MATH70037 Galois theory :: Lecture notes

Lecturer: Alexei Skorobogatov

Last edited: 19th May 2025

Contents

Week 2, lecture 1, 8th October

History and motivation

Évariste Galois (1811 Bourg-la-Reine–1832 Paris) was a human being and the namesake of this module.

The theory originates from the question of solving polynomials. We know all about the quadratic equation $x^2 + bx + c = 0$ where $b, c \in \mathbb{Q}$: we use the Babylonian completing the square and obtain $x = \dfrac{-b \pm \sqrt{b^2 - 4c}}{2}$. The cubic $x^3 + px + q$ took people more time, and Cardano eventually arrived at

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

A quartic equation is also solvable (meaning we can write down a general formula for its roots) but the formula takes too many pages so it's ommitted here.

It turned out that quintics are not solvable. The genius of Galois was this big new idea: associate to a polynomial a certain finite group (which was a concept invented by Galois as well), now called the Galois group. Consider a field K (an abelian group for addition and multiplication (without 0)) and

$$\mathrm{Aut}(K) = \{\text{bijective } g : K \to K : \forall x, y \in K,\ g(x+y) = g(x) + g(y), g(xy) = g(x)g(y)\},$$

the set of automorphisms of K, which is a group under composition.

The case for $K = \mathbb{Q}$ is simple since any $g \in \mathrm{Aut}(\mathbb{Q})$ respects 1 and any element in $\mathbb{Q}$ is $\frac{r}{s} = \dfrac{\overbrace{1 + \cdots + 1}^{r}}{\underbrace{1 + \cdots + 1}_{s}}$, hence $\mathrm{Aut}(\mathbb{Q}) = \{\mathrm{id}\}$. The case for e.g. $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}))$ where $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ is a bit more intersting. Consider $\sqrt{2}$ as the solution to $x^2 - 2 = 0$. Since $g \in \mathrm{Aut}(\mathbb{Q}(\sqrt{2}))$ respects addition and multiplication, one has $g(x)^2 - 2 = 0$, hence either $\sqrt{2} \mapsto \sqrt{2}$ (then $g = \mathrm{id}$) or $\sqrt{2} \mapsto -\sqrt{2}$. We claim that $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})) \cong \mathbb{Z}/2$ and we will later see some formal and general justification. In this case, we say the Galois group of $x^2 - 2$ is $\mathbb{Z}/2$.

In general, if $f(x)$ is a polynomial of degree n over a field, its Galois group is a subgroup of S_n. It turns out that if an equation is solvable by radicals then its Galois group is solvable, i.e. G has a chain of subgroups $G = G_0 \supset G_1 \supset G_2 \supset \cdots$ such that G_i is a normal subgroup of G_{i-1} and G_{i-1}/G_i is cyclic. In particular, every cyclic group if solvable. S_3 is solvable since $S_3 \supset \{e, (123), (132)\} \cong \mathbb{Z}/3 \supset \{e\}$. S_4 is too, but S_5 is not; recall that the only nontrivial proper normal subgroup of S_n is A_n for $n \geq 5$ and A_n is simple for $n \geq 5$. Quintics are therefore not generally solvable since there are some quintics with Galois group S_5.

Galois theory is not just some smart trick to solve a classical problem. The core of the theory, the Galois correspondence, provides an essential philosophy in e.g. topology.

Week 2, lecture 2, 11th October

1 Field extensions

1.1 Definitions

Recall definitions of a ring (we always assume $1 \in R$), a ring homomorphism (importantly $f(1) = 1$) and a field (commutative multiplication with inverses).

Remark 1.1.1. If $f : R_1 \to R_2$ is a homomorphism of rings, then $\ker f$ is an ideal in R_1. For every ideal we associate a quotient ring R/I and $R_1/\ker f \to R_2$ is injective.

Remark 1.1.2. In this module we are primarily interested in fields, which is boring since their only ideals are 0 and itself; indeed, if $a \in I \lhd \mathbb{F}$ where $a \neq 0$ then by definition of an ideal, $a^{-1}a = 1 \in I$ so $x = x \cdot 1 \in I\ \forall x \in \mathbb{F}$. As a result, any homomorphism of fields is injective; indeed, consider a field homomorphism $f : K \to L$ and $\ker f$ as an ideal of K is either 0 or K, but $\ker f \neq K$ since $1 \notin \ker f$ by definition of a ring homomorphism. In this sense, every field homomorphism is an *embedding*, i.e. a small field sits inside a bigger one, or that every field is an *extension* of another.

Definition 1.1.3. $\mathrm{Emb}(K, L) := \{f : K \hookrightarrow L\}$ is the set of embeddings of K into L.

$\mathrm{Aut}(K) = \mathrm{Emb}(K, K)$ is the set of embeddings of K into itself, i.e. *automorphisms*.

Definition 1.1.4. *Low-level definition*: the *characteristic* of a field K is the smallest p such that $\underbrace{1 + \cdots + 1}_{p} = 0$.

If such p exists, write $\mathrm{char}\, K = p$ and if not, write $\mathrm{char}\, K = 0$. It turns out p is always prime.

A higher-level definition: there is a unique ring homomorphism $f : \mathbb{Z} \to R$ since $\mathbb{Z} = (1)$ and $f(1) = 1$. Since $\mathbb{Z}$ is a PID, $\ker f = (p)$ for some $p \in \mathbb{Z}$. We call p the *characteristic* of R.

