\rangle$. And there is the trivial subgroup, $\{\mathrm{id}\}$. So the lattice of subgroups look like below.



To see why $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ is Galois, we start by picking $u = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \in \mathbb{Q}(\sqrt{2}, \sqrt{3}) \setminus \mathbb{Q}$, where at least one of $b, c, d \neq 0$. If $b \neq 0$, then $\sigma_{-\sqrt{2},\pm\sqrt{3}}(u) \neq u$; if $c \neq 0$, then $\sigma_{\pm\sqrt{2},-\sqrt{3}}(u) \neq u$. If $d \neq 0$, then $\sigma_{-\sqrt{2},\sqrt{3}}(u) \neq u$ and $\sigma_{\sqrt{2},-\sqrt{3}}(u) \neq u$. Therefore $(\mathrm{Aut}_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}, \sqrt{3}))' = \mathbb{Q}$. Therefore we have a Galois extension.

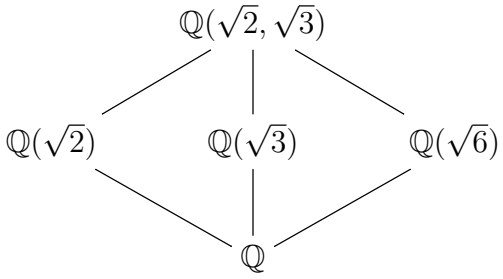
Now we need to find the corresponding fields for each group. Which subfield does the automorphisms in $\langle\sigma_{\sqrt{2},-\sqrt{3}}\rangle$ fix? note that

$$\sigma_{\sqrt{2},-\sqrt{3}}(u) = a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6},$$

so $-c = c$ and $-d = d$, or $c = d = 0$. Thus u is of the form $a + b\sqrt{2}$. Therefore $\langle\sigma_{\sqrt{2},-\sqrt{3}}\rangle' = \mathbb{Q}(\sqrt{2})$. Similarly, we have $\langle\sigma_{-\sqrt{2},\sqrt{3}}\rangle' = \mathbb{Q}(\sqrt{3})$. For the last remaining order-2 subgroup $\langle\sigma_{-\sqrt{2},-\sqrt{3}}\rangle$, note that

$$\sigma_{-\sqrt{2},-\sqrt{3}}(u) = a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6},$$

so $-b = b$ and $-c = c$, or $b = c = 0$. Thus $\langle \sigma_{-\sqrt{2},-\sqrt{3}} \rangle' = \mathbb{Q}(\sqrt{6})$. So the lattice of the subfields looks as follows.



Lemma 7.1. *Let F/K be a field extension (need not be finite; need not be Galois either), and let L, M be intermediate fields of F/K. Similarly, let H, J be subgroups of $\operatorname{Aut}_K F = G$. Then the following are true:*

(i) $F' = \{\mathrm{id}\}, K' = G$
(i') $\{\mathrm{id}\}' = F$ *and* $G' \supseteq K$. *The equality holds if and only if F/K is Galois.*
(ii) $L \subseteq M \Rightarrow L' \geq M$
(ii') $H \leq J \Rightarrow H' \supseteq J'$
(iii) $L \subseteq L''$ *and* $H \leq H''$
(iv) $L' = (L'')'$ *and* $H' = (H'')'$

Proof (sketch). We only need to prove (iv). By (iii), we see that $L' \leq (L')''$, so $L' \leq (L'')'$. But then $L'' \supseteq L$ by (ii), so $(L'')' \leq L'$ by (ii) also. Thus we get the first equality $L' = (L'')'$ as required. The other equality can be proven using a similar technique. □

Definition 7.3. Call an object X (either an intermediate field or a subgroup) *closed* if $X'' = X$.

Remark. F is Galois over K if and only if K is closed.

8. September 21

Theorem 8.1. *Let F be an extension over K. Then there is a one-to-one correspondence between:*

(1) closed intermediate fields of the extension; and
(2) the closed subgroups of the Galois group,

given by $E \mapsto E' = \operatorname{Aut}_E F$.

Proof (sketch). Inverse of the correspondences is given by assigning each subgroup H to its fixed field H'. □

Remark. All "primed" objects are closed.

Remark. To use this theorem, we need to determine which intermediate fields and which subgroups are closed.

Lemma 8.1. *Let F be a field extension of K, and $L \subset M$ intermediate fields. If $[M : L]$ is finite, then $[L' : M'] \leq [M : L]$. In particular, for F/K finite, we have $|\operatorname{Aut}_K F| \leq [F : K]$.*

Proof. Induction on $n := [M : L]$. The base case $[M : L] = 1$ is trivial. now suppose that $n > 1$, and assume that the theorem is true for all $1 \leq i < n$. Now choose $u \in M \setminus L$ which we know we can choose as $[M : L] > 1$. Since $[M : L]$ is finite, u is algebraic over L, with irreducible polynomial, say, $f \in L[x]$ of degree $k > 1$. Then $[L(u) : L] = k$, and $[M : L(u)] = n/k$. Now consider the following tower:

$$\begin{array}{ccc} M & \longleftrightarrow & M' \\ | & & | \\ L(u) & \longleftrightarrow & L(u)' \\ | & & | \\ L & \longleftrightarrow & L' \end{array}$$

Now we have two cases:

(1) $k < n$. Then $1 < n/k < n$, so by the induction hypothesis $[L' : L(u)'] \leq k$ and $[L(u)' : M'] \leq n/k$. Hence

$$[L' : M'] = [L' : L(u)'][L(u)' : M'] \leq k \cdot \frac{n}{k} = n = [M : L].$$

(2) $k = n$. Then $[M : L(u)] = 1$, so $M = L(u)$.

For now, we shall assume that there is an injective map from the set of all left cosets of M' in L' (call this set S) to the set of all distinct roots (in F) of $f \in L[x]$ (call this set T). We will prove this claim afterwards, as Lemma 8.2. By Lemma 8.2, we have $|S| \leq |T|$. It is also known that $|T| \leq n$ and $|S| = [L' : M']$ (by definition). Hence $[L' : M'] \leq |T| \leq n = [M : L]$. This implies that the final statement of Theorem 8.1 (with $L = K$ and $M = F$, since $|\operatorname{Aut}_K F| = [\operatorname{Aut}_K F : 1] = [K' : F'] \leq [F : K]$. □

Lemma 8.2. *Let M, L, M', L' be the same as in Lemma 8.1. Then there is an injective map from the set*

$$S := \{\textit{all left cosets of } M' \textit{ in } L'\}$$

to the set

$$T := \{\textit{all distinct roots (in } F\textit{) of } f \in L[x]\}.$$

Proof. Let $\tau M'$ be a left coset of M' in L'. If $\sigma \in M' = \operatorname{Aut}_M F$, then since $u \in M$ we have $\tau(\sigma(u)) = \tau(u)$. Hence every element of the coset $\tau M'$ has the same effect on u (namely, $u \mapsto \tau(u)$).

Since $\tau \in L' = \operatorname{Aut}_L F.$, and u is a root of $f \in L[x]$, it follows that $\tau(u)$ is a root of f also (Theorem 2.2 in Hungerford). Hence, the map $S \to T$ given by $\tau M' \mapsto \tau(u)$ is well-defined.

It still remains to show that it is injective. Suppose that $\tau(u) = \tau_0(u)$ where $\tau, \tau_0 \in L'$. Then $\tau_0^{-1}\tau(u) = u$, so $\tau_0^{-1}\tau$ fixes u. Hence $\tau_0^{-1}\tau$ fixes $L(u) = M$ element-wise (Theorem 1.6(iv) in Hungerford), and so $\tau_0^{-1}\tau \in M'$. So $\tau_0 M' = \tau M'$, as required. □

9. September 25

Lemma 9.1 (The subgroup counterpart for Lemma 8.1)**.** *Let F be a field extension of K, and let $H \leq J$ be subgroups of $\operatorname{Aut}_K F$. If $[J : H]$ is finite, then $[H' : J'] \leq [J : H]$.*

Proof. We will prove this by contradiction. So suppose that $[J : H] = n$ is finite but that $[H' : J'] > n$. Then we can find a J'-independent subset, say $\{u_1, \ldots, u_{n+1}\}$ of H'. Now let $\{\tau_1, \ldots, \tau_n\}$ be a complete set of representatives for the cosets of H in J (i.e., $J = \bigsqcup_{i=1}^{n} \tau_i H$). Now consider the linear system

$$[\tau_i(u_j)]_{\substack{1 \le i \le n \\ 1 \le j \le n+1}} \tilde{x} = \tilde{0}.$$

This system has a nontrivial system, as there are more columns than rows. So let a nontrivial solution be $x_1 = a_1, \ldots, x_r = a_r$, and $x_{r+1} = \cdots = x_{n+1} = 0$ having the least number of non-zero components. We will now show that, under the given circumstances, it is possible to come up with another nontrivial solution that has fewer than r non-zero components. Then Exactly one of the $\tau_i H$ is H; say $\tau_1 H = H$, without loss of generality. Then $\tau_1 \in H$, so τ_1 fixes all elements of H'. Hence $\tau_1(u_j) = u_j$ for all j. So the first equation is reduced into $u_1 a_1 + \cdots + u_r a_r = 0$. Since $\{u_1, \ldots, u_{n+1}\}$ is linearly independent over J', it follows that $a_j \notin J'$ for some j. Let a_2 be such element. Since we can scale solutions, we can assume that $a_1 = 1$. Since $a_2 \notin J'$, for some $\sigma \in J$ we have $\sigma(a_2) \neq a_2$. Note also that $\{\sigma\tau_1, \ldots, \sigma\tau_n\}$ is also a complete set of representatives for H in J, and the system $[\sigma\tau_i(u_j)]\tilde{x} = \tilde{0}$ is just the original system (with equations put in a different order, possibly). But then $x_1 = \sigma(a_1), \ldots, x_r = \sigma(a_r)$, and $x_{r+1} = \cdots = x_{n+1} = \sigma(0) = 0$ is a solution to this system. But then the difference of our two solutions is also a solution. Therefore, $(1-1, a_2 - \sigma(a_2), \ldots, a_r - \sigma(a_r), 0, \ldots, 0) = (0, a_2 - \sigma(a_2), a_3 - \sigma(a_3), \ldots, a_r - \sigma(a_r), 0, \ldots, 0)$ is another solution. But note that $a_2 - \sigma(a_2) \neq 0$. Thus, this is a nontrivial solution that has more zero components than our initial solution, thereby contradicting the minimality assumption. □

Lemma 9.2. *Let F/K be an extension, $L \le M$ intermediate fields, and $H \le J$ subgroups of $\mathrm{Aut}_K F$.*

(i) If L is closed and $[M : L]$ finite, then M is closed and $[L' : M'] = [M : L]$.
(ii) If H is closed and $[J : H]$ finite, then J is closed and $[H' : J'] = [J : H]$.
(iii) Let F/K be finite and Galois. Then all intermediate fields E and all subgroups H are closed. Also, we have $\#\,\mathrm{Aut}_K F = [F : K]$.

Proof. (i) Let L be closed and $[M : L] < \infty$. Recall that $[L' : M'] \le [M : L]$ and $[M'' : L''] \le [L' : M']$. But since $M \subseteq M''$, it follows $[M : L] \le [M'' : L]$. But then L is closed, so $L'' = L$. Hence $[M : L] \le [M'' : L] = [M'' : L''] \le [L' : M'] \le [M : L]$, so this string of inequality actually has equality throughout. But since $L \subseteq M \subseteq M''$ and $[M : L] = [M'' : L]$, it follows $M = M''$. Thus M is closed. (ii) can be proven as similarly (or, refer to the textbook).

(iii) Let F/K be Galois and finite, and E an intermediate field. Since K is closed (as F/K Galois) and $[E : K]$ is finite (as F/K is finite), from part (i) it follows that E is closed. Also, by (i) we have $\#\,\mathrm{Aut}_K F = [F : K]$ is finite. Similarly, each subgroup H is finite. So $[H : \{\mathrm{id}\}]$ is finite; hence by part (ii), H is closed (since $\{\mathrm{id}\}$ is evidently closed). □

Remark. At this point, we finished proving the first half of Theorem 7.2.

10. September 27

Today, we want to prove that whenever F/K is Galois (let $K \subseteq E \subseteq F$ be a tower of extensions), so is F/E. However, the same cannot be said about E/K. In fact, E/K is Galois if and only if $E' \trianglelefteq G$. Particularly, in this case, $\operatorname{Aut}_K E \cong G/E'$.

Definition 10.1. E is *stable* if every $\sigma \in \operatorname{Aut}_K F$ maps E to itself.

Remark. If E is stable, then $\sigma|_E \in \operatorname{Aut}_K E$ for all $\sigma \in \operatorname{Aut}_K F$; furthermore, both σ and σ^{-1} map E onto itself.

Lemma 10.1. *Let F/K be any field extension. Then the following are true.*

(i) If E is stable, then $E' \trianglelefteq G$.
(ii) if $H \trianglelefteq G$, then H' is stable.

Proof. (i) Suppose $\tau \in E'$. Then $\tau(u) = u$ for all $u \in E$. Since E is stable, so if $u \in E$ then $\sigma(u) \in E$. Hence $\tau\sigma(u) = \sigma(u)$, or equivalently $\sigma^{-1}\tau\sigma(u) = u$. Therefore $\sigma^{-1}\tau\sigma \in E'$, so indeed $E' \trianglelefteq G$, as required.

(ii) let $H \trianglelefteq G = \operatorname{Aut}_K F$. We need to show that H' is stable, i.e., for any $\sigma \in G$ and $u \in H'$, we need to show $\sigma(u) \in H'$. In other words, we need to show that $\tau\sigma(u) = \sigma(u)$ for all $\tau \in H$. But this holds – since $H \trianglelefteq G$, we see that $\sigma^{-1}\tau\sigma \in H$. So $\sigma^{-1}\tau\sigma(u) = u$ for all $u \in H'$. This completes the proof. □

Lemma 10.2. *Let F/K be Galois, and E be stable, where $K \subseteq E \subseteq F$ is a tower of field extensions. Then E/K is Galois.*

Proof. Let $u \in E \setminus K$. We need to show that $\tau(u) \neq u$ for some $\tau \in \operatorname{Aut}_K E$. Since F/K is Galois, indeed $\sigma(u) \neq u$ for some $\sigma \in \operatorname{Aut}_K F$. Since E is stable, we have $\sigma|_E \in \operatorname{Aut}_K E$. From this $\sigma|_E(u) \neq u$. Thus E/K is Galois. □

Lemma 10.3. *Let F/K be any field extension. E be a subextension that is both algebraic and Galois over K. Then E is stable.*

Proof. Let $u \in E$, and let $f(x) \in K[x]$ be a minimal polynomial of u over K. Let $u = u_1, u_2, \ldots, u_r$ be the distinct roots of f that lie in E. If $\tau \in \operatorname{Aut}_K E$, then τ permutes the roots of f. So let $g(x) = (x-u_1)(x-u_2)\cdots(x-u_r)$. The coefficients on g are the elementary symmetric functions in $u_1, \ldots, u_r$. So the coefficients are fixed by $\operatorname{Aut}_K E$. But then since E/K is Galois, it follows that the coefficients all lie in K.

But then $\deg g \leq \deg f$, so $g = f$ – since f is the minimal polynomial over u over K. Finally, for $\sigma \in \operatorname{Aut}_K F$, we see that $\sigma(u) \in E$ since $\sigma(u)$ is a root of g and *all* roots of G lie in E. Therefore E is stable, as required. □

Definition 10.2. Let $K \subseteq E \subseteq F$ be a tower of field extensions. Then $\tau \in \operatorname{Aut}_K E$ is *extendible to* F if $\tau = \sigma|_E$ for some $\sigma \in \operatorname{Aut}_K F$.