Example 1.1.5. All finite fields have posiitve characteristic, but also $\mathbb{F}_p(t) := \left\{ \frac{\sum a_i t^i}{\sum b_j t^j} : a_i \in \mathbb{F}_p, b_j \in F_p \right\}$. In some way one can think of $\mathbb{F}_p$ as the smallest field with characteristic p and any field containing it will have the same char, similarly for $\mathbb{Q}$ with $\mathrm{char}\, \mathbb{Q} = 0$.

1.2 Finite extensions

Definition 1.2.1. Let $K \subset L$ be fields, i.e. we have an extension of fields. Then L is a vector space over K (easy to check by definition). Such an extension is *finite* if L is a finite-dimensional K-vector space. We call $\dim_K L$ the *degree* of extension, write it as $[L : K]$.

Theorem 1.2.2 (Tower law)**.** If $\mathbb{F} \subset K \subset L$ are finite extensions of fields, then

$$[L : \mathbb{F}] = [L : K] \cdot [K : \mathbb{F}]$$

Example 1.2.3. For any field K, $K(t)$ where t is a variable is not a finite extension.

Definition 1.2.4. Let $K \subset L$ be a finite extension of fields. Take $\alpha \in L$ and suppose n is the smallest number such that $1, \alpha, \ldots, \alpha^{n-1}$ are linearly dependent (such n exists since every $[L : K] + 1$ elements are linearly dependent). This means $\exists a_0, \ldots, a_{n-1} \in K$ not all equal to 0 such that

$$a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0 \qquad \text{where } a_{n-1} \neq 0$$

Since K is a field, WLOG one can assume $a_{n-1} = 1$. Hence we've found a monic polynomial $f \in K[x]$ of least degree such that $f(\alpha) = 0$. This is the *minimal polynomial* of α.

A higher-level definition: consider the ring homomorphism $\varphi_\alpha : K[x] \to L : x \mapsto \alpha$. Since $K[x]$ is a PID (see below), $\ker \varphi_\alpha = (f)$ for some $f \in K[x]$. Since $\dim_K L$ is finite, $\ker \varphi_\alpha$ contains the characteristic polynomial of α (consider α as a K-linear map $L \to L : v \mapsto \alpha v$ and Caylet–Hamilton theorem), so $f \neq 0$. We call f the *minimal polynomial* of α.

Week 2, lecture 3, 11th October

Let K be a field and consider the ring $K[x]$. Euclid's algorithm works: for $f, g \in K[x]$ one has $f = qg + r$ where $r = 0$ or $\deg r < \deg g$, i.e. $K[x]$ is a Euclidean ring, in particular is a PID. Prime ideals in $K[x]$ are exactly maximal ideals, which are generated by irreducible polynomials. Hence if $f \in K[x]$ is irreducible then $K[x]/(f) =: L$ is a field. Note that a minimal polynomial by its naive definition must be irreducible, so we can reverse the construction of an extension by starting with a polynomial.

L has a basis consisting of images of $1, x, x^2, \ldots, x^{d-1}$ where $d = \deg f$; indeed, $f(x) = x^d + a_{d_1}x^{d-1} + \cdots + a_0 = 0 \in L$, i.e. $x^d = -(a_{d-1}x^{d-1} + \cdots + a_0)$ and with this any higher power of x can be expressed with lower powers. In particular, $[L : K] = d$.

Now let $\alpha \in L$ be the image of x, then $f(\alpha) = 0$, i.e. f has a root in L.

How do we connect the above with the definition of a minimal polynomial?

Definition 1.2.5. Let $K \subset L$ and $\alpha \in L$. Define $K(\alpha)$ to be the smallest subfield of L containing K and α (the intersection of all subfields of L containing K and α).

Explicitly, $K(\alpha)$ is spanned by $1, \alpha, \ldots, \alpha^{d-1}$ where d is the degree of minimal polynomial of α. This is indeed closed under division: any nonzero element can be written as $b_{d-1}\alpha^{d-1} + \cdots + b_1\alpha + b_0$, so $\exists g \in K[x]$ with $\deg g < d$ such that this element is $g(\alpha)$. Then f and g are coprime by definition of minimal polynomial, hence $\exists r, s \in K[x] : rf + sg = 1 = sg \in K[x]/(f)$, i.e. we found an inverse of $g(\alpha)$ in L to be $s(\alpha)$.

Proposition 1.2.6. $K(\alpha) \cong K[x]/(f)$ where f is the minimal polynomial of α.

Proof. Consider $\varphi : K[x] \to K(\alpha) : x \mapsto \alpha$.

- φ is surjective: for an element $a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1}$ we simply set $f \in K[x]$ to be $a_0 + a_1 x + \cdots + a_{d-1}x^{d-1}$.
- $\ker\varphi$ is all polynomials vanishing at α, which by the higher-level definition is generated the minimal polynomial.

□

Let $K \subset L$ be an extension of fields and $\alpha_1, \ldots, \alpha_n \in L$. Define $K(\alpha_1, \ldots, \alpha_n)$ to be the smallest subfield of L containing K and $\alpha_1, \ldots, \alpha_n$. Explicitly, we consider the chain of extensions $K \subset K(\alpha_1) \subset K(\alpha_1, \alpha_2) \subset \cdots K(\alpha_1, \ldots, \alpha_n)$. Again $K(\alpha_1, \ldots, \alpha_n)$ is a K-vector space spanned by finitely many monomials $\alpha_1^{r_1}, \ldots, \alpha_n^{r_n}$.

Lemma 1.2.7. Let $k \subset K$ be a finite field extension. Then there are $\alpha_1, \ldots, \alpha_n \in K : K = k(\alpha_1, \ldots, \alpha_n)$. We say $\alpha_1, \ldots, \alpha_n$ *generate* K over k.

Proof. Assume $k \neq K$ and take any $\alpha_1 \in K \backslash k$. Consider $k(\alpha_1) \subset K$. If $k(\alpha_1) = K$ then stop. Otherwise, $\exists \alpha_2 \in K \backslash k(\alpha_1)$ and one proceeds. By definition, $k(\alpha_1)(\alpha_2) = k(\alpha_1, \alpha_2)$ as expected. This process terminates after finitely many steps by the tower law. □

Week 3, lecture 1, 15th October

Example 1.2.8. Consider $\mathrm{Aut}(\mathbb{Q}(\sqrt{a}))$ where a is not a square in $\mathbb{Q}$. We claim it is $\{\mathrm{id}, \text{“conjugation”}\}$ (see also observation in History and motivation). Note that by previous argument, $\varphi(x) = x \ \forall x \in \mathbb{Q} \ \forall \varphi \in \mathrm{Aut}(\mathbb{Q}(\sqrt{a}))$, so

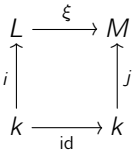
$$\varphi(x + y\sqrt{a}) = \varphi(x) + \varphi(y)\varphi(\sqrt{a}) = x + y\varphi(\sqrt{a}),$$

i.e. $\varphi(\sqrt{a})$ determines φ. Now $\varphi((\sqrt{a})^2) = (\varphi(\sqrt{a}))^2 = a$, so $\varphi(\sqrt{a}) = \pm\sqrt{a}$.
Now consider $\mathrm{Emb}(\mathbb{Q}(\sqrt{a}), \mathbb{Q}(\sqrt{b}))$ where a, b are not squares in $\mathbb{Q}$ and $a \neq bc^2 \ \forall c \in \mathbb{Q}$. We claim this is $\varnothing$, since $\varphi(\sqrt{a})$ is still a root of $x^2 = a$ by above, but suppose for $x, y \in \mathbb{Q}$

$$a = (x + y\sqrt{b})^2 = x^2 + 2xy\sqrt{b} + y^2 b,$$

so $2xy = 0$, i.e. either x or $y = 0$. If $x = 0$ then $a = y^2 b$, if $y = 0$ then $a = x^2$, both contradicting assumption.

Definition 1.2.9. Suppose $k \subset L$ is a field extension and $k \subset M$ is another. Define $\mathrm{Emb}_k(L, M)$ to be the set of all embeddings of L into M which are identity on k, i.e. the set of homomorphisms $\xi : L \to M$ such that $\xi i = j$.
Similarly define $\mathrm{Aut}_k(L)$, the *automorphism group* of L over k.

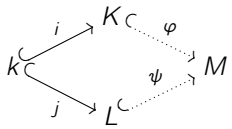


Example 1.2.10. $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{C}) = \mathrm{Aut}(\mathbb{C})$ by above.

$\mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$ similarly is determined by $\varphi(i) = \pm i$, so again it's isomorphic to $\mathbb{Z}/2$.

Remark 1.2.11. If $K \subset L$ and $K \subset M$ are field extensions and $[L : K] < \infty$, then $\mathrm{Emb}_K(L, M)$ is a finite set. Using 1.2.7, we write $L = K(\alpha_1, \ldots, \alpha_n)$ for some $\alpha_i \in L$. Suppose $\xi : L \to M$ fixes K (or is K-linear), so it is determined by $\xi(\alpha_i)$. Let f_i be minimal polynomials of α_i over K. Then $0 = \xi(f_i(\alpha_i)) = f_i(\xi(\alpha_i))$, i.e. $\forall i \ \xi(\alpha_i)$ is a root of f_i, but there are finitely many such possibilities.

Proposition 1.2.12. If $k \subset K$ and $k \subset L$ are field extensions such that $[K : k] < \infty$, then $\exists M : k \subset M$ and both K, L have k-linear embeddings into M. Moreover, M can be chosen to be such that $[M : L] < \infty$.



We want φ and $\psi : \varphi i = \psi j$.

Proof. Induction on $d = [K : k]$. If $d = 1$, i.e. $K = k$, we take $M = L$.
If $d \geq 2$, let $a \in K \backslash k$ and $f(x)$ be the minimal polynomial of a over k. Consider $k' = k[x]/(f) \cong k(a)$ with the map $x \mapsto a$. This is therefore an embedding of k' into K with image $k(a)$.

Week 3, lecture 2, 18th October

Now note that $[k' : k] = \deg f \geq 2$. The tower law implies that $[K : k'] < d$, Consider f as an element of $L[x]$. Let $g \in L[x]$ be an irreducible factor of f in $L[x]$ and consider $L' = L[x]/(g)$. This is a field extension of L. Denote by b the image of x in L', then $g(b) = 0$, so $f(b) = 0$. We have a natural map $k[x] \hookrightarrow L[x] \twoheadrightarrow L'$ and f is in its kernel, but f is irreducible and monic so it must generate the kernel (which is a principal ideal), so in particular k' embeds into L'. Now by inductive hypothesis one can find M such that K, L' embed k'-linearly into M, but by above one has K, L embed k-linearly into M as well since $L \subset L'$ and $k \subset k'$. □

1.3 Normal extensions

Definition 1.3.1. Let k be a field and $f \in k[x]$ be monic. A finite field extension $K \supset k$ is a *splitting field* of f if f completely splits in K, i.e. $f(x) = \prod_{i=1}^{n}(x - \alpha_i)$ for some $\alpha_i \in K$ and $K = k(\alpha_1, \ldots, \alpha_n)$, i.e. K is the smallest field containing k and all roots of f.

Proposition 1.3.2. Every polynomial $f \in k[x]$ has a splitting field which is unique up to k-linear isomorphism.