Proposition 10.1. *The set of extendible automorphisms in $\operatorname{Aut}_K E$ is a subgroup of $\operatorname{Aut}_K E$. Furthermore, if E is stable, then $E' = \operatorname{Aut}_E F \trianglelefteq G$. Therefore G/E' is defined.*

Lemma 10.4. *Let F/K be any extension, and $K \subseteq E \subseteq F$ a tower of extensions, where E is stable. Also, let Z be the set of extendible automorphisms in $\operatorname{Aut}_K E$. Then $G/E' \cong Z$.*

Proof. Consider the map $\varphi : G \to \operatorname{Aut}_K E$ where $\sigma \mapsto \sigma|_E$. Since E is stable, the map φ is a well-defined homomorphism with image Z and kernel E'. The claim now easily follows from the first isomorphism theorem. □

Now we are ready to prove the remaining parts of the fundamental theorem (Theorem 7.2):

Theorem 7.2 (Fundamental theorem of Galois theory)**.** *Let F/K be a* finite *Galois extension. Then the maps $E \mapsto E'$ and $H \mapsto H'$ induce a one-to-one, inclusion-reversing correspondence between the set of all intermediate fields of F/K and the set of all subgroups of $G = \operatorname{Aut}_K F$ such that:*

(i) The relative dimension of intermediate fields is equal to the corresponding relative index of subgroups, i.e., $[M : L] = [L' : M']$. In particular, we have $\#G = [G : \{\mathrm{id}\}] = [F : K]$.
(ii) F is automatically Galois over intermediate fields E.
(iii) However, E/K is Galois if and only if E' is a normal subgroup *of G; and in this case, $\operatorname{Aut}_K E \cong G/E'$.*

Proof of Theorem 7.2. First we will prove that F/E is Galois. First, let $u \in F$ that is fixed by e'. Then $u \in E' = E$ since all intermediate fields are closed. Therefore F/E is Galois. Second, we will prove the property regarding E/K being Galois. If E/K is Galois, then E/K is finite, so E/K is algebraic over K. Now recall that then E is stable, so $E' \trianglelefteq \operatorname{Aut}_K F$ as required. Conversely, assume $E' \trianglelefteq G$. Then E'' is stable. But since E is closed, we see $E'' = E$. So E is stable. Thus E/K is Galois.

Finally, note that

$$\#G/E' = [G : E'] = [E'' : G] = [E : K] = \operatorname{Aut}_K E,$$

which is enough to show that the set of extendible automorphisms in $\operatorname{Aut}_K E$ is in fact a subgroup of $\operatorname{Aut}_K E$ having the same finite size, so these two sets are in fact equal. Therefore $G/E' \cong \operatorname{Aut}_K E$ as required. □

Theorem 10.1. *Let F be a field, and G be any group of automorphism of F. Then F is Galois over the fixed field K of G. Furthermore, if G is finite, then F/K is a finite Galois extension whose Galois group is G.*

11. September 28

Definition 11.1. Let K be a field, and $f \in K[x]$ a non-constant polynomial. Then f *splits over* K if $f(x) = (x - u_1)(x - u_2)(x - u_3) \cdots (x - u_n)$ for some $u_1, u_2, \ldots, u_n \in K$.

Definition 11.2. F is a *splitting field of S over K*, for a subset S of $K[x]$ if:

- every polynomial in S splits in F.
- $F = K(U)$ where U is the set of all roots of all polynomials in S that lie in F.

Intuitively, the splitting field over K for some polynomials in $K[x]$ is equal to the smallest extension of K containing all roots of all polynomials in S.

Example. $\mathbb{Q}(\sqrt{2})$ is a splitting field extension for $x^2 - 2$ over $\mathbb{Q}$ since $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\pm\sqrt{2})$. Similarly, $\mathbb{C} = \mathbb{R}(i) = \mathbb{R}(i, -i)$ is a splitting field extension of x^2+1 ovecr $\mathbb{R}$ since $\mathbb{C} = \mathbb{R}(\pm i)$.

Example. However, $\mathbb{Q}(\sqrt[3]{2})$ is *not* a splitting field extension of x^3-2 over $\mathbb{Q}$ since the complex roots $\sqrt[3]{2}\zeta$ and $\sqrt[3]{2}\zeta^2$ where $\zeta := e^{2\pi i/3}$ do not lie in $\mathbb{Q}(\sqrt[3]{2})$.

Remark. Splitting fields over K are algebraic over K. They are in fact finite for finitely many polynomials.

Remark. If $S = \{f_1, \ldots, f_n\}$ is a finite set of polynomials in $K[x]$, then a splitting field extension for $\{f_1, \ldots, f_n\}$ over K will coincide with a splitting field extension of the single polynomial $f := f_1 f_2 \ldots f_n$. Therefore, we only need to study the cases of a single polynomial or infinitely many polynomials.

Remark. Every set of polynomials S in $K[x]$ has a splitting field extension. Also, splitting field extensions for a given set are unique up to a K-isomorphism (hence *the* splitting field of...).

Theorem 11.1. *Let K be a field and $f \in K[x]$ a polynomial of degree $n \geq 1$. Then f has a splitting field extension F/K of degree $[F : K] \leq n!$.*

Proof. We will prove via induction on n. If $n = 1$, then $F = K$ is (trivially) the splitting field extension of f over K of degree $[K : K] = 1 \leq 1!$. Fix $l \geq 1$, and suppose that the result holds for all polynomials in $K[x]$ of degree l. Let $f(x)$ have degree $(l + 1)$.

Case I. f splits over K. In this case $F = K$ is a splitting field, so $[F : K] = [K : K] = 1 \leq (l + 1)!$.

Case II. f has an irreducible factor $g \in K[x]$ with degree $\deg g \geq 2$. Then there is a simple extension $K(u)/K$ of degree $[K(u) : K] = \deg g \geq 2$, where u is a root of g, and so a root of f. So $f(x) = (x - u)h(x)$ for some $h(x) \in K(u)[x]$ of degree l. By the inductive hypothesis, h has a splitting field extension over $K(u)$ of degree $\leq l!$. Say $F/K(u)$.

Now we claim that F is a splitting field extension of f over K of degree $[F : K] \leq (l + 1)!$. This is not that hard to see considering the tower below.

$$\begin{array}{c} F \\ \Big| \leq l! \\ K(u) \\ \Big| \deg g \\ K \end{array}$$

Since $F = K(u)(\text{all roots of } h) = K(\text{all roots of } f)$, it follows that F/K is a splitting field extension of f. Finally,

$$[F : K] = [F : K(u)][K(u) : K] = [F : K(u)] \deg g \leq l! \deg g = l!(l + 1) = (l + 1)!.$$

So the result follows by induction. □

Clearly, infinite case is much harder. It is hard to show in general that there is a field containing the roots of infinitely many polynomials.

Theorem 11.2. *Let F be any field. Then the following are equivalent:*

(i) Every non-constant polynomial $f \in F[x]$ has a root in F.

(ii) Every non-constant $f \in F[x]$ splits over F.
(iii) Every irreducible $f \in F[x]$ has degree one.
(iv) F has no proper field extensions.
(v) F is algebraic over a field K for which every $f \in K[x]$ splits over F.

Proof (sketch). ((i) $\Rightarrow$ (ii)) Exercise.
((ii) $\Rightarrow$ (iii)) Exercise.
((iii) $\Rightarrow$ (iv)) Assume that every irreducible $f \in F[x]$ has degree 1. If L/F is an algebraic extension and $u \in L$, then the min polynomial of u ovre F has degree 1. So $u \in F$.
((iv) $\Rightarrow$ (v)) Exercise.
((v) $\Rightarrow$ (i)) If $f \in F[x]$ has u as a root, then the minimal polynomial of u over K in $K[x]$, then u as well as all the roots lies in F. $\square$

Definition 11.3. If F satisfies these equivalent conditions outlines in Theorem 11.2, then F is said to be *algebraically closed*.

Theorem 11.3. *Let F/K be any field extension. Then the following are equivalent:*

(i) F/K is algebraic, and F is algebraically closed.
(ii) F is a splitting field extension over K for the set of all non-constant polynomials in $K[x]$.

Definition 11.4. An extension F of K is an *algebraic closure* of K if it satisfies the equivalent conditions listed in Theorem 11.3.

Theorem 11.4. *Every field K has an algebraic closure, and any two such fields are K-isomorphic.*

Corollary 11.1. *Every set S of non-constant polynomials in $K[x]$ has a splitting field extension.*

Proof (sketch). We will only cover the finite case. Note that constructing a splitting field for $\{f_1, \dots, f_n\}$ is equivalent to constructing one for $f := f_1 f_2 \dots f_n$. If $u_1, \dots, u_r$ are all of the roots in an algebraic closure, then $K(u_1, \dots, u_r)$ is a splitting field. $\square$

Theorem 11.5 (Uniqueness of a splitting field extension)**.** *Let F be a splitting field of $S = \{f_i\} \subseteq K[x]$ and M a splitting field of $S' = \{\sigma f_i\} \subseteq L[x]$. Then there is an extension $\overline{\sigma} : F \to M$ which is an isomorphism so that $\overline{\sigma}|_K = \sigma$.*

$$\begin{array}{ccc} F & \xrightarrow{\overline{\sigma}} & M \\ | & & | \\ K & \xrightarrow[\sigma]{\simeq} & L \end{array}$$

Proof (sketch). For finite S and S', one can further reduce it to $S = \{f\}$ and $S' = \{\sigma f\}$ as we did in the proof of Corollary 11.1. So let roots of f be $u_1, \dots, u_n$, and roots of σf be $\sigma(u_1), \dots, \sigma(u_n)$. By a previous result, we see that σ extends to an isomorphism

$\sigma_i : K(u_1, \ldots, u_i) \to L(\sigma(u_1), \ldots, \sigma(u_i))$.

$$\begin{array}{ccc}
F = K(u_1, \ldots, u_n) & \xrightarrow[\sigma_n]{\simeq} & M = L(\sigma(u_1), \ldots, \sigma(u_n)) \\
\big| & & \big| \\
K(u_1, \ldots, u_{n-1}) & \xrightarrow[\sigma_{n-1}]{\simeq} & L(\sigma(u_1), \ldots, \sigma(u_{n-1})) \\
\big| & & \big| \\
\vdots & & \vdots \\
\big| & & \big| \\
K(u_1) & \xrightarrow[\sigma_1]{\simeq} & L(\sigma(u_1)) \\
\big| & & \big| \\
K & \xrightarrow[\sigma]{\simeq} & L
\end{array}$$

Now consider the special case $K = L$ and $\sigma = \mathrm{id}$. Then any two splitting fields of a set S of polynomials in $K[x]$ are K-isomorphic. In particular, any two algebraic closure of K are K-isomorphic. □

Remark. Any automorphism of K can be extended to the splitting field extension of K.

12. October 2: Galois extensions as splitting fields

Definition 12.1. Let K be any field, and let $f \in K[x]$ be a non-zero polynomial, and let c be a root of f. Then $f(x) = (x - c)^m g(x)$ where $g(x) \neq 0$ and $m \in \mathbb{N}$. Then c is a *simple root* (resp. *multiple root*) if $m = 1$ (resp. $m > 1$).

Definition 12.2. Let $f \in K[x]$ be irreducible.

(i) f is *separable* if f has only simple roots.
(ii) If F/K is a field extension, and $u \in F$ is algebraic, then u is *separable over* K if its minimal polynomial over K is separable.
(iii) F/K is separable if every $u \in F$ is separable over K.

Remark.
- If f is separable, then f has no repeated roots in *any* splitting field extension.
- An irreducible polynomial $f \in K[x]$ is separable if and only if the derivative of f is non-zero. Particularly, in characteristic zero, *all* non-constant irreducible polynomials are separable.
- In characteristic zero, *all* algebraic extensions are separable.

13. October 4

Theorem 13.1. *Let F/K be a field extension. Then the following are equivalent:*

(i) F/K is Galois and algebraic.
(ii) F/K is separable, and F is the splitting field extension of some set S of polynomials in $K[x]$.
(iii) F is the splitting field of some set T of separable polynomials in $K[x]$.

Remark. Theorem 13.1 implies that algebraic Galois extensions are splitting fields of separable polynomials. So one can rephrase the "splitting field" part and arrive at our intuitive idea of Galois: the isomorphisms you get for free all end up being automorphisms.

Definition 13.1. Let F/K be algebraic. Then F is *normal* over K if every irreducible $f \in K[x]$ that has a root in F actually splits over F.

Theorem 13.2. *Let F/K be algebraic. Then the following are equivalent:*

(1) F/K is normal.
(2) F is a splitting field over K for some sets of polynomials in $K[x]$.
(3) Every K-embedding/monomorphism from F into an algebraic closure $\overline{K}$ of K is actually an automorphism of F.

Proof. ((i) $\Rightarrow$ (ii)) Assume that F/K is normal. Let $\{u_i\}_{i\in I}$ be a K-basis for F. Then F is the splitting field extension over K of the set of all minimal polynomials of the u_i. Each minimal polynomial has a root in F (namely, one of the basis elements). But since F is normal, F contains *all* roots of *all* minimal polynomials. F is the smallest algebraic extension of K containing these elements, so this completes this direction.

((ii) $\Rightarrow$ (iii)) Assume that F is the splitting field extension over K of some set of polynomials in $K[x]$. So $F = K(\{u_i\}_{i\in I})$ for certain u_i that constitute *all* roots of the polynomials in question. Assume $\sigma : F \to \overline{K}$ is some K-monomorphism. Then σ permutes $\{u_i\}_{i\in I}$. Thus $\sigma : K(\{u_i\}_{i\in I}) \to K(\{u_i\}_{i\in I})$ where $F = K(\{u_i\}_{i\in I})$ is the image. Thus σ is in fact a K-automorphism of F.

((iii) $\Rightarrow$ (i)) Assume that every $\sigma : F \to \overline{K}$ over K is a K-automorphism of F (i.e., $\operatorname{im}\sigma = F$). Suppose that $f \in K[x]$ is irreducible and has a root $u \in F$. Let v be any root of f such that $\sigma(u) = v$.

$$\begin{array}{ccc}
\overline{K} & \xrightarrow{\overline{\sigma}} & \overline{K} \\
| & & | \\
F & \xrightarrow{\overline{\sigma}|_F} & \overline{K} \\
| & & | \\
K(u) & \xrightarrow{\sigma} & K(v) \\
| & & | \\
K & \xrightarrow{\text{id}} & K
\end{array}$$

We have a K-isomorphism $\sigma : K(u) \to K(v)$ where $u \mapsto v$. Also since $\overline{K}/K$ is a splitting field, so is $\overline{K}/K(u)$ since $\overline{K}$ is an algebraic closure of $K(u)$. So σ has an extension $\overline{\sigma} : \overline{K} \to \overline{K}$. But then $\overline{\sigma}|_F : F \to \overline{K}$ is a monomorphism over K, so $\operatorname{im}\overline{\sigma}|_F = F$. Thus $v = \sigma(u) = \overline{\sigma}|_F \in F$. □

Corollary 13.1. *Let F/K be algebraic, Then F/K is Galois if and only if F/K is separable and normal. Specifically, if K has characteristic 0, then F/K is Galois if and only if F/K is normal.*

Theorem 13.3. *Let E/K be algebraic. Then there is an extension F of E such that:*

(i) F/K is normal;

(ii) no intermediate field of F and K is normal over K;
(iii) if E/K is separable, then F/K is Galois; and
(iv) if E/K is finite, then F/K is finite also.

Example. $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not normal since the complex roots of the $\mathbb{Q}$-minimal polynomial of $\sqrt[4]{2}$ are not contained in $\mathbb{Q}(\sqrt[4]{2})$. So the normal closure is $\mathbb{Q}(\sqrt[4]{2}, -\sqrt[4]{2}, \sqrt[4]{2}i, -\sqrt[4]{2}i) = \mathbb{Q}(\sqrt[4]{2}, i)$.