Proof. Induction on $n = \deg f$. If $n = 1$ then the root of f is in k so k is a splitting field. Now suppose $n \geq 2$. Choose an irreducible factor g of f and define $L = k[x]/(g)$, which is a field extension of k. Let α be the image of x in L, then $g(\alpha) = 0$, so $f(\alpha) = 0$, in particular $\frac{f(x)}{(x-\alpha)} \in L[x]$ and it has degree strictly less than n, so by inductive hypothesis it has a splitting field $K \supset L$. But then K is the splitting field of f as well.

Week 3, lecture 3, 18th October

Now suppose $K, L \supset k$ are splitting fields of $f \in k[x]$. By 1.2.12, $\exists \varphi : K \to M, \psi : L \to M$ such that φ, ψ are k-linear homomorphisms. Write $K = k(\alpha_1, \ldots, \alpha_n)$ and $L = k(\alpha'_1, \ldots, \alpha'_n)$. Let $\beta_1, \ldots, \beta_n$ be roots of f in M. Then

$$\varphi(f(x)) = \psi(f(x)) = f(x) = \prod_{i=1}^{n}(x - \beta_i) = \prod_{i=1}^{n}(x - \varphi(\alpha_i)) = \prod_{i=1}^{n}(x - \psi(\alpha'_i)),$$

so $\varphi(\alpha_i) = \psi(\alpha'_i) = \beta i \ \forall i$, hence $K \cong \varphi(K) = \psi(L) \cong L$. □

Definition 1.3.3. An extension of fields $L \supset k$ is *normal* if for any two k-linear embeddings $\psi_1, \psi_2 : L \hookrightarrow M$ there a k-automorphism $\sigma : L \to L : \psi_2 = \psi_1\sigma$.

i.e. $L \supset k$ is normal if the map $\mathrm{Aut}_k(L) \to \mathrm{Emb}_k(L, M)$ given by composing with some embedding of L into M is bijective.

Example 1.3.4. The extension $L \supset k$ where $k = \mathbb{Q}, L = \mathbb{Q}[x]/(x^2 - 2)$ is normal. Take $M = \mathbb{C}$ and define ψ_1 by $\mathbb{Q}[x] \to M : x \mapsto \sqrt{2}$ and ψ_2 by $x \mapsto -\sqrt{2}$. One sees that $\sigma : x \mapsto -x$ is the desired automorphism.
But now let $L = \mathbb{Q}[x]/(x^3 - 2)$ and define ψ_1 by $x \mapsto \sqrt[3]{2}$ and ψ_2 by $x \mapsto \sqrt[3]{2}e^{\frac{2\pi i}{3}}$. We claim $\nexists$ such σ and therefore $L \supset k$ is not normal, since $\psi_1(L) \subset \mathbb{R}$ and $\psi_2(L) \not\subset \mathbb{R}$, in particular $\psi_1(L) \neq \psi_2(L)$.

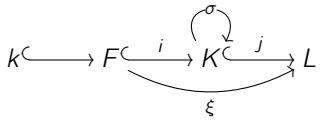
Remark 1.3.5. $L \supset k$ is normal $\iff \psi_1(L) = \psi_2(L)$ $\forall k$-linear embeddings $\psi_1, \psi_2 : L \hookrightarrow M$.

Proof. $\psi_2 = \psi_1\sigma$ where $\sigma \in \mathrm{Aut}_k(L) \implies \psi_1(L) = \psi_2(L)$ is clear. The converse is also clear via the diagram on the right since $\psi_1 : L \to \psi_1(L)$ and $\psi_2 : L \to \psi_2(L)$ are bijections. □

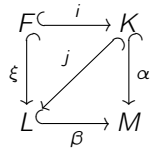
$$\begin{array}{ccc} L & \xrightarrow{\psi_1} & \psi_1(L) \\ {\scriptstyle\sigma}\,\vdots & & \| \\ L & \xrightarrow[\psi_2]{} & \psi_2(L) \end{array}$$

Week 4, lecture 1, 22nd October

Lemma 1.3.6. Let $k \hookrightarrow F \overset{i}{\hookrightarrow} K \overset{j}{\hookrightarrow} L$ be finite field extensions where i and j are k-linear and $K \supset k$ is normal. Then any k-linear embedding $\xi : F \hookrightarrow L$ is equal to the composition $\xi = j\sigma i$ where $\sigma \in \mathrm{Aut}_k(K)$.



In particular, the image of any embedding $F \hookrightarrow L$ is contained in K. Informally, F "cannot escape" from K.



Proof. Since $F \subset K$ and $F \subset L$, by 1.2.12, $\exists M, \alpha, \beta : \alpha : K \to M, \beta : L \to M$ are F-linear (in particular k-linear) embeddings so that $\alpha i = \beta \xi$. Notice by the diagram that K has two ways of embedding into M: βj and α. But $K \supset k$ is normal, so by definition $\exists \sigma \in \mathrm{Aut}_k(K) : \alpha = \beta j \sigma$. Then $\alpha i = \beta j \sigma i = \beta \xi$, so $\xi = j \sigma i$ since β is injective. □

Corollary 1.3.7. Same setup as previous lemma, then the map $\mathrm{Aut}_k(K) \to \mathrm{Emb}_k(F, L) : \sigma \mapsto j \sigma i$ is surjective.

Proof. This is simply another way of stating the lemma. □

Remark 1.3.8. An important case of above is taking $K = L$, then any the corollary says any k-linear embedding of F into a normal extension K of k is obtained from one such embedding by composing with a k-linear automorphism of K.