14. October 5: Fundamental theorem of algebra

Some required background materials:

(1) Analytic
  (a) Every positive real number has a positive square root.
  (b) Every odd degree polynomial in $\mathbb{R}[x]$ has a root in $\mathbb{R}$.
(2) Algebraic (Sylow)
  (a) If G is a finite group of order $p^n m$ for $n \geq 1$ and m relatively prime to p. Then G has subgroups of order p^j for all $0 \leq j \leq n$.

Lemma 14.1. *Let K be an infinite field, and F/K be a finite separable extension. Then $F = K(u)$ for some $u \in F$, i.e., F/K is simple.*

Proof. Let F_1/K be a normal closure of F/K. Then F_1/K is finite Galois. So $\mathrm{Aut}_K F_1$ is finite, which implies that $\mathrm{Aut}_K F_1$ has finitely many subgroups. By correspondence, only finitely many fields are intermediate to F_1 and K. So only finitely many intermediate fields of F and K. So we choose an intermediate field $K(u)$ that is maximal. Now suppose that $K(u) \subsetneq F$. Let $v \in F \setminus K(u)$. Consider fields of the form $K(u+av)$ where $a \in K$. Since there are only finitely many of these and K is infinite, we must have $K(u+av) = K(u+bv)$ for $a, b \in K$ and $a \neq b$. Thus $(u+av)-(u+bv) = (a-b)v \in K(u+av)$. Since $a-b \neq 0$, indeed $v \in K(u+av)$. Also, $u = (u+av)-av$, so $u \in K(u+av)$ as well. Hence, $K(u) \subsetneq K(u+av)$. But this contradicts the maximality of $K(u)$, so $F = K(u)$. □

Lemma 14.2. $\mathbb{C}$ *has no extensions of degree* 2.

Proof. Suppose that $E/\mathbb{C}$ is of degree 2. Then by Lemma 14.1, there is $u \in E$ such that $E = \mathbb{C}(u)$, and the minimal polynomial of u over $\mathbb{C}$ is of the form $f_u(x) = x^2 + sx + t$ for $s, t \, in \mathbb{C}$. The quadratic formula says

$$u = \frac{-s \pm \sqrt{s^2 - 4t}}{2}.$$

Thus $E = \mathbb{C}(-s \pm \sqrt{s^2-4t}) = \mathbb{C}(\sqrt{s^2-4t}) = \mathbb{C}(\sqrt{\alpha})$ for some $\alpha \in \mathbb{C}$. So we are done once we prove that $\sqrt{\alpha} \in \mathbb{C}$ for all $\alpha \in \mathbb{C}$. Solve for c and d where $(c+di)^2 = a+bi$. We can conclude $c, d \in \mathbb{R}$ since positive reals have positive square roots. So $c+di \in \mathbb{C}$. This gives us the desired contradiction. □

Theorem 14.1 (Fundamental theorem of algebra)**.** $\mathbb{C}$ *is algebraically closed.*

Proof. Suppose that $E_1/\mathbb{C}$ is a finite extension. Then $E_1/\mathbb{R}$ is a finite extension of even degree. So let $F/\mathbb{R}$ be a normal closure of $E_1/\mathbb{R}$, and $G := \mathrm{Aut}_{\mathbb{R}} F$. We prove that $E_1 = \mathbb{C}$ by showing that, in fact, $F = \mathbb{C}$. Let $\#G = 2^n m$ for some $n \geq 1$ and m odd (since

$\#G = [\#G : \{\mathrm{id}\}] = [F : \mathbb{R}] = [F : \mathbb{C}][\mathbb{C} : \mathbb{R}] = [F : \mathbb{C}] \cdot 2)$. Let $H \leq G$ such that $\#H = 2^n$, and let $E = H'$ (i.e., the intermediate field fixed by H).

$$\begin{array}{ccc} F & \longleftrightarrow & \{\mathrm{id}\} \\ {\scriptstyle 2^n}\big| & & \big| \\ E & \longleftrightarrow & H \\ {\scriptstyle m}\big| & & \big| \\ \mathbb{R} & \longleftrightarrow & G \end{array}$$

So $F/\mathbb{R}$ is finite Galois. Note that for some $u \in E$, we have $E = \mathbb{R}(u)$; and the minimal polynomial of u over $\mathbb{R}$ has odd degree m. Irreducibility implies that $m = 1$, since otherwise it will be reducible (since every odd-degree polynomial over the reals has at least one real root). Hence $E = \mathbb{R}$, so $\#G = 2^n$ for some $n \geq 1$.

$$\begin{array}{ccc} F & \longleftrightarrow & \{\mathrm{id}\} \\ \big| & & \big| \\ J' & \longleftrightarrow & J \\ {\scriptstyle 2}\big| & & \big|{\scriptstyle 2} \\ \mathbb{C} & \longleftrightarrow & \mathrm{Aut}_{\mathbb{C}} F \end{array}$$

Therefore $\mathrm{Aut}_{\mathbb{C}} F$ has order 2^l for some $0 \leq l \leq n$, since it is a subgroup of $G = \mathrm{Aut}_{\mathbb{R}} F$. Now, if $l > 0$, then choose subgroup J of $\mathrm{Aut}_{\mathbb{C}} F$ of index 2. This means that J' is a degree 2 extension of $\mathbb{C}$, but this contradicts Lemma 14.2. This means $l = 0$. Hence indeed $[F : \mathbb{C}] = 2^0 = 1$, so $F = \mathbb{C}$. □

15. October 4: the Galois group of a polynomial

Definition 15.1. Let K be a field. Then the *Galois group of* $f \in K[x]$ is the group $\mathrm{Aut}_K F$ where F is some splitting field of f over K.

Definition 15.2. Let S_n be the group of permutation on $\{1, 2, \ldots, n\}$. Then a subgroup G of S_n is *transitive* if for any $1 \leq i \neq j \leq n$, there is $\sigma \in G$ with $\sigma(i) = j$.

Theorem 15.1. *Let K be a field, and G be the Galois group of $f \in K[x]$.*

(i) G is isomorphic to a subgroup of S_n, for some n.

(ii) If f is separable of degree n, then $n \,|\, \#G$, and G is isomorphic to a transitive subgroup of S_n.

Proof (sketch). (i) Assignment #3, Problem #1.

(ii) If f is separable, then F/K is Galois, where F is the splitting field of f over K. If u is a root of f, then under Galois correspondence, there is a subgroup of index n (namely the subgroup of K-automorphisms fixing $K(u)$). Thus $n \,|\, \#G$. □

Now we can determine the Galois groups of polynomials of degrees 1, 2, 3, 4.

Proposition 15.1. *Let $f \in K[x]$ be irreducible over K. If $\deg f = 1$, then $G = \mathrm{Aut}_K K = \{\mathrm{id}\}$. If $\deg f = 2$, then $G = \{\mathrm{id}\}$ if f is not separable; if f is separable, then $G \cong \mathbb{Z}/2\mathbb{Z}$.*

Proof. The degree 1 case readily follows. If $u \neq v$ are the distinct roots of f, then $\operatorname{Aut}_K F = \{\sigma_1 = \mathrm{id}, \sigma_2\}$ where $\sigma_2 : u \mapsto v$. If $u = v$ then $\sigma_2 = \sigma_1$, so the claim follows. □

Proposition 15.2. *If $f \in K[x]$ is irreducible over K, is separable, and is of degree 3, then the Galois group of f is isomorphic to either one of A_3 or S_3.*

Proof. Suppose that $\deg f = 3$, and f is separable over K. then F/K is Galois as F is the splitting field of a separable polynomial f. Since the only transitive groups of S_3 are A_3 and S_3, then the Galois group of separable cubic polynomials must be one of A_3 or S_3. □

To determine whether G is isomorphic to A_3 or S_3, we need to compute the discriminant of f.

Definition 15.3. Let K be a field with $\operatorname{char} K \neq 2$, and let $f \in K[x]$ be irreducible over K and of degree n, with distinct roots $u_1, \ldots, u_n \in F$. Then the *discriminant of f* is

$$D = \Delta^2,$$

where

$$\Delta := \prod_{i<j} (u_i - u_j) \in F.$$

Proposition 15.3. *Let D and Δ be defined as above.*

(i) $D = \Delta^2 \in K$.

(ii) Suppose $\sigma \in \operatorname{Aut}_K F \leq S_n$. Then σ is even (resp. odd) if and only if $\sigma(\Delta) = \Delta$ (resp. $\sigma(\Delta) = -\Delta$).

Proof (sketch). (ii) σ can be viewed as a permutation of the u_j, so it can be viewed as a product of transpositions. And each transposition reverses the order of some factor $u_i - u_j$. Thus it introduces a minus sign into the product. Thus σ is odd if and only if there is an odd number of switches (as there is an odd number of minus signs introduced in the product), so this is equivalent to $\sigma(\Delta) = -\Delta$.

(i) For any $\sigma \in \operatorname{Aut}_K F$, we have

$$\sigma(D) = \sigma(\Delta^2) = \sigma(\Delta)^2 = (\pm\Delta)^2 = \Delta^2 = D,$$

so $D \in K$. □

Corollary 15.1. *In the Galois correspondence, the intermediate field $K(\Delta)$ corresponds to $G \cap A_n$. In particular, $G \leq A_n$ if and only if $\Delta \in K$.*

Proof. We know that $\sigma \in A_n$ is equivalent to $\sigma(\Delta) = \Delta$. The claim follows upon noting that $K(\Delta)$ is the fixed field of $G \cap A_n$. □

Corollary 15.2. *Let $f \in K[x]$ be separable and $\deg f = 3$. Then G is isomorphic to A_3 or S_3. If $\operatorname{char} K \neq 2$, then $G = A_3$ if and only if $\Delta \in K$.*

Proposition 15.4. *Let $\operatorname{char} K \neq 2, 3$, and let $f(x) = x^3 + bx^2 + cx + d \in K[x]$ be separable. Then $g(x) = f(x - \frac{b}{3})$ has the form $x^3 + px + q$. This polynomial has discriminant of the form $-4p^3 - 27q^2$.*

Proof. If u is a root of f, then $u + b/3$ is a root of g. But the factors in the definition of Δ are the same since, for roots u_i and u_j we have $u_i - u_j = (u_i + b/3) - (u_j + b/3)$. Thus f and g have the same Δ, hence D. □

Example. Let $f = x^3 - 3x + 1 \in \mathbb{Q}[x]$. Then ± 1 are not roots, so by the rational root theorem, f is irreducible. Since $\operatorname{char} \mathbb{Q} = 0$, f is separable. Compute the discriminant: $D = -4(-3)^3 - 27(1)^2 = 81 = 9^2$. Thus D is the square of something in $\mathbb{Q}$, so $G = A_3$.

Example. Let $f(x) = x^3 + 3x^2 - x - 1 \in \mathbb{Q}[x]$. For the same reason as $x^3 - 3x + 1$ in the previous example, $f(x)$ is also separable over $\mathbb{Q}$. Note that $g(x) = f(x - 3/3) = f(x - 1) = (x-1)^3 + 3(x-1)^2 - (x-1) - 1 = x^3 - 4x + 2$. So $D = -4(-4)^3 - 27(2)^2 = 148$. So this is not a square in $\mathbb{Q}$, so $G = S_3$.

16. October 12 & 16: Moving onto the quartic case

Let $f \in K[x]$ be a separable degree-four polynomial, and let u_1, u_2, u_3, u_4 be distinct roots in the splitting field F. F/K is Galois with Galois group G, a transitive subgroup of S_4 of order divisible by 4. Let $V := \{(1), (12)(34), (13)(24), (14)(23)\} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Note that V is a normal subgroup of S_4, so $V \cap G$ is a normal subgroup of G.

Lemma 16.1. *Write $(\alpha, \beta, \gamma) := (u_1u_2 + u_3u_4, u_1u_3 + u_2u_4, u_1u_4 + u_2u_3)$. Then there is a correspondence between $K(\alpha, \beta, gamma)$ and $V \cap G$, via Galois correspondence.*

Proof. Since F/K is Galois, so is $F/K(\alpha, \beta, \gamma)$. So $K(\alpha, \beta, \gamma)$ is the fixed field for the group of all K-automorphisms that fix α, β, γ. We claim that if $\sigma(V \cap G) = \tau(V \cap G)$, then $\sigma(\delta) = \tau(\delta)$ for $\delta \in \{\alpha, \beta, \gamma\}$. Note that the elements in V fix α, β, γ – so indeed $\sigma(V \cap G) = \tau(V \cap G)$. Therefore $\sigma = \tau\mu$ for some $\mu \in V \cap G$. But then $\mu(\delta) = \delta$ for $\delta \in \{\alpha, \beta, \gamma\}$, so $\sigma(\delta) = \tau(\mu(\delta)) = \tau(\delta)$. Now, we have that

$$S_4 = V \sqcup (12)V \sqcup (13)V \sqcup (14)V \sqcup (123)V \sqcup (132)V.$$

So finally, we have

$$\begin{aligned}
(12)(\beta) &= u_2u_3 + u_1u_4 \neq \beta \\
(13)(\alpha) &= u_2u_3 + u_1u_4 \neq \alpha \\
(14)(\alpha) &= u_2u_4 + u_1u_3 \neq \alpha \\
(123)(\alpha) &= u_2u_3 + u_1u_4 \neq \alpha \\
(132)(\alpha) &= u_2u_3 + u_1u_4 \neq \alpha.
\end{aligned}$$

So only the elements in G that lie in V fix α, β, γ, as required. □

Remark. Furthermore, $K(\alpha, \beta, \gamma)/K$ is Galois with the Galois group $G/(G \cap V)$.

Definition 16.1. The polynomial $g(x) = (x - \alpha)(x - \beta)(x - \gamma)$ is the *resolvent cubic of f*.

Remark. It seems at first glance that a resolvent cubic of f lies in $F[x]$, but in fact it lies in $K[x]$.

Lemma 16.2. *Let $f(x) = x^4 + bx^3 + cx^2 + dx + e \in K[x]$. Then the resolvent cubic g is given by $g(x) = x^3 - cx^2 + (bd - 4e)x + b^2e + 4ce - d^2$.*

Proposition 16.1. *Let $f \in K[x]$ be a separable quartic polynomial, and F/K be the splitting field of f over K. Let G be the Galois group, which is isomorphic to a transitive subgroup of S_4 of 4, 8, 12, or 24. Let also $m = [K(\alpha, \beta, \gamma) : K]$. Then*

(i) $m = 6 \Leftrightarrow G = S_4$
(ii) $m = 3 \Leftrightarrow G = A_4$

(iii) $m = 1 \Leftrightarrow G = V$
(iv) $m = 2 \Leftrightarrow G \cong D_4$ *or* $\mathbb{Z}/4\mathbb{Z}$.

In particular, we get D_4 *if* f *is irreducible over* $K(\alpha, \beta, \gamma)$ *(and* $\mathbb{Z}/4\mathbb{Z}$ *otherwise).*

Example. Let $f(x) = x^4 + 4x^2 + 2 \in \mathbb{Q}[x]$. Then the resolvent cubic of f is $g(x) = x^3 - 4x^2 - 8x + 32 = (x-4)(x^2-8)$. Thus $\alpha = 4, \beta = \sqrt{8}, \gamma = -\sqrt{8}$. So $\mathbb{Q}(\alpha, \beta, \gamma) = \mathbb{Q}(\beta) = \mathbb{Q}(\sqrt{2})$. So $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. Hence $G = \mathbb{Z}/4\mathbb{Z}$ or $G = D_4$. But then $f(x) = x^4 + 4x + 2 = (x^2 - (-2 + \sqrt{2}))(x^2 - (-2 - \sqrt{2})) \in \mathbb{Q}(\sqrt{2})[x]$. Therefore $G = \mathbb{Z}/4\mathbb{Z}$.