Theorem 1.3.9 (Main theorem of normal extensions)**.** For a finite field extension $K \supset k$, the following are equivalent:

1. $K \supset k$ is normal.
2. K is a splitting field of some $f \in k[x]$.
3. For any irreducible $g \in k[x]$, either g has no roots in K or all of its roots are in K. One out, all out!

Proof. $2 \implies 1$: Let K be a splitting field of $f \in k[x]$ and L an extension of k with $\psi : K \hookrightarrow L$ a k-linear embedding. It suffices to show $\psi(K)$ does not depend on choice of ψ. Note that f splits completely in $\psi(K) \cong K$ and $L \supset K$. Let $\alpha_1, \ldots, \alpha_n$ be roots of f in L, but then $k(\alpha_1, \ldots, \alpha_n) \cong \psi(K)$ by 1.3.2, in particular $\psi(K)$ does not depend on ψ since roots of $f \in k(x)$ does not depend on ψ.

$3 \implies 2$: Since $K \supset k$ is finite, one has $\alpha_1, \ldots, \alpha_n \in K : K = k(\alpha_1, \ldots, \alpha_n)$ by 1.2.7. Let $f_i \in k[x]$ be the minimal polynomial of α_i. Then each f_i splits completely in K, so $f = \prod_{i=1}^n f_i$ splits completely in K. Hence K is a splitting field of f.

$1 \implies 3$: Let $g \in k[x]$ be irreducible with $g(\alpha) = 0$ for some $\alpha \in K$ and $L \supset k$ be a splitting field of g. By 1.2.12, $\exists M \supset k : K$ and L embed k-linearly into M. Let β be any other root of g in M and we want to show $\beta \in K$. Consider $F = k[x]/(g) \cong k(\alpha) \cong k(\beta)$. One has two embeddings $F \hookrightarrow K : x \mapsto \alpha$ and $F \hookrightarrow M : x \mapsto \beta$. But since $K \supset k$ is normal, by 1.3.6, the image of any embedding $F \hookrightarrow M$ is in K, in particular $\beta \in K$. □

Week 4, lecture 2, 25th October

Corollary 1.3.10. Let $K \supset L \supset k$ be finite field extensions. If $K \supset k$ is normal then $K \supset L$ is normal.

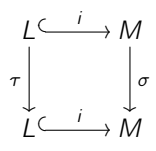
Proof. By 1.3.9, $\exists f \in k[x] : K$ is its splitting field. But then clearly K is also a splitting field of $f \in L[x]$. □

Example 1.3.11. We've seen $\mathbb{Q}(\sqrt[3]{2}) \supset \mathbb{Q}$ is not normal (now with 1.3.9, this is easily seen by considering the irreducible $f(x) = x^3 - 2$ with $e^{\frac{2\pi i}{3}} \sqrt[3]{2} \notin \mathbb{Q}(\sqrt[3]{2})$). But we can embed $\mathbb{Q}(\sqrt[3]{2})$ into a larger field $\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$, which is normal over $\mathbb{Q}$.

Proposition 1.3.12. Let $L \supset k$ be a finite field extension. Then $\exists f \in k[x]$ such that L embeds k-linearly into a splitting field of f. In particular, any finite field extension of k can be embedded k-linearly into a normal extension.

Proof. By 1.2.7, write $L = k(\alpha_1, \ldots, \alpha_n)$. Let f_i be the minimal polynomials of α_i over k and M be a splitting field of $f = \prod_{i=1}^n f_i$ over L. But by construction $L = k(\alpha_1, \ldots \alpha_n)$ where $\alpha_1, \ldots, \alpha_n$ are roots of f, so M is a splitting field of $f \in k[x]$ as well. □

Proposition 1.3.13. Let $M \supset L \supset K$ be finite field extensions. If $L \supset K$ is normal, then $\mathrm{Aut}_L(M)$ is a normal subgroup of $\mathrm{Aut}_K(M)$. Moreover, there is an injective homomorphism $\mathrm{Aut}_K(M)/\mathrm{Aut}_L(M) \to \mathrm{Aut}_K(L)$. If one also supposes $M \supset K$ is normal, then the above is surjective.



Proof. Let $i \in \mathrm{Emb}_K(L, M)$. By definition of normality, for any $\sigma \in \mathrm{Aut}_K(M)$, $\exists! \tau \in \mathrm{Aut}_K(L) : \sigma i = i \tau$. One therefore has the group homomorphism $\mathrm{Aut}_K(M) \to \mathrm{Aut}_K(L) : \sigma \mapsto \tau$. Its kernel is clearly $\mathrm{Aut}_L(M)$, which is therefore a normal subgroup of $\mathrm{Aut}_K(M)$.

Now suppose $M \supset K$ is normal and take any $\tau \in \mathrm{Aut}_K(L)$. Note that both $i, i\tau \in \mathrm{Emb}_K(L, M)$, so $\exists \sigma \in \mathrm{Aut}_K(M) : i\tau = \sigma i$. □

Week 4, lecture 3, 25th October: example class

Recall Gauss' lemma and Eisenstein's criterion.

Week 5, lecture 1, 29th October

1.4 Separable extensions

Definition 1.4.1. A polynomial $f \in K[x]$ is *separable* if in its splitting field, its roots are pairwise distinct, i.e. no roots with multiplicity.

Proposition 1.4.2. f is separable $\iff \gcd(f, f') = 1$.

Proof. Let L be a splitting field of f. If f is not separable, then one can write $f(x) = (x-\lambda)^2 g \in L[x]$. Then $f' = (x-\lambda)^2 g' + 2(x-\lambda)g$, so $x - \lambda \mid f, f'$.

Now suppose $x-\lambda \mid f, f'$ and write $f = (x-\lambda)g$. Then $f' = (x-\lambda)g' + g$, so $x-\lambda \mid g$ and hence $(x-\lambda)^2 \mid f$. □

Corollary 1.4.3. For an irreducible $f \in K[x]$, if $\operatorname{char} K = 0$ then f is separable, and if $\operatorname{char} K = p$ then f is inseparable $\iff \exists g \in K[x]$ irreducible such that $f = g(x^p)$.

Proof. Since f is irreducible, $\gcd(f, f') = 1$ or f, but $\deg f' < \deg f$ and $f \nmid f'$ (we can rule out $f' = 0$ since $\operatorname{char} K = 0$) so $\gcd(f, f') = 1$ and hence f is separable.

Now if $\operatorname{char} K = p$ then $\gcd(f, f') \neq 1 \iff f' = 0$, which happens only if the powers are all divisible by p, i.e. f is of the desired form. □

Example 1.4.4. Consider $K = \mathbb{F}_p(T)$ and $f(x) = x^p - T \in K[x]$, which is irreducible by Eisenstein, and by the corollary above it's inseparable. Now a root u of f is in $K[x]/(x^p - T)$, which is the image of x under the natural quotient map. But then $x^p - T = (x-i)^p$ since all binomial coefficients between are divisible by p, so f is *totally inseparable*: it has only one root. (Note that $f(x) = x^p - tx - t \in K[x]$ is separable.)

But why did we have to go to this strange field $\mathbb{F}_p(T)$ to look for irreducible separable polynomials?

Definition 1.4.5. A field K with $\operatorname{char} K = p > 0$ is *perfect* if $\forall b \in K,\ \exists a \in K : a^p = b$, i.e. every element has a p-th root.

Remark 1.4.6. If K is perfect, then $f \in K[x]$ is irreducible $\implies$ f is separable. Indeed, suppose $f \in K[x]$ is inseparable and write $f(x) = g(x^p)$ where $g(x) = b_0 x^n + \cdots + b_n$. Now let $h(x) = a_0 x^n + \cdots + a_n$ where a_i are p-th roots of b_i, i.e. $a_i^p = b$. Then $f(x) = g(x^p) = (h(x))^p$ again by freshman's dream $(a+b)^p = a^p + b^p$, so f is not irreducible, a contradiction.

Note that all finite fields $\mathbb{F}_q$ where $q = p^n$ are perfect, since the map $F : \mathbb{F}_q \to \mathbb{F}_q : a \mapsto a^p$ is a homomorphism by freshman's dream. But any field homomorphism is injective, and any injective map between finite sets is bijective.

Week 5, lecture 2, 1st November

Definition 1.4.7. A field extension $L \supset K$ is *separable* if $\forall a \in L$, the minimal polynomial $f(x) \in K[x]$ of a is separable.

Definition 1.4.8. For a finite field extension $L \supset K$, define its *separable degree* (denoted by $[L : K]_s$) to be $\#\operatorname{Emb}_K(L, M)$ such that $M \supset K$ is normal with $\operatorname{Emb}_K(L, M) \neq \varnothing$.

Remark 1.4.9 (Why did we define this horrible thing?)**.** Suppose $f \in K[x]$ is irreducible and let a be a root of f. Let M be any field extension of K, then one has $\operatorname{Emb}_K(K(a), M) = \{b \in M : f(b) = 0\}$. In otherwords, $[K(a) : K]_s = \#\{\text{roots of } f \text{ in its splitting field}\}$, which would be precisely $\deg f = [K(a) : K]$ is f is separable.

Theorem 1.4.10 (Tower law for separable degrees)**.** For $K \subset L \subset M$, $[M : K]_s = [M : L]_s \cdot [L : K]_s$.

Lemma 1.4.11. $[L : K]_s < [L : K]$ for all $L \supset K$.

Proof. Realise $K \subset L$ as a tower of primitive extensions $K \subset K_1 \subset \cdots \subset K_n = L$ where $K_i = K_{i-1}(a_i)$. But then $[K(a) : K]_s \leq [K(a) : K]$ by the remark above (any polynomial f has at most $\deg f$ roots), so by tower laws one has the desired. □

Theorem 1.4.12 (Main theorem of separable extensions)**.** For a finite field extension $L \supset K$, the following are equivalent:

1. $L \supset K$ is separable.
2. $L = K(a_1, \ldots, a_n)$ with $K \subset K(a_1) \subset \cdots \subset K(a_1, \ldots, a_n)$, and the minimal polynomial $f_i \in K(a_1, \ldots, a_{i-1})[x]$ of a_i over $K(a_1, \ldots, a_{i-1})$ is separable.
3. $[L : K] = [L : K]_s$.
4. For all towers $K \subset K_1 \subsetneqq K_2 \subset L$, one has $[K_2 : K_1]_s \geq 2$.

Proof. $2 \implies 3$: by remark above, f_i is separable $\iff$ $[K(a_1, \ldots, a_i) : K(a_1, \ldots, a_{i-1})] = [K(a_1, \ldots, a_i) : K(a_1, \ldots, a_{i-1})]_s$, and the desired follows from the two tower laws, one for the usual degrees and the other for separable degrees.

Week 5, lecture 3, 1st November

$1 \implies 2$: Since L is finite, write $L = K(a_1, \ldots, a_n)$ and denote $K(a_1, \ldots, a_i)$ by K_i, so that $K_i = K_{i-1}(a_i)$. By assumption, every minimal polynomial $F_i \in L[x]$ of a_i is separable. But then $f_i \in K_{i-1}[x]$ must be separable as well since $f_i \mid F_i$.

$3 \implies 1$: let $a \in L$. We want show its minimal polynomial $f \in K[x]$ is separable.