Example. Let $f(x) = x^4 - 2 \in \mathbb{Q}[x]$. Then $g(x) = x^3 + 8x = x(x + \sqrt{8}i)(x - \sqrt{8}i)$. Thus $\alpha = 0, \beta = \sqrt{8}i, \gamma = -\sqrt{8}i$. So $\mathbb{Q}(\alpha, \beta, \gamma) = \mathbb{Q}(\sqrt{8}i)$. Since $[\mathbb{Q}(\sqrt{8}i) : \mathbb{Q}] = 2$, we see that $G = \mathbb{Z}/4\mathbb{Z}$ or D_4. But since f is irreducible over $\mathbb{Q}(\sqrt{8}i)$, it follows $G = D_4$.

Theorem 16.1. *Let* p *be prime, and* $f \in \mathbb{Q}[x]$ *be irreducible where* $\deg f = p$. *Suppose also that there are exactly two non-real roots in* $\mathbb{C}$. *Then the Galois group of* f *is* S_p.

Proof. We can view G as a subgroup of S_p; recall that G is a transitive subgroup of S_p with $p | \#G$. Cauchy's theorem implies that G thus has an element σ of order p. Order of σ is the lcm of the orders of its disjoint cycles. Since p is prime, there can be only one cycle; thus σ is a p-cycle. Further, complex conjugation is a $\mathbb{Q}$-automorphism of the splitting field F of f over $\mathbb{Q}$. Complex conjugation fixes the real roots and swaps the two non-real roots. So G contains a transposition, say (ab). So we can write $\sigma = (aj_2 \cdots j_p)$. So some power σ^k is of the form $\sigma^k = (abi_3 \cdots i_p)$. So G contains (ab) and $(abi_3 \cdots i_p)$ (re-order if necessary). Then G contains $(12), (123 \cdots p)$. Hence $G \supseteq \langle (12), (123 \cdots p) \rangle = S_p$, so $G = S_p$ as required. $\square$

17. October 16, 18, & 19: Finite fields

Theorem 17.1. *Let* F *be any field, and let*

$$P := \bigcap \{K \mid K \text{ is a subfield of } F\}.$$

Then P *is a field having no proper subfields. If* $\operatorname{char} F = 0$, *then* $P \cong \mathbb{Q}$; *if* $\operatorname{char} F = p > 0$, *then* $P \cong \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Definition 17.1. The P as defined in Theorem 17.1 is called the *prime subfield* of F. In particular, P is the subfield generated by 1_F.

Proof. Since $0, 1 \in P$ we know that $P \neq \emptyset$. For any $u, v \in P$, indeed $u, v \in K$ for all subfields K of F. Then $u - v, uv^{-1} \in K$ for all such K (clearly, $v \neq 0$ for uv^{-1}), so $u - v, uv^{-1} \in P$. So if K is a subfield of P, then K is a subfield of F. Hence $P \subseteq K$, so $P = K$. Thus P cannot have any proper subfield.

For the second part, consider $\varphi : \mathbb{Z} \to P$ such that $m \mapsto m \cdot 1_F$. Then φ is a homomorphism with kernel (m) where $m = \operatorname{char} F$.

(1) Case I: $m = p$ where p is a prime
In this case we get an isomorphism between $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ and $\operatorname{im} \varphi \leq P$, per the first isomorphism theorem. So $\operatorname{im} \varphi$ is a field. But $\operatorname{im} \varphi$ is a subfield of P which has no proper subfields. This forces $\operatorname{im} \varphi = P$, so $\mathbb{F}_p \cong P$.

(2) Case II: $m = 0$
For this case, we see that $\varphi : \mathbb{Z} \to P$ is a monomorphism. This naturally induces a monomorphism $\overline{\varphi} : \mathbb{Q} \to P$ (just apply φ to both numerator and denominator).

Then $\operatorname{im}\overline{\varphi} \cong \mathbb{Q}$ is a field. Thus $\operatorname{im}\overline{\varphi}$ is a subfield of P, but P doesn't have any proper subfields. Indeed $\operatorname{im}\overline{\varphi} = P$, so $P \cong \mathbb{Q}$ as required. □

Corollary 17.1. *If F is a finite field, then $\operatorname{char} F = p$ where p is a prime. Furthermore, $\#F = p^n$ for $n \in \mathbb{N}$.*

Proof. $\operatorname{char} F = p$ since $P \cong \mathbb{F}_p$ for some prime p. (Alternative for P is $\mathbb{Q}$, but $\mathbb{Q}$ is infinite whereas F is assumed to be finite.) Finally, $F/\mathbb{F}_p$ is an extension of finite degree since otherwise F would be infinite. Say $[F : \mathbb{F}_p] = n$. So $\#F = p^n$ since $F \cong \mathbb{F}_p^n$. □

Theorem 17.2. *Let F be a field, and G a finite subgroup of F^*. Then G is cyclic. In particular, the multiplicative group of a finite group is cyclic.*

Proof. Let G be a finite subgroup of F^*. Then G is a finite abelian group. If $G = \{1\}$, then G is cyclic. Otherwise, then by the fundamental theorem of abelian groups, we have

$$G = \mathbb{Z}/m_1\mathbb{Z} \oplus \mathbb{Z}/m_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_k\mathbb{Z}$$

for some $m_j \in \mathbb{N}, m_1 > 1$, and $m_1 \mid m_2 \mid \cdots \mid m_k$. We thus have $u^{m_k} = 1$ for all $u \in G$. In other words, the polynomial $x^{m_k} - 1 \in F[x]$ has at least $\#G$ roots. But this polynomial has at most m_k roots in F, so $\#G \leq m_k$. At the same time, we have $\#G = m_1 m_2 \cdots m_k$, so this forces $k = 1$. Hence $G \cong \mathbb{Z}/m_k\mathbb{Z}$ is cyclic. In particular, F is finite, so F^* is cyclic as required. □

Remark. Taking $F = \mathbb{F}_p$, we see that the primes have primitive roots.

Corollary 17.2. *If F is finite, then $F = \mathbb{F}_p(u)$ for some $u \in F$. In other words, F is a simple extension of $\mathbb{F}_p$.*

Proof. Let F^* be generated by u. Then $F = \mathbb{F}_p(u)$. □

Lemma 17.1. *Let $\operatorname{char} F = p$ and $r \in \mathbb{N}$. Then the map $\varphi : F \to F$ defined by $u \mapsto u^{p^r}$ is a $\mathbb{F}_p$-monomorphism. In case F is finite, φ is in fact a $\mathbb{F}_p$-automorphism of F.*

Proof (sketch). Basically this follows from the Freshman's dream. In characteristic p, we have $(u \pm v)^{p^r} = u^{p^r} \pm v^{p^r}$, so φ is a homomorphism. Furthermore, since $\varphi(1) = 1^{p^r} = 1 \neq 0$, φ is a non-zero map. φ is a non-zero field homomorphism, so φ is a field monomorphism also.

Finally, pick p consecutive integers as the representatives of the elements in $\mathbb{F}_p$ (say $\mathbb{F}_p = \{1, 2, \ldots, p\}$). Then note that

$$\begin{aligned}
\varphi(1) &= 1 \\
\varphi(2) &= \varphi(1+1) = \varphi(1) + \varphi(1) = 2 \\
&\vdots \\
\varphi(p) &= \varphi(\underbrace{1 + 1 + \cdots + 1}_{p \text{ times}}) = \underbrace{\varphi(1) + \cdots + \varphi(1)}_{p \text{ times}} = 1 + \cdots + 1 = p.
\end{aligned}$$

Therefore φ is a $\mathbb{F}_p$-monomorphism. Furthermore, if F happens to be finite, then $\operatorname{im}\varphi$ has the same size as F, so $\operatorname{im}\varphi = F$. The last claim follows. □

Proposition 17.1. *Let p be a prime, and $n \in \mathbb{N}$. Then F is a finite field with p^n elements if and only if F is a splitting field extension over $\mathbb{F}_p$ of $x^{p^n} - x$.*

Proof. ($\Rightarrow$) Suppose that $\#F = p^n$. Then $\#F^* = p^n - 1$. So $u^{p^n-1} = 1$ for all $u \in \mathbb{F}^*$. All elements of F^* satisfy $x^{p^n-1}-1$, so they all satisfy $x(x^{p^n-1}-1) = x^{p^n}-x$ (including 0). Hence every element of F is a root of $x^{p^n}-x$. In conclusion, $F = \mathbb{F}_p(F) = \mathbb{F}_p(\{\text{all roots of } x^{p^n} - x\})$, which is a splitting field over $\mathbb{F}_p$ of $x^{p^n} - x$, as required.

($\Leftarrow$) Assume that F is the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$. Note that $(x^{p^n} - x)' = p^n x^{p^n-1} - 1 = -1$ since $\operatorname{char} F = p$, so $x^{p^n} - x$ is relatively prime to its derivative. This implies that $x^{p^n} - x$ is separable in F, and so has p^n distinct roots.

Let E be the set of all roots of $x^{p^n} - x$ in F. If we can show that E is a field, then we would have $E = F$ has size p^n. Note that $u \in E$ if and only if $\varphi(u) = u$, where $\varphi : F \to F$ sending u to u^{p^n}. Clearly $\varphi(1) = 1$, so $1 \in E$. For any $u, v \in E$ where $\varphi(u) = u$ and $\varphi(v) = v$, it follows $\varphi(u - v) = \varphi(u) - \varphi(v) = u - v \in E$. For any $v \neq 0$, we have $\varphi(uv^{-1}) = \varphi(u)\varphi(v)^{-1} = uv^{-1}$, so $uv^{-1} \in E$. Thus E is a subfield of F, so $E = F$ as required. □

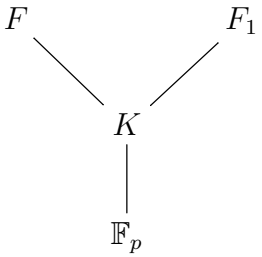
Corollary 17.3. *Let p be a prime and $n \in \mathbb{N}$. Then there exists a field with p^n elements, and any two such field are $\mathbb{F}_p$-isomorphic.*

Proof. Any finite fields with p^n elements are splitting fields of $x^{p^n} - x$ over $\mathbb{F}_p$, so we know that there exist such field(s), and any two of them are $\mathbb{F}_p$-isomorphic. □

Corollary 17.4. *Let K be any finite field, and let $n \in \mathbb{N}$. Then there is a simple extension $F = K(u)$ with $[F : K(u)] = n$. Furthermore, any two such F's are K-isomorphic.*

Proof. Let $\#K = p^r$ where p is a prime, and $r \in \mathbb{N}$. Define F to be a splitting field extension of $x^{p^{rn}} - x$ over K. For any $u \in K$ we have $u^{p^r} = u$, so inductively we can also claim $u^{p^{rn}} = u$. Thus F is a splitting field extension of $x^{p^{rn}} - x$ over $\mathbb{F}_p$ also. Every element in K is a root of $x^{p^{rn}} - x$, so $F = \mathbb{F}_p(\{\text{all roots of } x^{p^{rn}} - x\})$ since $F = K(\{\text{all roots of } x^{p^{rn}} - x\})$. Hence $\#F = p^{rn}$, and F consists precisely of the p^{rn} roots of $x^{p^{rn}} - x$. So $p^{rn} = \#F = (\#K)^{[F:K]} = p^{r[F:K]}$, from which $[F : K] = n$ follows.

Furthermore, if $[F_1 : K] = n$, then $[F_1 : \mathbb{F}_p] = rn$. So both F and F_1 are splitting field extensions of $x^{p^{rn}} - x$ over $\mathbb{F}_p$.



So F and F_1 are K-isomorphic, as both are splitting field extensions of $x^{p^{rn}} - x$ over K. Finally, we have already shown that any finite extension over a finite field is simple, so the proof is complete. □

Corollary 17.5. *If K is a finite field, then $K[x]$ contains irreducible polynomials of every positive degree.*

Proof. Let $n \in \mathbb{N}$, and let $F = K(u)$ be a simple extension of degree n. Then the minimal polynomial of u over K is an irreducible polynomial in $K[x]$ of degree n. □

Definition 17.2. Let F/K be a Galois extension. Then F/K is a *cyclic extension* if $\operatorname{Gal}_K F$ is cyclic.

Proposition 17.2. *Every finite extension of a finite field is Galois with cyclic Galois group.*

Proof. Let F/K be finite, and let K be a finite field whose characteristic is p. Then $F/\mathbb{F}_p$ is finite since F/K and $K/\mathbb{F}_p$ are both finite.

$$\begin{array}{c} F \\ | \\ K \\ | \\ \mathbb{F}_p \end{array}$$

Say $[F : \mathbb{F}_p] = n$. Then $\#F = p^n$, so F is a splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$. In fact, F consists precisely of the p^n distinct roots of $x^{p^n} - x$. Thus F is a splitting field extension over $\mathbb{F}_p$ of the polynomial $x^{p^n} - x$ that has separable irreducible factors. Hence $F/\mathbb{F}_p$ is Galois, so F/K is Galois also. Finally, note that $\operatorname{Gal}_K F \leq \operatorname{Gal}_{\mathbb{F}_p} F$, and all subgroups of a cyclic group are cyclic also. So it is sufficient to prove that $\operatorname{Gal}_{\mathbb{F}_p} F$ is cyclic. So we want to prove that there exists φ such that $\operatorname{Gal}_{\mathbb{F}_p} F = \langle \varphi \rangle$, where $\varphi : F \to F$ is the Frobenius map, i.e., the $\mathbb{F}_p$-automorphism given by $\varphi(u) = u^p$ for all $u \in F$. First, we claim that $\varphi^n = \mathrm{id}$. Indeed, note that $\varphi^n(u) = u^{p^n} = u$ since every $u \in F$ is a root of $x^{p^n} - x$. If $\varphi^k = \mathrm{id}$ then every $u \in F$ would satisfy $x^{p^k} - x$. This forces $k \geq n$ – otherwise, all p^n elements would be roots of the polynomial $x^{p^k} - x$, which has degree strictly less than p^n. Hence $\operatorname{ord} \varphi = n$. But then $\operatorname{ord} \varphi = [F : \mathbb{F}_p] = \# \operatorname{Gal}_{\mathbb{F}_p} F$. Thus the claim follows. □

18. October 23: Separability (Chapter VI)

Definition 18.1. An element u, algebraic over K, is *purely inseparable over* K if it is the only root of it minimal polynomial in $K[x]$. In other words, its minimal polynomial factors as $(x - u)^m$ for some $m \geq 1$. F/K is *purely inseparable* if each $u \in F$ is purely inseparable over K.

Theorem 18.1. *The elements that are both separable and purely inseparable over K are precisely the elements in K.*

Proof. Let u be separable and purely inseparable over K, and let f_u be the minimal polynomial of u over K. Since u is purely inseparable, u is the only root of f_u, i.e., $f_u = (x - u)^m$ for $m \in \mathbb{N}$. But since u is separable also, f_u has distinct roots. Therefore $m = 1$. So $\deg_K(u) = 1$, so $u \in K$ as required. □

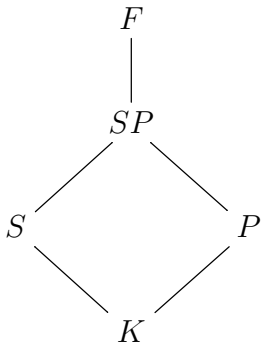
Remark. This result implies that whenever F/K is separable (such as when $\operatorname{char} K = 0$), the only purely inseparable elements are the elements in K. So we need only characterize purely inseparable extensions in characteristic $p > 0$, where p is a prime.

19. October 26: Characterization of purely inseparable extensions in characteristic p

u is purely inseparable over K if and only if the minimal polynomial of $u \in K[x]$ has only one root. Similarly, u is separable if and only if the minimal polynomial of $u \in K[x]$ has distinct roots. In general, only the elements in K are separable and purely inseparable.

Thus, If F/K is separable (resp. purely inseparable), pure inseparability (resp. separability) isn't interesting to look at (e.g. $\operatorname{char} K = 0$).

Let S be the separable closure of K in F; similarly let P be the purely inseparable closure of K in F.



(Recall that $K = S \cap P$).