Consider the tower $K \subset K(a) \subset L$. By tower laws,

$$[L : K] = [L : K(a)][K(a) : K] \quad \text{and} \quad [L : K]_s = [L : K(a)]_s[K(a) : K]_s,$$

but then by 1.4.11,

$$[L : K(a)]_s[K(a) : K]_s \leq [L : K(a)][K(a) : K] = [L : K] = [L : K]_s = [L : K(a)]_s[K(a) : K]_s, ,$$

so it must be that $[K(a) : K] = [K(a) : K]_s$, which gives the desired by 1.4.9.

$3 \implies 4$: by tower laws, write

$$[L : K] = [L : K_2][K_2 : K_1][K_1 : K] \quad \text{and} \quad [L : K]_s = [L : K_2]_s[K_2 : K_1]_s[K_1 : K]_s,$$

and again by a similar argument $[K_2 : K_1]_s = [K_2 : K_1] \geq 2$ since $K_2 \neq K_1$.

$4 \implies 1$: again let $a \in L$ and we want show its minimal polynomial $f \in K[x]$ is separable. Since f is irreducible, the only case that it's inseparable is that $\operatorname{char} K = p$ and $f = g(x^p)$ for some irreducible $g \in K[x]$. Write $b = a^p$, which has minimal polynomial g. Consider $K \subset K(b) \subset K(a) \subset L$. Note that a is a root of $x^p - b = (x - a)^p \in K(b)[x]$, a totally inseparable polynomial, so $[K(a) : K(b)]_s = 1$, but clearly $K(a) \neq K(b)$ (in particular, $[K(a) : K(b)] = p$), a contradiction. □

One can push this further and prove actually $[L : K]_s \mid [L : K]$ and the tower law for *inseparable degree* $[L : K]_i := \frac{[L:K]}{[L:K]_s}$ holds, and $[L : K]_i = p^m$ where $p = \operatorname{char} K$. An extension $L \supset K$ is *purely inseparable* if $[L : K] = [L : K]_i$. If one wants, one can devote their entire life into the study of purely inseparable extensions. Now let's prove the unproved.

Proof of 1.4.10. Let $N \supset M \supset L \supset K$ and suppose $N \supset K$ is normal. By 1.3.10, one has $N \supset M$ and $N \supset L$ are normal, so that $[M : K]_s = \#\operatorname{Emb}_K(M, N)$, $[M : L]_s = \operatorname{Emb}_L(M, N)$ and $[L : K]_s = \operatorname{Emb}_K(L, N)$ are well-defined. Consider the natural restriction map

$$\rho : \operatorname{Emb}_K(M, N) \to \operatorname{Emb}_K(L, N) : (x : M \to N) \mapsto (\rho(x) : L \to N),$$

which is surjective by 1.3.6. Now let $y \in \operatorname{Emb}_K(L, N)$ and consider the size of $\rho^{-1}(y) = \{x \in \operatorname{Emb}_K(M, N) : \rho(x) = y\}$. But that's precisely $\#\operatorname{Emb}_L(M, N)$: the number of embeddings from M to N that fix L. Hence

$$\#\operatorname{Emb}_K(M, N) = \#\operatorname{Emb}_K(L, N) \cdot \#\operatorname{Emb}_L(M, N),$$

which is exactly what's desired. □

Lemma 1.4.13. $\#\operatorname{Aut}_K(L) \leq [L : K]_s$ with equality iff L/K is normal.

Week 6, lecture 1, 5th November

2 Galois theory

2.1 The fundamental theorem

Definition 2.1.1. A finite field extension is *Galois* if it is normal and separable.

Hence, by 1.4.11 and 1.4.13, $L \supset K$ is Galois $\iff |\mathrm{Aut}_K(L)| = [L:K]_s = [L:K]$.

Definition 2.1.2. If $K \subset L$ is a Galois extension, then $\mathrm{Aut}_K(L)$ is denoted by $\mathrm{Gal}(L/K)$ and called the *Galois group* of L/K.

Remark 2.1.3. If $K \subset F \subset L$ are fields and L/K is Galois, then L/F is Galois. This follows from 1.3.10 and 1.4.12. Note that F/K in this case is not necessarily Galois, e.g. $K = \mathbb{Q}, F = \mathbb{Q}(\sqrt[3]{2}), L = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$.

Definition 2.1.4. Let $K \subset L$ be a finite field extension and G a subgroup of $\mathrm{Aut}_K(L)$. Then define $L^G = \{x \in L : g(x) = x \ \forall g \in G\}$, and call it the *fixed field* (or *invariant field*) of G.

Theorem 2.1.5 (Fundamental)**.** Let $K \subset L$ be a Galois extension. There is a bijection, called the *Galois correspondence*, between subgroups of $\mathrm{Gal}(L/K)$ and subfields F with $K \subset F \subset L$ given by $G \mapsto L^G$ and $\mathrm{Aut}_F(L) \hookleftarrow F$. Moreover, under this correspondence, the normal subgroups correspond to normal extensions $F \supset K$. In this case, $\mathrm{Gal}(F/K) = \mathrm{Gal}(L/K)/\mathrm{Gal}(L/F)$.

Proof. Let F be a field with $K \subset F \subset L$. Clearly $\mathrm{Aut}_F(L) \subset \mathrm{Aut}_K(L)$. We show that $L^{\mathrm{Aut}_F(L)} =: F_1 = F$. Clearly $F \subset F_1$. Then $\mathrm{Aut}_{F_1}(L) \subset \mathrm{Aut}_F(L)$. But by definition, every $\sigma \in \mathrm{Aut}_F(L)$ acts on F_1 as the identity, i.e. $\mathrm{Aut}_F(L) \subset \mathrm{Aut}_{F_1}(L)$, so $\mathrm{Aut}_F(L) = \mathrm{Aut}_{F_1}(L)$. Now we know L is Galois over F and F_1, so $[L:F] = |\mathrm{Aut}_F(L)| = |\mathrm{Aut}_{F_1}(L)| = [L:F_1]$, so by the tower law $[F_1:F] = 1$, i.e. $F = F_1$.