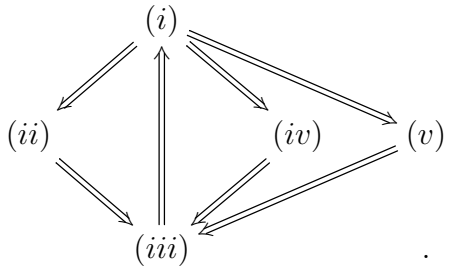
Lemma 19.1. *Let F/K be a field extension, and* $\operatorname{char} K = p$ *where p is a prime. For every $u \in F$ algebraic over K, then u^{p^n} is separable over K for some n.*

Proof. We will prove this by induction on $[K(u) : K]$. If $[K(u) : K] = 1$, then $u \in K$. So by Theorem 18.1, $u^{p^0} = u$ is separable over K. So suppose $k \geq 1$ and suppose the result holds for elements of degree $1, 2, \ldots, k-1$ over K; and let u have degree k over K. If u is separable over K, then the result follows from the base case. If u isn't separable, then $f_u \in K[x]$ has a repeated root. So this root satisfies f_u' also. But f_u is minimal, so $f_u' = 0$. If $f_u = \sum a_j x^j$, then $f_u' = \sum j a_j x^{j-1} = 0$; therefore $j a_j = 0$ for all j. This implies that either $a_j = 0$ or $p \,|\, j$ for all j. Thus every exponent is divisible by p, so f_u is a polynomial in x^p. Write $f_u = g(x^p)$ for some $g \in K[x]$. Then $\deg g = kp^{-1} < k$, so u^p has degree over K in the range $1, 2, \ldots, k-1$. Apply the inductive hypothesis implies $(u^p)^{p^{n-1}}$ is separable K, so u^{p^n} is separable over K. □

Theorem 19.1. *Let F/K be algebraic, and* $\operatorname{char} K = p > 0$ *where p is a prime. Then the following are equivalent.*

(i) F/K is purely inseparable.
(ii) Every $u \in F$ has minimal polynomial in $K[x]$ of the form $x^{p^n} - a$.
(iii) For every $u \in F$, we have $u^{p^n} \in K$ for some $n \geq 0$.
(iv) F contains no non-trivial (as in not in K) elements that are separable over K.
(v) F is generated over K by a set of elements purely inseparable over K.

We will prove the equivalence by following the map below.



.

Proof. ((i) $\Rightarrow$ (ii)) If F/K is purely inseparable, $u \in F$ and $f_u \in K[x]$ is the minimal polynomial, then $f_u(x) = (x-u)^m$ for some m. Write $m = p^r n$ for $p \nmid n$ (if $m = 1$, then $u \in K$ anyway; so assume $m > 1$). Then $f_u(x) = (x-u)^m = (x-u)^{p^r n} = [(x-u)^{p^r}]^n = (x^{p^r} - u^{p^r})^n \in K[x]$. Then the coefficient of $x^{p^r(n-1)}$ is $-nu^{p^r} \in K$. But since $p \nmid n$, we have $u^{p^r} \in K$. So $n = 1$ since f_u is of lease degree satisfied by u. So $f_u(x) = x^{p^r} - a$ for $a = u^{p^r} \in K$.

((i) $\Rightarrow$ (iv)) Immediate.

((i) $\Rightarrow$ (v)) Any generating set will consist entirely of purely inseparable elements.

((ii) $\Rightarrow$ (iii)) Let $u \in F$, and let

$$f_u(x) = x^{p^n} - a.$$

Then $0 = f_u(u) = u^{p^n} - a$, so $u^{p^n} = a \in K$

((v) $\Rightarrow$ (iii)) Let $F = K(u_1, \ldots, u_n)$ where each u_i is purely inseparable over K. Repeating the argument presented in ((i) $\Rightarrow$ (ii)), we see that for all j there is n_j such that $u_j^{p^{n_j}} \in K$. Define $n = \max\{n_j\}$. Then $u_j^{p^n} \in K$ for all j. Finally, if $u \in F$ then u is a rational function in the u_j. Then freshman's dream implies $u^{p^n} \in K$.

((iv) $\Rightarrow$ (iii)) If $u \in F$ then u^{p^n} is separable over K for some n by Lemma 19.1. So by (iv), $u^{p^n} \in K$.

((iii) $\Rightarrow$ (i)) Suppose $u \in F$. So by (iii), we see $u^{p^n} \in K$ for some n. Note that $f(x) = x^{p^n} - u^{p^n} \in K[x]$ is satisfied by u. Since $f(x) = (x-u)^m$ has only one root, the same is true for the divisor $f_u(x) \in K[x]$. Thus u is purely inseparable over K as desired. $\square$

Corollary 19.1. *If F/K is finite and purely inseparable with* $\operatorname{char} K = p$*, then $[F:K] = p^n$ for some n.*

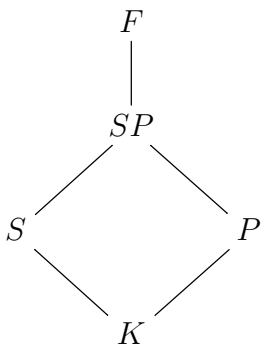
Proof (sketch). Let $F = K(u_1, \ldots, u_n)$ where each u_i is purely inseparable over K. Then consider the tower

$$K \subseteq K(u_1) \subseteq K(u_1, u_2) \subseteq \cdots \subseteq K(u_1, \ldots, u_n).$$

Note that each u_j is purely inseparable over $K(u_1, \ldots, u_{j-1})$. So we may reduce to proving the result for simple extensions. Finally, $[K(u):K] = p^n$ for p^n with minimal polynomial being $x^{p^n} - a \in K[x]$. $\square$

20. October 30

As we discuss purely inseparable extensions, we will be referring to the following very helpful diagram often.



(where $K = S \cap P$. S is the separable closure of K, and P is the purely inseparable closure of K. Note that we are required to show that S and P actually are fields (thereby being subfields of F)).

Theorem 20.1. *Let F/K be algebraic.*

(i) S is the largest subfield of F that is separable over K.
(ii) F/S is purely inseparable. That is, the S/K is the "separable" portion of the extension, so the remaining portion (F/S) is the purely inseparable portion.
(iii) P is the largest subfield of F that is purely inseparable over K.
(iv) $S \cap P = K$
(v) F/P is separable if and only if $F = SP$.
(vi) If F/K is normal, then S/K and F/P are Galois with $\mathrm{Aut}_K S \cong \mathrm{Aut}_P F = \mathrm{Aut}_K F$.

Before proving the theorem, we are required to prove the following lemma, as this lemma will be used in the proof of Theorem 20.1.

Lemma 20.1. *If $F = K(X)$, and every element of X is separable over K, then F/K is separable.*

Proof. Let $v \in F$. Then $v \in K(u_1, \ldots, u_n)$ for some $u_j \in X$; let $f_j \in K[x]$ be the minimal polynomial of u_j for each j. Als, let E be a splitting field over K of the u_j. Then $K(u_1, \ldots, u_n) \subseteq E$. But since E/K is Galois, it follows that E/K is separable over $v \in E$. Thus v is separable over K. □

Proof of Theorem 20.1. (i) Let $1 \in S$, and $u, v \in S$. Then $u, v \in K(u, v)$. Thus $u - v \in K(u, v)$, and $uv^{-1} \in K(u, v)$ (provided $v \neq 0$). But $K(u, v) \in S$, so S is a field.

(iii) Let $1 \in P$, and $u, v \in P$. Then $u, v \in K(u, v)$. Thus $u - v \in K(u, v)$, and $uv^{-1} \in K(u, v)$ (provided $v \neq 0$). But $K(u, v) \in P$, so P is a field.

(iv) This is Theorem 18.1.

(ii) Let $u \in F$. Note that we need to cover both the characteristic p case and the characteristic 0 case. Let $\mathrm{char}\, K = p$. Then u^{p^n} is separable over K for some n, i.e., $u^{p^n} \in S$ for some n. Thus F/S is purely inseparable as required. If $\mathrm{char}\, K = 0$, then every element of F is separable over K. Thus $F = S$, so F/S is (trivially) purely inseparable (and separable at the same time).

(v) ($\Rightarrow$) If F/P is separable, then F/SP is separable also. Also, F/S is purely inseparable, so F/SP is purely inseparable also. The only extension that is both separable and purely inseparable is the trivial extension; therefore $F = SP$ as required. ($\Leftarrow$) Assume $F = SP$. We may view F as $F = P(S)$. So any elements in S that are separable over K are separable over P also. Since the generators (the elements in S) are separable, indeed F/P is separable.

(vi) We first prove that $(\mathrm{Aut}_K F)' = P$. Pick $u \in P$. Then $f_u(x)(x-u)^m \in K[x]$. For any $\sigma \in \mathrm{Aut}_K F$, $\sigma(u)$ is a root of f_u. There is only one root of $f_u(x)$, so this forces $\sigma(u) = u$. Hence $P \subseteq (\mathrm{Aut}_K F)'$. Conversely, assume $u \in (\mathrm{Aut}_K F)'$, and assume that v is another root of $f_u(x)$. Then there is a K-isomorphism $\tau : K(u) \to K(v)$ such that $u \mapsto v$. Since F/K is normal, F/E is also a splitting field of some set of polynomials (where E is an intermediate field between F and K), τ extends to some element $\overline{\tau} \in \mathrm{Aut}_K F$. So for some $\overline{\tau}$ we have $v = \overline{\tau}(u) = u$, as u is the only root of $f_u(x)$. This means $u \in P$. This proves the reverse inclusion, so we have $(\mathrm{Aut}_K F)' = P$, hence $\mathrm{Aut}_K F = \mathrm{Aut}_P F$.

Now consider the map $\theta : \mathrm{Aut}_P F \to \mathrm{Aut}_K S$ defined by $\sigma \mapsto \sigma|_S$. First, we need to prove that θ is well-defined. Let $\sigma \in \mathrm{Aut}_P F = \mathrm{Aut}_K F$. Then $\theta(\sigma) \in \mathrm{Aut}_K S$ since $\sigma|_S(S)$ is

a subfield of F isomorphic to S. So the separability is preserved, i.e.., $\operatorname{im}(\sigma|_S) \subseteq S$. Now looking at $\sigma^{-1}|_S$ shows that $\sigma|_S \in \operatorname{Aut}_K S$.

As for surjectivity, note that F/S is normal since F/K is normal. This means that $\tau \in \operatorname{Aut}_K S$ is extendible to F. In other words, there is $\sigma \in \operatorname{Aut}_K F = \operatorname{Aut}_P F$ with $\sigma|_S = \tau$. Such σ satisfies $\theta(\sigma) = \tau$; thus θ is surjective.

It remains to show injectivity To do so, we shall prove that $\ker\theta$ is trivial. Suppose $\sigma \in \ker\theta$. This means $\sigma|_S = \mathrm{id}_S$, so σ must fix S. But then $\sigma \in \operatorname{Aut}_P F$, so σ fixes P also. Hence σ fixes SP. But then we already proved that F/P is Galois, so F/P is separable. Recall that $F = SP$ (from (v)) so $\sigma = \mathrm{id}_F$. Thus $\ker\theta$ is trivial. □

Corollary 20.1. *Let F/K be a field extension and E an intermediate field. If F/E and E/K are separable, then F/K is separable also.*

Proof. Assume F/E and E/K are separable. Then $E \subseteq S$. F/S is both purely inseparable and separable: F/S is separable since F/E is separable, and $E \subseteq S$ (consult the diagram below).

$$\begin{array}{c} F \\ | \\ S \\ | \\ E \end{array}$$

Thus $F = S$ is separable over K. □

21. November 1

Let $\operatorname{char} F = p$. Then

- For all $n \in \mathbb{N}$, $F^{p^n} = \{u^{p^n} : u \in F\}$ is a subfield of F – recall $F^{p^n} = \operatorname{im}\varphi$ where $\varphi : F \to F$ defined by $u \mapsto u^{p^n}$.
- F/F^{p^n} is purely inseparable. Thus F/E is purely inseparable for any intermediate field.

These facts lead us to the following corollaries.

Corollary 21.1. *Let* $\operatorname{char} K = p$*, and suppose that F/K is algebraic.*

(1) If F/K is separable, then $F = KF^{p^n}$ for every $n \in \mathbb{N}$.
(2) If $[F : K]$ is finite, and $F = KF^p$, then F/K is separable.
(3) u is separable over K if and only if $K(u) = K(u^p)$.

Lemma 21.1. *Suppose* $\operatorname{char} K = p$*, and suppose that F/K is algebraic. Suppose also that $[F : K]$ is finite. Then there exists $n \in \mathbb{N}$ such that $S = KF^{p^n}$.*

Lemma 21.2. *Suppose* $\operatorname{char} K = p$*, and suppose that F/K is algebraic. Suppose also that $[F : K]$ is finite. Then for any $t \geq 1$,*

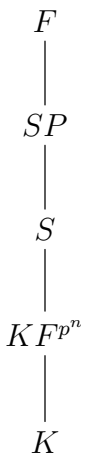
$$KF^{p^t} = K(u_1^{p_t} \ldots, u_m^{p^t})$$

for any choice of generators u_j.

Proof. By Freshman's Dream, we have $F = K(u_1, u_2, \ldots, u_m) = K(u_1^p, \ldots, u_m^p)$ if $F = KF^p$ (since each u_j is a generator). Similarly, since each u_j^p is a generator, it also follows that $F = K(u_1^p, \ldots, u_m^p) = K(u_1^{p^2}, \ldots, u_m^{p^2})$. Continuing on with this argument, we see that $K(u_1^{p^n}, \ldots, u_m^{p^n}) = KF^{p^n} = S$. Thus F/K is separable. □

Proof. (a) If F/K is separable, then for any n, the extension F/KF^{p^n} is separable. But F/KF^{p^n} is also purely inseparable, so $F = KF^{p^n}$.

For parts (b) and (c), we will assume that $[F : K]$ is finite. First we show that there exists $n \in \mathbb{N}$ such that $S = KF^{p^n}$. Since $F = K(u_1, \ldots, u_m) = S(u_1, \ldots, u_m)$, indeed F/S is purely inseparable. So each u_j is purely inseparable over S. Thus there is n with $u_j^{p^n} \in S$ for all j. Hence $F^{p^n} \subseteq S$, so $KF^{p^n} \subseteq S$.



Since S/K is separable, S/KF^{p^n} is separable also. Yet S/KF^{p^n} is purely inseparable also, so $S = KF^{p^n}$. □

22. November 2

Definition 22.1. Let F/K be an algebraic extension, and S is the separable closure of K in F. Then $[S : K]$ is called the *separable degree of* F/K, denoted by $[F : K]_s$. $[F : S]$ is called the *inseparable degree of* $[F : K]$, denoted by $[F : K]_i$.

Remark. Some properties of $[F : K]_s$ and $[F : K]_i$

- $[F : K] = [F : K]_s[F : K]_i$.
- F/K is separable if and only if $[F : K]_s = [F : K]$ and $[F : K]_i = 1$.
- F/K is purely inseparable if and only if $[F : K]_s = 1$ and $[F : K]_i = [F : K]$.
- If F/K is a finite extension in prime characteristic p, then $[F : K]_i$ is a power of p.

Lemma 22.1. *Let N be a normal extension of K containing F. Let E be an intermediate field of F and K. Then*

$$\#\operatorname{Hom}_K(F, N)^\star = \#\operatorname{Hom}_K(E, N)^\star \#\operatorname{Hom}_E(F, N)^\star,$$

where $\#\operatorname{Hom}_K(F, N)^\star$ denotes the number of non-zero K-homomorphisms from F to N.

Proof. Let $\operatorname{Hom}_K(E, N)^\star = \{\sigma_1, \ldots, \sigma_t\}$, and $\operatorname{Hom}_E(F, N)^\star = \{\tau_1, \ldots, \tau_r\}$. Each σ_i extends to an element $\overline{\sigma}_i \in \operatorname{Aut}_K(N)$. In fact, $\overline{\sigma}_i|_F \in \operatorname{Hom}_K(F, N)^\star$. So all products of $\sigma_i\tau_j$ (abuse of notation here – write σ_i for $\overline{\sigma}_i$) are K-monomorphisms of F into N. Here we make the

claim that $\operatorname{Hom}_K(F,N)^\star = \{\sigma_i\tau_j : i,j\}$ and that all of $\sigma_i\tau_j$ are distinct. Note that proving this claim will complete the proof since we would have

$$\#\operatorname{Hom}_K(F,N)^\star = rt = \#\operatorname{Hom}_K(E,N)^\star \cdot \#\operatorname{Hom}_E(F,N)^\star.$$

To start off, one of the inclusions ($\{\sigma_i\tau_j\} \subseteq \operatorname{Hom}_K(F,N)^\star$) is immediate. Conversely, if $\sigma \in \operatorname{Hom}_K(F,N)^\star$, then $\sigma|_E \in \operatorname{Hom}_K(E,N)^\star$. Thus $\sigma|_E = \sigma_i$ for some i. But this tells us that $\sigma^{-1}\sigma \in \operatorname{Hom}_K(F,N)^\star$, and this will fix everything in E. Thus $\sigma^{-1}\sigma \in \operatorname{Hom}_E(F,N)^\star = \{\tau_j\}$. Therefore $\sigma_i^{-1}\sigma = \tau_j$ for some j, so σ is of the form $\sigma_i\tau_j$. Therefore $\operatorname{Hom}_K(F,N)^\star = \{\sigma_i\tau_j : i,j\}$.

Finally, if

$$\sigma_i\tau_j = \sigma_a\tau_b, \tag{$*$}$$

then $\sigma_a^{-1}\sigma_i\tau_j = \tau_b$ fixes E. If $u \in E$, then

$$\begin{aligned}
\sigma_a^{-1}\sigma_i\tau_j(u) &= \tau_b(u)\\
\sigma_a^{-1}\sigma_i(u) &= u\\
\sigma_a^{-1}\sigma_i &\in \operatorname{Hom}_E(F,N)^\star\\
\sigma_a^{-1}\sigma_i &= \mathrm{id},
\end{aligned}$$

since $\sigma_a, \sigma_i = E \to N$. Thus $\sigma_a = \sigma_i$ is injective, and from ($*$), we have $\tau_j = \tau_b$ also. Thus $\sigma_i\tau_j$ are in fact distinct as $a = i, b = j$. □

Lemma 22.2. *Let $[F : K]$ be finite, and let N be the normal closure of F over K (i.e, $N \supseteq F$, and N/K is normal). Then $\#\operatorname{Hom}_K(F,N)^\star = \#\operatorname{Hom}_K(S,N)^\star$.*

Proof. Every element in $\operatorname{Hom}_K(S,N)^\star$ extends to an element of $\operatorname{Aut}_K N$, and then restricts to an element in $\operatorname{Hom}_K(F,N)^\star$. All in all, every element of $\operatorname{Hom}_K(S,N)^\star$ extends to an element of $\operatorname{Hom}_K(F,N)^\star$. So we just need to show that if $\sigma, \tau \in \operatorname{Hom}_K(F,N)^\star$ and $\sigma|_S = \tau|_S$, then $\sigma = \tau$. If $\operatorname{char} K = 0$, then the lemma becomes evident as $S = F$. So suppose that $\operatorname{char} K = p > 0$. Then F/S is purely inseparable, so for any $u \in F$, there exists some n so that $u^{p^n} \in S$. Thus $\sigma(u^{p^n}) = \tau(u^{p^n})$. Since $\sigma(u)^{p^n} = \tau(u)^{p^n}$, and we can take advantage of Freshman's Dream, we have $(\sigma(u) - \tau(u))^{p^n} = 0$. Thus $\sigma(u) = \tau(u)$. Hence $\sigma(u) = \tau(u)$ on F. □

Proposition 22.1. *Let $[F : K]$ be finite, $N \supseteq F$, and N/K normal. Then $\#\operatorname{Hom}_K(F,N)^\star = [F : K]_s$.*

Proof. By Lemma 22.2, we are reduced to proving that $\#\operatorname{Hom}_K(F,N)^\star = [F : K]$ for finite and separable F/K. We will prove this by induction on $[F : K]$. If $[F : K] = 1$, then the claim trivially holds. Let $[F : K] > 1$, and assume that result holds for all finite separable extensions. Pick $u \in F \setminus K$, and let $[F : K(u)] = m$ and $[K(u) : K] = n$. By the inductive hypothesis, indeed $\#\operatorname{Hom}_{K(u)}(F,N) = m$ and $\#\operatorname{Hom}_K(K(u),N) = n$. Thus $\#\operatorname{Hom}_K(F,N) = mn = [F : K]$, as required. □

23. November 6

Corollary 23.1. *Let E be an intermediate field to F and K. Then $[F : K]_s = [F : E]_s[E : K]_s$ and $[F : K]_i = [F : E]_i[E : K]_i$.*

Proof. Let $N \supseteq F$ be a normal closure so that N/K is normal. Then $[F:K]_s$ is the number of K-monomorphisms from F to N, which is equal to the product of the number of E-monomorphisms of F and the number of K-monomorphisms of E. Therefore $[F:E]_s[E:K]_s$ as required. Finally, note that

$$\begin{aligned}[F:K]_s[F:K]_i = [F:K] &= [F:E][E:K] \\ &= [F:E]_s[F:E]_i[E:K]_s[E:K]_i \\ &= [F:K]_s[F:E]_i[E:K]_i.\end{aligned}$$

Cancel $[F:K]_s$, and the $[F:K]_i = [F:E]_i[E:K]_i$ as required. □

Definition 23.1. The *separable (resp. inseparable) degree of u over K* to be the separable (resp. inseparable) degree of $K(u)$ over K.

Corollary 23.2. *Let $f \in K[x]$ be a monic irreducible polynomial.*

(i) All roots of f have the same separable and inseparable degree over K.
(ii) All roots of f have the same multiplicity.
(iii) The common separable degree is the number of distinct roots of f; the common inseparable degree is the common multiplicity of roots.
(iv) Let r be the common multiplicity of roots of f; let u be any root of f. Then u^r is separable over K.

Proof. If $\operatorname{char} K = 0$, then we get the separable extension for free, so all the four claims follow evidently. So it suffices to consider the $\operatorname{char} K = p > 0$ case. Let F/K be a splitting field of f over K, and let $u = u_1, u_2, \ldots, u_n$ be distinct roots of f in F. Then $f(x) = (x-u_1)^{r_1}(x-u_2)^{r_2}\cdots(x-u_n)^{r_n} \in F[x]$. So for any j, indeed $[K(u_j):K]_s$ is the number of K-monomorphisms of $K(u_j)$ onto F. Each monomorphism is determined by where u_j is sent to, and there are exactly n (the number of distinct roots of f) choices. Thus $[K(u_j):K]_s = n$. So, every root of f has the same separable degree over K, namely the number of distinct roots of f.

Given any j, k, choose a K-isomorphism $\sigma : K(u_j) \to K(u_k)$ such that $\sigma(u_j) = u_k$. Then the factor of f corresponding to u_k is $(x-u_k)^{r_k} = (x-\sigma(u_j))^{r_j}$. But the unique factorization gives $r_k = r_j$. Hence every root has the same multiplicity, which we shall call r.

It still remains to show that r is actually the inseparable degree. Note we can re-write $f(x) = [(x-u_1)(x-u_2)\cdots(x-u_n)]^r$. So $rn = \deg f = [K(u_j):K] = [K(u_j):K]_s[K(u_j):K]_i = n[K(u_j):K]_i$. Cancel n, from which it follows $r = [K(u_j):K]_i$. Our choice of u_j was arbitrary, so every root has multiplicity equal to the common inseparable degree. This finishes the proof of (i), (ii), and (iii).

As for (iv), let $g(x) = (x-u_1^r)\cdots(x-u_n^r)$. Then by Freshman's Dream, $f(x) = (x^r - u_1^r)(x^r-u_2^r)\cdots(x_r-u_n^r)$. So if u is any root of f then u^r is a root of g. Thus u^r is separable over K as required. □

Definition 23.2. A *primitive element for F/K* is an element u such that $F = K(u)$.

Theorem 23.1 (Primitive element theorem)**.** *A finite-dimensional extension is simple if and only if there are only finitely many intermediate fields. In particular, every finite-dimensional separable extension is simple.*

Proof. We shall assume the first statement in order to prove the second statement first. Since F/K is finite-dimensional and separable, if N is the normal closure of F/K then N/K is

finite and Galois. Hence $\mathrm{Aut}_K N$ has finitely many subgroups. By the Fundamental theorem of Galois theory (Theorem 7.2), N/K has finitely many intermediate fields, so there can only be finitely many intermediate fields between F and K also. The claim follows from the first statement.

($\Rightarrow$ of the first statement) Suppose that $F = K(u)$ is simple, and let $f(x)$ be the minimal polynomial of u over K. Then we claim that every intermediate field corresponds to a factor of f.

($\Leftarrow$ of the first statement) Suppose there are only finitely many intermediate fields between F and K. We will prove that F is simple by taking a maximal intermediate field of the form $K(u)$, and then show that F is actually equal to $K(u)$. □

24. November 8: Cyclic extensions

Definition 24.1. Let F/K be a finite-dimensional extension, and let $\overline{K}$ be some algebraic closure of K containing F. For any $u \in F$, the *norm of* u (resp. *trace of* u) denoted by $\mathrm{N}_{F/K}(u)$ (resp. $\mathrm{Tr}_{F/K}(u)$) is given by

$$\mathrm{N}_{F/K}(u) = \left(\prod_{\sigma} \sigma(u)\right)^{[F:K]_i}$$

resp.

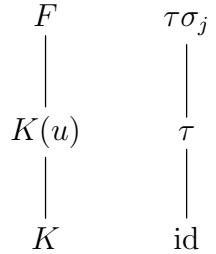
$$\mathrm{Tr}_{F/K}(u) = [F:K]_i \sum_{\sigma} \sigma(u),$$

where σ ranges over the K-monomorphisms $F \to \overline{K}$.

Remark. If F/K is separable, then $[F:K]_i = 1$. Particularly, if $u \in F$, then $\mathrm{N}_{K(u)/K}(u)$ is the product of conjugates of u; similarly, $\mathrm{Tr}_{K(u)/K}(u)$ is just the sum of conjugates of u. However, $\mathrm{N}_{F/K(u)}(u)$ is the product of conjugates powered by $[F : K(u)]$; similiarly, $\mathrm{Tr}_{F/K(u)}(u)$ is the sum of the conjugates of u multiplied by $[F : K(u)]$. Note that the additional automorphisms in a bigger field creates some repetitions, which justifies the extra power or the extra multiple, respectively. Thus it is important to *always take note of over which field the norm or the trace of an element is being calculated.*

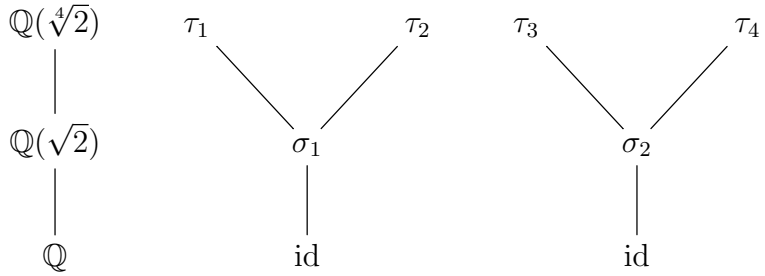
Remark. Call the roots of the minimal polynomial of u in $K[x]$ the conjugates of u. Then the conjugates are precisely the $\tau_i(u)$ for $1 \le i \le [K(u) : K]_s$, where the τ_i are the K-monomorphisms of $K(u)$, and the minimal polynomial of u over K is $(x - \tau_1(u))(x - \tau_2(u)) \cdots (x - \tau_l(u))$ where $l = [K(u) : K]_s$. In general, the K-monomorphisms of F are precisely the $\tau_i\sigma_j$ where the τ_i are as before, and the σ_j are $K(u)$-monomorphisms of F.

Consider the following diagram, where $1 \le j \le [F : K(u)]_s$.



So, each $\tau\sigma_j$ extends τ since if $v \in K(u)$ then $\sigma_j(v) = v$, and so $\tau\sigma_j(v) = \tau(v)$. The monomorphisms of F/K are just the extensions of the monomorphisms of E/K, each repeated $[F : E]_s$ times.

Example. Consider the extension



where

$$\begin{aligned}
\sigma_1 &: \sqrt{2} \mapsto \sqrt{2} \\
\sigma_2 &: \sqrt{2} \mapsto -\sqrt{2} \\
\tau_1 &: \sqrt[4]{2} \mapsto \sqrt[4]{2} \\
\tau_2 &: \sqrt[4]{2} \mapsto -\sqrt[4]{2} \\
\tau_3 &: \sqrt[4]{2} \mapsto i\sqrt[4]{2} \\
\tau_4 &: \sqrt[4]{2} \mapsto -i\sqrt[4]{2}.
\end{aligned}$$

We will compute the norm and traces of $\sqrt[4]{2}$ over $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$.

$$\begin{aligned}
\mathrm{N}_{\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})}(\sqrt[4]{2}) &= \tau_1(\sqrt[4]{2})\tau_2(\sqrt[4]{2}) \\
&= \sqrt[4]{2}(-\sqrt[4]{2}) = -\sqrt{2} \\
\mathrm{Tr}_{\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})}(\sqrt[4]{2}) &= \tau_1(\sqrt[4]{2}) + \tau_2(\sqrt[4]{2}) \\
&= \sqrt[4]{2} - \sqrt[4]{2} = 0. \\
\mathrm{N}_{\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}}(\sqrt[4]{2}) &= \tau_1(\sqrt[4]{2})\tau_2(\sqrt[4]{2})\tau_3(\sqrt[4]{2})\tau_4(\sqrt[4]{2}) \\
&= \sqrt[4]{2}(-\sqrt[4]{2})(i\sqrt[4]{2})(-i\sqrt[4]{2}) = -2 \\
\mathrm{Tr}_{\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}}(\sqrt[4]{2}) &= \tau_1(\sqrt[4]{2}) + \tau_2(\sqrt[4]{2}) + \tau_3(\sqrt[4]{2}) + \tau_4(\sqrt[4]{2}) \\
&= 0.
\end{aligned}$$

Also, the norm of traces of $\sqrt{2}$ over different field extensions:

$$\begin{aligned}
\mathrm{N}_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(\sqrt{2}) &= \sigma_1(\sqrt{2})\sigma_2(\sqrt{2}) \\
&= \sqrt{2}(-\sqrt{2}) = -2 \\
\mathrm{Tr}_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(\sqrt[4]{2}) &= \sigma_1(\sqrt{2}) + \sigma_2(\sqrt{2}) \\
&= \sqrt{2} - \sqrt{2} = 0. \\
\mathrm{N}_{\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}}(\sqrt{2}) &= \tau_1(\sqrt{2})\tau_2(\sqrt{2})\tau_3(\sqrt{2})\tau_4(\sqrt{2})
\end{aligned}$$

$$= \sqrt{2}\sqrt{2}(-\sqrt{2})(-\sqrt{2}) = 4$$
$$\mathrm{Tr}_{\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}}(\sqrt{2}) = \tau_1(\sqrt{2}) + \tau_2(\sqrt{2}) + \tau_3(\sqrt{2}) + \tau_4(\sqrt{2})$$
$$= 0.$$

Note that the norms and traces of the same element do differ depending on which field extension they are taken.

Theorem 24.1. *Let $[F : K]$ be finite with $u, v \in F$. Then the following hold:*

(1) $\mathrm{N}_{F/K}(uv) = \mathrm{N}_{F/K}(u)\,\mathrm{N}_{F/K}(v)$ *and* $\mathrm{Tr}_{F/K}(u+v) = \mathrm{Tr}_{F/K}(u) + \mathrm{Tr}_{F/K}(v)$.

(2) if $u \in K$, *then* $\mathrm{N}_{F/K}(u) = u^{[F:K]}$ *and* $\mathrm{Tr}_{F/K}(u) = [F : K]u$.

(3) $\mathrm{N}_{F/K}(u), \mathrm{Tr}_{F/K}(u) \in K$.

(4) If the minimal polynomial of u over K is $f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n$, then

$$\mathrm{N}_{F/K}(u) = ((-1)^n a_0)^{[F:K(u)]}$$
$$\mathrm{Tr}_{F/K}(u) = [F : K(u)]a_{n-1}.$$

25. November 9

Lemma 25.1. *Let $K \subseteq F$, and $u \in F \setminus K$. Then*

$$\mathrm{N}_{F/K}(u) = \big(\mathrm{N}_{K(u)/K}(u)\big)^{[F:K(u)]}$$
$$\mathrm{Tr}_{F/K}(u) = [F : K(u)]\,\mathrm{Tr}_{K(u)/K}(u).$$

Proof. Start from the definition. Note that σ in the product denotes K-monomorphisms of F, and τ the K-monomorphisms of $K(u)$.

$$\mathrm{N}_{F/K}(u) = \left(\prod_\sigma \sigma(u)\right)^{[F:K]_i} = \left[\left(\prod_\tau \tau(u)\right)^{[F:K(u)]_s}\right]^{[F:K]_i}$$
$$= \left(\prod_\tau \tau(u)\right)^{[F:K(u)]_s[F:K(u)]_i[K(u):K]_i} = \left[\left(\prod_\tau \tau(u)\right)^{[K(u):K]_i}\right]^{[F:K(u)]}$$
$$= (\mathrm{N}_{K(u)/K}(u))^{[F:K(u)]}.$$

One can make a similar argument for trace (except that you use the additive reasoning rather than multiplicative). □

Theorem 25.1. *Let $u, v \in F$, and $c \in K$; and let E be an intermediate field between K and F.*

(i) Norm is multiplicative: $\mathrm{N}_{F/K}(uv) = \mathrm{N}_{F/K}(u)\,\mathrm{N}_{F/K}(v)$

(ii) Trace is K-linear: $\mathrm{Tr}_{F/K}(cu + v) = c\,\mathrm{Tr}_{F/K}(u) + \mathrm{Tr}_{F/K}(v)$

(iii) $\mathrm{N}_{F/K}(c) = c^{[F:K]}$ *and* $\mathrm{Tr}_{F/K}(c) = [F : K]c$

(iv) If the minimal polynomial of u over K is $f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n$, then

$$\mathrm{N}_{F/K}(u) = ((-1)^n a_0)^{[F:K(u)]}$$
$$\mathrm{Tr}_{F/K}(u) = -[F : K(u)]a_{n-1}.$$

(v) $\mathrm{N}_{F/K} = \mathrm{N}_{E/K} \circ \mathrm{N}_{F/E}$ *and* $\mathrm{Tr}_{F/K} = \mathrm{Tr}_{E/K} \circ \mathrm{Tr}_{F/E}$.

Proof. For the first part, note

$$\begin{aligned}\mathrm{N}_{F/K}(uv) &= \left(\prod_\sigma \sigma(uv)\right)^{[F:K]_i} = \left(\prod_\sigma \sigma(u)\sigma(v)\right)^{[F:K]_i} \\ &= \left(\prod_\sigma \sigma(u)\right)^{[F:K]_i}\left(\prod_\sigma \sigma(v)\right)^{[F:K]_i} = \mathrm{N}_{F/K}(u)\,\mathrm{N}_{F/K}(v).\end{aligned}$$

One can use a similar argument to obtain the trace counterpart (ii). As for (iii), pick $u \in K$. Then every $\sigma : F \to \overline{K}$ is a K-monomorphism that maps u to itself, and recall that there are $[F:K]_s$ of these maps. Thus

$$\begin{aligned}\mathrm{N}_{F/K}(u) &= \left(\prod_\sigma \sigma(u)\right)^{[F:K]_i} = \left(\prod_\sigma u\right)^{[F:K]_i} \\ &= u^{[F:K]_s[F:K]_i} = u^{[F:K]}.\end{aligned}$$

From (iii), we know that $\mathrm{N}_{F/K}(u)$ and $\mathrm{Tr}_{F/K}(u)$ are in K. Also, thanks to Lemma 25.1, we are reduced to proving that $\mathrm{N}_{K(u)/K}(u) = (-1)^n a_0$ and $\mathrm{Tr}_{K(u)/K}(u) = -a_{n-1}$. Let the σ in the below product denote the K-monomorphisms of $K(u)$. Then

$$f(x) = \prod_\sigma (x - \sigma(u))^{[K(u):K]_i}.$$

Thus

$$a_0 = (-1)^{[K(u):K]_i[K(u):K]_s}\left(\prod_\sigma \sigma(u)\right)^{[K(u):K]_i} = (-1)^n\,\mathrm{N}_{K(u)/K}(u).$$

Hence $\mathrm{N}_{K(u)/K}(u) = (-1)^n a_0$ as required. A similar type of argument shows that $a_{n-1} = -\mathrm{Tr}_{K(u)/K}(u)$.

As for part (v), let τ be a K-monomorphism from E to F and σ a K-monomorphism from K to E. Then

$$\begin{aligned}\mathrm{N}_{F/K}(u) &= \left(\prod_{\sigma,\tau} \sigma(\tau(u))\right)^{[F:K]_i} = \prod_\sigma \sigma\left(\prod_\tau \tau(u)\right)^{[F:K]_i} \\ &= \prod_\sigma \sigma\left(\left(\prod_\tau \tau(u)\right)^{[F:E]_i}\right)^{[E:K]_i} = \prod_\sigma \left(\mathrm{N}_{F/E}(u)\right)^{[E:K]_i} \\ &= \left(\prod_\sigma \sigma(\mathrm{N}_{F/E}(u))\right)^{[E:K]_i} = \mathrm{N}_{E/K}(\mathrm{N}_{F/E}(u)).\end{aligned}$$

One can employ a similar argument to derive the trace counterpart. □

26. November 20

Definition 26.1. Let S be a non-empty set of automorphisms of F. Then S is *linearly independent* if $a_1\sigma_1 + \cdots + a_n\sigma_n = 0$ for $\sigma_i \in S$ and $a_i \in F$ for all $1 \le i \le n$ implies $a_1 = a_2 = \cdots = a_n = 0$.

Lemma 26.1. *Any non-empty set of automorphisms on a field is linearly independent.*

Proof. Suppose otherwise, i.e., $S \neq \emptyset$ is a set of automorphisms on F that is not linearly independent. Thus there are $\sigma_1, \ldots, \sigma_n \in S$ and $a_1, \ldots, a_n \in F$ non-zero such that

$$a_1\sigma_1 + \cdots + a_n\sigma_n = 0. \tag{$\dagger$}$$

Then of all such relations, choose one with n minimal.

Suppose that $n > 1$ and $\sigma_1 \neq \sigma_2$. Let $v \in F$ be such that $\sigma_1(v) \neq \sigma_2(v)$, and let $u \in F$. Then apply ($\dagger$) to uv. Then ($\dagger$) becomes

$$a_1\sigma_1(u)\sigma_1(v) + a_2\sigma_2(u)\sigma_2(v) + \cdots + a_n\sigma_n(u)\sigma_n(v) = 0. \tag{$\dagger\dagger$}$$

Now apply ($\dagger$) to u, then multiply by $\sigma_1(v)$.

$$a_1\sigma_1(u)\sigma_1(v) + a_2\sigma_2(u)\sigma_1(v) + \cdots + a_n\sigma_n(u)\sigma_1(v) = 0. \tag{$\ddagger\ddagger$}$$

Subtract ($\ddagger\ddagger$) from ($\dagger\dagger$).

$$\sum_{k=2}^{n} a_k\sigma_k(u)(\sigma_k(v) - \sigma_1(v)) = 0.$$

But clearly $a_2(\sigma_2(v) - \sigma_1(v)) \neq 0$, so we have a contradiction to the minimality of n. □

Definition 26.2. Let F/K be an algebraic Galois extension. Then F/K is a *cyclic extension* if $\mathrm{Aut}_K F$ is cyclic. If $\mathrm{Aut}_K F$ is abelian, then F/K is said to be an *abelian extension*.

Example. If F/K is a finite extension and $\#K = q = p^r$ where $\mathrm{char}\, K = p$, then F/K is cyclic. In fact, we have a canonical generator given by the Frobenius map φ, where $\varphi(u) := u^q$ (i.e, $\mathrm{Aut}_K F = \langle\varphi\rangle$).

Theorem 26.1 (Kronecker-Weber theorem)**.** *Every finite-degree abelian extension over $\mathbb{Q}$ is contained in a cyclotomic field.*

The next theorem explores the connection of norm and trace to cyclic extensions.

Theorem 26.2. *Let F/K a cyclic extension of degree n; suppose $G = \mathrm{Aut}_K F = \langle\sigma\rangle$, and $u \in F$.*

(i) $\mathrm{Tr}(u) = 0$ *if and only if* $u = v - \sigma(:v)$ *for some* v *(i.e.,* $u \in \mathrm{im}(\mathrm{id} - \sigma)$*).*

(ii) (Hilbert's Theorem 90) $\mathrm{N}(u) = 1$ *if and only if* $u = v\sigma(v)^{-1}$ *for some* $v \neq 0$ *(i.e.,* $u \in \mathrm{im}(\mathrm{id}\,/\sigma)$*).*

Proof. Write $\mathrm{Aut}_K F = \{1, \sigma, \sigma^2, \ldots, \sigma^{n-1}\}$. Then $\mathrm{Tr} = 1 + \sigma + \sigma^2 + \cdots + \sigma^{n-1}$ and $\mathrm{N} = 1 \times \sigma \times \sigma^2 \times \cdots \times \sigma^{n-1}$. Note that F/K is separable by default, so there is no need to worry about the inseparable degree that might affect trace and norm. For any u, we have

$$\mathrm{Tr}(u) = \mathrm{Tr}(\sigma(u)) = \mathrm{Tr}(\sigma^2(u)) = \cdots = \mathrm{Tr}(\sigma^{n-1}(u))$$
$$\mathrm{N}(u) = \mathrm{N}(\sigma(u)) = \mathrm{N}(\sigma^2(u)) = \cdots = \mathrm{N}(\sigma^{n-1}(u)).$$

The above observation provides an easy proof for the ($\Leftarrow$) direction for both (i) and (ii). Note that

$$\mathrm{Tr}(v - \sigma(v)) = \mathrm{Tr}(v) - \mathrm{Tr}(\sigma(v)) = \mathrm{Tr}(v) - \mathrm{Tr}(v) = 0$$
$$\mathrm{N}(v\sigma(v)^{-1}) = \mathrm{N}(v)\,\mathrm{N}(\sigma(v))^{-1} = \mathrm{N}(v)\,\mathrm{N}(v)^{-1} = 1.$$

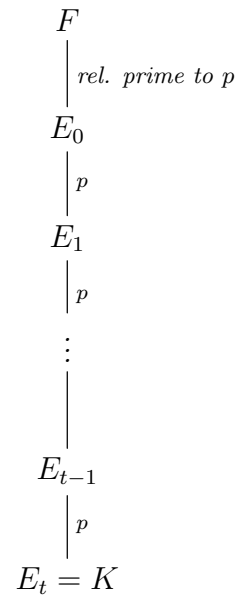
((i), $\Rightarrow$) For this direction, we need to show that if $u \in F$ and $\mathrm{Tr}(u) = 0$, then $u = v - \sigma(v)$ for some v. Choose an element w with $T(w) = 1$. Since $\{1, \sigma, \sigma^2, \ldots, \sigma^{n-1}\}$ is linearly independent, there exists $z \in F$ with $\mathrm{Tr}(z) = z + \sigma(z) + \cdots + \sigma^{n-1}(z) \neq 0$. But then $\mathrm{Tr}(z) \in K$, and Tr is K-linear; so if $w := \mathrm{Tr}(z)^{-1}z$, then $\mathrm{Tr}(w) = \mathrm{Tr}(\mathrm{Tr}(z)^{-1}z) = \mathrm{Tr}(z)^{-1}\,\mathrm{Tr}(z) = 1$. Then one can show that $u = v - \sigma(v)$ where

$$v := uw + (u + \sigma(u))\sigma(w) + (u + \sigma(u) + \sigma^2(u))\sigma^2(w) + \cdots + (u + \sigma(u) + \cdots + \sigma^{n-2}(u))\sigma^{n-2}(w).$$

(Verifying that this v works is left as an exercise.) $\square$

27. November 22

Proposition 27.1. *Let F/K be cyclic of degree n where $n = p^t m$ with p prime and $\gcd(p, m) = 1$. Then there is a chain of intermediate fields $E_0 \supseteq E_1 \supseteq \cdots \supseteq E_t = K$ such that F/E_0 is cyclic of order m and E_i/E_{i+1} is cyclic of order p for all i.*



Proof. $\operatorname{Aut}_K F$ is cyclic of order $n = p^t m$. Since $\operatorname{Aut}_K F$ is cyclic, all subgroups are normal, and all subextensions E/K are thus Galois. Since all the quotient and subgroups of a cyclic group are cyclic, it follows that all subextensions of F/K are cyclic. In other words, if $L \subseteq M$ are two intermediate fields, then M/L is cyclic. Now, let E_0 be the fixed field of the unique subgroup of $\operatorname{Aut}_K F$ of size m (per Galois correspondence). Therefore $[F : E_0] = m$, so E_0/K is cyclic of order p^t. So there is a chain of subgroups $H_1 \leq H_2 \leq \cdots \leq H_t = \operatorname{Aut}_K E_0$, where $\#H_j = p^j$. We can take advantage of the Galois correspondence in order to map over to the fixed fields to get the chain $E_1 \supseteq E_2 \supseteq \cdots \supseteq E_t = K$. □

Proposition 27.2. *Let* $\operatorname{char} K = p$. *Then F/K is cyclic of degree p if and only if F/K is the splitting field of an irreducible polynomial of the form $x^p - x - a \in K[x]$. In this case, if u is any root of $x^p - x - a$ in F, then $F = K(u)$.*

Proof. ($\Rightarrow$) Let F/K be cyclic of degree p. Then $\operatorname{Tr}(1) = [F : K] \cdot 1 = p \cdot 1 = 0$. So where $\operatorname{Aut}_K F = \langle \sigma \rangle$, there exists some v such that $1 = v - \sigma(v)$. Write $u = -v$, and let $a := u^p - u$. Note that $\sigma(u) = -\sigma(v) = 1 - v = 1 + u \neq u$. Thus $u \notin K$, so $F = K(u)$. Then $\sigma(a) = \sigma(u^p - u) = \sigma(u)^p - \sigma(u) = (u + 1)^p - (u + 1) = u^p + 1 - u - 1 = u^p - u$, so indeed $a \in K$. Hence $u \in F$ is a root of $x^p - x - a \in K[x]$, so $\deg u = p$ (since $F = K(u)$). Since $x^p - x - a$ is the minimal polynomial, it is irreducible also. Finally, if w is any root of $x^p - x - a$, then $F = K(w)$. So F is a splitting field of $x^p - x - a$ over K.

($\Leftarrow$) Let F/K be a splitting field of irreducible $x^p - x - a \in K[x]$. If u is any root of $x^p - x - a$, then all the roots are given by $u, u + 1, \ldots, u + p - 1$. Recall that $l^p = l$ for any $l \in \mathbb{F}_p$, so $(u + l)^p - (u + l) - a = u^p + l^p - u - l - a = u^p + l - l - u - a = u^p - u - a = 0$. Clearly $u, u + 1, \ldots, u + p - 1$ are all distinct; therefore, $x^p - x - a$ is separable, whence we

conclude F/K is Galois. But then F/K is Galois of order p, so $\#\operatorname{Aut}_K F = p$. Any group of prime order is cyclic, so $\operatorname{Aut}_K F$ is cyclic as desired. □

Definition 27.1. Let K be a field and $n \in \mathbb{N}$. Then $\zeta \in K$ is an *n-th root of unity* if $\zeta^n = 1$.

Proposition 27.3. *Let G be the set of the n-th roots of unity. Then G a subgroup of $K^\star$ such that $\#G \leq n$. Since G is finite, G is cyclic.*

Remark. Thus Proposition 27.3 implies that the n-th roots of unity in any field form a cyclic group of size n or smaller under multiplication.

Definition 27.2. $\zeta \in K$ is a *primitive n-th root of unity* if $\zeta^n = 1$ but $\zeta^d \neq 1$ for any $1 \leq d < n$.

Remark. Suppose that $\operatorname{char} K = p$. Then the following hold:

- If $p \mid n$ and $n = p^t m$ with $\gcd(p, m) = 1$, then $x^n - 1 = (x^m - 1)^{p^t}$ by virtue of the freshman's dream. In this case, there is no primitive n-th roots of unity, since all n-th roots of unity are actually m-th roots of unity.
- On the other hand, if $p \nmid n$, then $x^n - 1$ has distinct roots. Thus the set of n-th roots of unity is of size n and is cyclic. If ζ is a generator, then ζ is a primitive n-th root of unity.

Theorem 27.1. *Let K contain a primitive n-th root of unity ζ, and let F/K be a field extension. Then the following are equivalent:*

- *F/K is cyclic of degree dividing n.*
- *F/K is a splitting field over K of a polynomial of the form $x^n - a \in K[x]$.*
- *F/K is a splitting field extension over K for a polynomial of the form $x^d - a \in K[x]$ where $d \mid n$.*

28. November 23: Cyclotomic extensions

Definition 28.1. A *cyclotomic extension of order n over K* is a splitting field extension of $x^n - 1 \in K[x]$.

Remark. We only need to consider n not divisible by $\operatorname{char} K$. If $\operatorname{char} K = p$ and $p \mid n$, then we can write $n = p^t m$ where $\gcd(p, m) = 1$ and $t \geq 1$. Then $x^n - 1 = (x^m - 1)^{p^t}$, so any nth root of unity is mth root of uninty also. So either $\operatorname{char} K = 0$ or $\operatorname{char} K = p$ with $p \nmid n$, and then F is a cyclotomic extension of K of order n.

Definition 28.2. *Euler's φ-function* is an arithmetical function defined by

$$\varphi(n) := \#\{1 \leq m \leq n : \gcd(n, m) = 1\} = \#(\mathbb{Z}/n\mathbb{Z})^\times,$$

where $(\mathbb{Z}/n\mathbb{Z})^\times$ denotes the group of units modulo n (which is equivalent to invertible classes $m \bmod n$ such that $\gcd(n, m) = 1$).

Theorem 28.1. *Let ζ be a primitive nth root of unity.*

(i) *$F = K(\zeta)$.*
(ii) *$\operatorname{Aut}_K F$ is isomorphic to a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$.*
(iii) *F/K is abelian of degree dividing $\varphi(n)$. If n is prime, then F/K is not only abelian but also cyclic.*

Proof. (i) The nth roots of unity in F form a cyclic group of order n (since $x^n - 1$ has distinct roots). Let ζ be a generator. Then the nth roots of unity are $1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$, so $F = K(1, \zeta, \zeta^2, \ldots, \zeta^{n-1}) = K(\zeta)$.

(ii) F/K is the splitting field of separable polynomial $x^n - 1$, so F/K is Galois. For $\sigma \in \operatorname{Aut}_K F$, $\sigma(\zeta)$ is a root of $x^n - 1$; therefore $\sigma(\zeta) = \zeta^i$ for some i. But σ is an automorphism, so ζ and $\sigma(\zeta)$ must have the same order. In general, $\operatorname{ord}(\zeta^i) = \operatorname{ord}\zeta / \gcd(\operatorname{ord}\zeta, i) = n/\gcd(n, i)$. Therefore $\operatorname{ord}(\zeta^i) = n$ if and only if $\gcd(i, n) = 1$. Hence the elements of $\operatorname{Aut}_K F$ are determined by exponents i such that $\gcd(i, n) = 1$. It is a routine exercise to verify that the map from $\operatorname{Aut}_K F$ to $(\mathbb{Z}/n\mathbb{Z})^\times$ defined by $\sigma_i \mapsto i$ (where $\sigma_i(\zeta) = \zeta^i$) is a monomorphism.

(iii) Note $\#(\mathbb{Z}/n\mathbb{Z})^\times = \varphi(n)$, and $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic when n is prime. Thus (iii) follow from (ii), which we already proved. □

Remark. It is possible for $\operatorname{Aut}_K F$ to be isomorphic to a proper subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$. Let $\zeta \in \mathbb{C}$ be a primitive nth root of unity in $\mathbb{C}$. Consider the tower of extensions $\mathbb{R} \subseteq \mathbb{R}(\zeta) \subseteq \mathbb{C}$. $\mathbb{R}(\zeta)/\mathbb{R}$ has degree 1 or 2 since $[\mathbb{C} : \mathbb{R}] = 2$. But $(\mathbb{Z}/n\mathbb{Z})^\times$ has order $\varphi(n)$.

Definition 28.3. The *nth cyclotomic polynomial over K* $\Phi_n(x)$ is

$$\Phi_n(x) := \prod_{\substack{1 \le i \le n \\ \gcd(i,n)=1}} (x - \zeta^i),$$

where ζ is a primitive nth root of unity.

Proposition 28.1. *Let P be the prime subfield of K.*

(i) $x^n - 1 = \prod_{d \mid n} \Phi_d(x)$.

(ii) $\Phi_n(x) \in P[x]$.

Remark. If $\operatorname{char} K = 0$, then $P = \mathbb{Q}$, so coefficients lie in $\mathbb{Z}$.

Proof. (i) Partition the roots of $x^n - 1$ according to their order. Let $\prod_u$ denote the product across all the nth roots of unity, and let $\prod_d$ be the product of all the nth roots of unity whose order is d.

$$x^n - 1 = \prod_u (x - u) = \prod_{d \mid n} \prod_d (x - u) = \prod_{d \mid n} \Phi_d(x).$$

(ii) We will use induction for this claim. For $n = 1$, $\Phi_1(x) = x - 1 \in P[x]$. Now suppose that the claim holds for all $k < n$. Then

$$x^n - 1 = \prod_{d \mid n} \Phi_d(x) = \underbrace{\left(\prod_{\substack{d \mid n \\ d < n}} \Phi_d(x) \right)}_{=: f(x)} \Phi_n(x).$$

By the inductive hypothesis, we know $f(x) \in P[x]$. Thus

$$x^n - 1 = f(x)\Phi_n(x). \tag{1}$$

Now apply the division algorithm onto $x^n - 1, f(x) \in P[x]$. Then there exist unique $q, r \in P[x]$ with

$$x^n - 1 = f(x)q(x) + r(x), \tag{2}$$

where $r = 0$ or $\deg r < \deg f$. Compare (1) and (2) over F. Then by the uniqueness coming from the division algorithm, we conclude that $\Phi_n(x) = q(x)$. Thus $\Phi_n(x) \in P[x]$ as desired. □

Proposition 28.2. *Let $F = \mathbb{Q}(\zeta)$ where ζ is a primitive nth root of unity in $\mathbb{C}$. Then the following are true.*

(i) $\Phi_n(x)$ *is irreducible.*
(ii) $[F : \mathbb{Q}] = \varphi(n)$
(iii) $\operatorname{Aut}_{\mathbb{Q}} F = (\mathbb{Z}/n\mathbb{Z})^\times$.

Proof. (ii) and (iii) follow immediately from (i), so it suffices to only prove (i). We will, however, not prove (i) in full generality, but only when n is prime to illustrate a nice trick that can be applied in other settings. If $n = p$ is prime, then $\Phi_p(x) = (x^p - 1)/(x - 1) = x^{p-1} + x^{p-2} + \cdots + x + 1$. In fact,

$$\Phi_p(x + 1) = \frac{(x + 1)^p - 1}{x} = \sum_{i=1}^{p} \binom{p}{i} x^{i-1}.$$

Therefore $\Phi_p(x + 1)$ is irreducible since it is Eisenstein with respect to p. Hence $\Phi_p(x)$ is irreducible also. □

29. November 27: Radical extensions

Given a field K, does there exist a formula involving only field operations and extraction of roots which gives all the roots of all polynomials in $K[x]$? The answer is yes for the most part, as long as the polynomial in question is of degree 1, 2, 3, or 4. (We still say "for the most part" due to some extraordinary circumstances, e.g. for the quadratic formula the restriction $\operatorname{char} K \neq 2$ is needed since otherwise division by 2 makes no sense.) However, starting from degree 5, this is no longer true in general.

Definition 29.1. F/K is a *radical extension* if $F = K(u_1, \ldots, u_n)$ where, for each j, some power of u_j lies in $K(u_1, \ldots, u_{j-1})$. In other words, u_j is some roof of an element in $K(u_1, \ldots, u_{j-1})$.

Remark (Connection to the main problem). Given $f \in K[x]$, can we find a radical extension of K that contains all of the roots of f?

Definition 29.2. Let K be a field, and $f \in K[x]$. Then $f(x) = 0$ is *solvable by radicals* if there is a radical extension of K that contains a splitting field of F.

Lemma 29.1. *Let F/K be a radical extension, and let N/K be the normal closure of F/K. Then N is also a radical extension.*

Before proving this, we need to prove the following two claims.

Lemma 29.2. *The proof of Lemma is immediate from the next two lemmas. If F/K is any finite-dimensional extension, then $N = E_1E_2 \cdots E_r$ for suitable subfields E_j of N, each isomorphic to F.*

Proof. Let $\{w_1, w_2, \ldots, w_n\}$ be a basis for F/K, and $f_1, f_2 \cdots f_n \in K[x]$ be the corresponding minimal polynomials. Let v be any root of f_j for some j. Then there is a K-isomorphism $\sigma : K(w_j) \to K(v)$ such that $w_j \mapsto v$. Then there is an extension $\tau \in \operatorname{Aut}_K N$ since N/K is normal. Thus $\tau(F)$ is a subfield of N that is isomorphic to F and contains $v = \tau(w_j)$. Continuing this process yields subfields $E_1, \ldots, E_r \subseteq N$, each of which is isomorphic to F, and all roots of f_j lie in $E_1 E_2 \cdots E_r$. By virtue of the minimality of r, $E_1 E_2 \cdots E_r = N$. □

Lemma 29.3. *Composites of radical extensions are themselves radical.*

Proof. This is fairly straightforward; start with the two fields, and then try to prove this by induction. □

Definition 29.3. Let G be a group. Then the *commutator subgroup* of G, denoted by G' or $G^{(1)}$ is the subgroup of G generated by $\{aba^{-1}b^{-1} : a, b \in G\}$. $G^{(n)}$ is the *nth derived subgroup of* G. $G^{(n)}$ is equal to the commutator subgroup of $G^{(n-1)}$.

Upon taking the commutator subgroup multiple times, we obtain a sequence

$$G \geq G^{(1)} \geq G^{(2)} \geq \cdots \geq G^{(i)} \geq \cdots$$

which may or may not terminate.

Definition 29.4. If the sequence of commutator subgroups of G terminates eventually (i.e., $G^{(n)} = \langle e \rangle$), then G is *solvable*.

Remark. If G is abelian, then $G^{(1)} = \langle e \rangle$ (i.e., G is solvable).

Definition 29.5. A *solvable series* of a group is a subnormal series with simple quotients.

Remark. G is solvable if and only if G has a solvable series.

30. November 30

Theorem 30.1. *Let F/K be a radical extension, and let E be an intermediate field. Then $\operatorname{Aut}_K E$ is solvable.*

Proof (sketch). The proof has two parts.

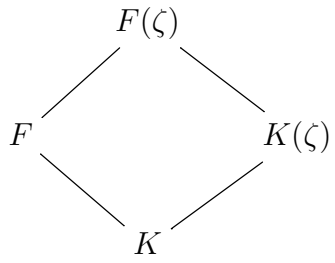
(I) Reduce the problem to showing that if F/K is Galois and radical, then $\operatorname{Aut}_K F$ is solvable.

(a) Prove that we may assume E/K is Galois.
Let $K_0 = (\operatorname{Aut}_K E)'$. Then E/K_0 is Galois with group $\operatorname{Aut}_{K_0} E = \operatorname{Aut}_K E$. F/K is radical, so F/K_0 is radical as well (if necessary, replace K with K_0. Thus we can assume that E/K is Galois.

(b) If N/K is the normal closure of F/K, then it is sufficient to show that $\operatorname{Aut}_K N$ is solvable.
If E/K, then E is stable with respect to $\operatorname{Aut}_K N$. Then the map $\theta : \operatorname{Aut}_K N \to \operatorname{Aut}_K E$ with $\sigma \mapsto \sigma|_E$ is surjective as N/K is normal. But homomorphic images of a solvable group are always solvable; and since θ is surjective, $\operatorname{Aut}_K E$ is solvable also.

(c) Now we can assume that N/K is Galois; switch back to the original notation by setting $N = F$.
N/K is normal, so if it is not Galois, then one can trade in K for the fixed field of $\operatorname{Aut}_K N$ just as we did in part (a).

(d) Proof of (I)
Let $F = K(u_1, \ldots, u_n)$. Then $u_i^{m_i} \in K(u_1, \ldots, u_{i-1}$ for all i. Thus we can assume that each m_i is prime to $\operatorname{char} K$ because one can replace m_i with r where $m_i = p^t r$ and $p^t \| m_i$. If $m = m_1 m_2 \cdots m_n$, and ζ is a primitive mth root of unity, then it suffices to prove that $\operatorname{Aut}_K F(\zeta)$ is solvable; in turn, it suffices to prove that $\operatorname{Aut}_{K(\zeta)} F(\zeta)$ is solvable. The proof is complete once we construct a solvable series, which shall be done in Part (II).



(II) Use roots of unity to construct a solvable series for a related extension.
Now we are ready to construct a solvable series. Let $H_n = \langle e \rangle \leq \cdots \leq H_i := \operatorname{Aut}_{E_i} F(\zeta) \leq \cdots \leq H_n = \operatorname{Aut}_{K(\zeta)} F(\zeta)$, where $E_i := K(\zeta, u_1, \ldots, u_i)$ for each i (note that $E_n = F(\zeta) \supseteq \cdots \supseteq E_i \supseteq \cdots \supseteq E_0 = K(\zeta)$ forms a tower of field extensions). This is a solvable series. □

Corollary 30.1. *Let $f \in K[x]$. If $f(x) = 0$ is solvable by radicals, then the Galois group of f is solvable.*

Proof. $f(x) = 0$ is solvable by radicals if and only if there is a splitting field E of f over K contained in a radical extension of K. So by Theorem 30.1, $\operatorname{Aut}_K E$ is solvable. Thus the Galois group of f is the Galois group of a splitting field extension of f over K. □

Corollary 30.2. *The general quintic is not solvable by radicals.*

Proof. Recall that if $f \in \mathbb{Q}[x]$ is of degree p for some prime p, and is irreducible over $\mathbb{Q}$, then f has exactly two non-real roots in $\mathbb{C}$. Thus the Galois group of f is (isomorphic to) S_5. However, S_5 is not solvable. □

Example. $f(x) = x^5 - 4x + 2 \in \mathbb{Q}[x]$ is irreducible by Eisenstein (with respect to 2). Sketching the graph shows that f has exactly three real roots, so the Galois group is S_5, which is not solvable.

Department of Mathematics and Statistics, Dalhousie University, 6316 Coburg Rd, Halifax, NS, Canada B3H 4R2
E-mail address: hsyang@dal.ca