Let G be a subgroup of $\mathrm{Aut}_K(L)$. We show that $G = \mathrm{Aut}_{L^G}(L)$. Again clearly $G \subset \mathrm{Aut}_{L^G}(L)$, so in particular $|G| \leq |\mathrm{Aut}_{L^G}(L)|$. But $L \supset L^G$ is Galois, so $[L : L^G] = |\mathrm{Aut}_{L^G}(L)|$. By tower law, it now suffices to show $|G| \geq [L : L^G]$.

Week 6, lecture 2, 8th November

Suppose $|G| = n$ and $G = \{g_1, \ldots, g_n\}$ where g_1 is the identity. It suffices to show that any collection of $n+1$ elements of L, say $b_1, \ldots, b_{n+1}$, is linearly dependent over L^G. Define an injective map $\varphi : L \to L^n$ by $b \mapsto (g_1 b, \ldots, g_n b)$. Note that L^n is a vector space over L of dimension n, so $\varphi(b_1), \ldots, \varphi(b_{n+1})$ must be linearly dependent, hence write

$$a_1\varphi(b_1) + \cdots + a_m\varphi(b_m) = 0 \tag{$*$}$$

where $m \leq n+1$ is the least number such that $L \ni a_1, \ldots, a_m \neq 0$ (after possible rearranging). WLOG $a_1 = 1$ and now write the g-coordinate of above

$$gb_1 + a_2 gb_2 + \cdots + a_m gb_m = 0. \tag{$**$}$$

Now $\forall h \in g$,

$$hgb_1 + ha_2 hgb_2 + \cdots + ha_m hgb_m = 0,$$

so for any $g \in G$,

$$gb_1 + ha_2 gb_2 + \cdots + ha_m gb_m = 0$$

for some $h \in G$. Together with $(**)$, one has

$$(ha_2 - a_2)gb_2 + \cdots + (ha_m - a_m)g(b_m) = 0,$$

but since m is chosen to be minimal, it must be that $h(a_i) = a_i \ \forall i = 2, \ldots, m \ \forall h \in G$, hence $a_i \in L^G \ \forall i = 2, \ldots, m$. But $a_1 = 1 \in L^G$ as well, hence from $(*)$ we have

$$\varphi(a_1 b_1 + \cdots + a_m b_m) = 0 \implies a_1 b_1 + \cdots + a_m b_m = 0,$$

a nontrivial linear relation of b_i's over L^G, which is exactly what's desired.

Week 6, lecture 3, 8th November

Recall 1.3.13, which says in this case if $F \supset K$ is Galois then $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/F) \cong \mathrm{Gal}(F/K)$. It remains to prove that if $G \subset \mathrm{Gal}(L/K)$ is a normal subgroup, then L^G is normal over K, i.e. for any other nontrivial embedding $j : L^G \hookrightarrow L$, one has $\mathrm{im}\, j \subset L^G$. Since L/K is normal, $\exists \sigma \in \mathrm{Gal}(L/K) : j = \sigma i$. Then

$$j(L^G) = \sigma i(L^G) = \sigma(L^G) = L^{\sigma G \sigma^{-1}} = L^G,$$

with the last equality follows from normality of G, so let's the prove the penultimate equality. Indeed, let $\sigma(x) \in \sigma(L^G)$ with $x \in L^G$, then

$$\sigma g \sigma^{-1}(\sigma(x)) = \sigma g(x) = \sigma(x).$$

Now the calculation can be done backwards, so we have equality. □

Remark 2.1.6. If $x \in L$ is fixed by every element of $\mathrm{Gal}(L/K)$, then $x \in K$. Indeed, the Galois correspondence associates to K the whole group $\mathrm{Gal}(L/K)$.

If $\sigma \in \mathrm{Gal}(L/K)$ fixes every element of L, then $\sigma = e$, since the whole field L corresponds to the trivial group $\{e\}$.

2.2 Galois groups of polynomials

Definition 2.2.1. Let K be a field and $f \in K[x]$ a separable polynomial. Let L be a splitting field of f, in particular L is a Galois extension of K by 1.3.9 and 1.4.12. Define the *Galois group* of f as $\mathrm{Gal}(L/K)$. This is well-defined by 1.3.2.

Let f be separable, $n = \deg f$ and $\alpha_1, \dots, \alpha_n$ roots of f in L, its splitting field. Assuming f is monic, one has $f(x) = \prod_{i=1}^n (x - \alpha_i)$. Then for any $\sigma \in \mathrm{Gal}(L/K) = \mathrm{Gal}(f)$, $\sigma(\alpha_i)$ is also a root of f, i.e. $\sigma(\alpha_i) = \alpha_j$ for some j. In particular, we get a group homomorphism $\mathrm{Gal}(f) \to S_n$. Moreover, it's injective, since if $\sigma \in \mathrm{Gal}(f)$ fixes all α_i's, it fixes the whole field $L = K(\alpha_1, \dots, \alpha_n)$, so the kernel is trivial. The philosophy is: for any separable polynomial f with $\deg f = n$, we can define a subgroup of S_n.

Week 7, lecture 1, 12th November: solutions to coursework 1

Week 7, lecture 2, 15th November

Let's formally state what we discussed last time.

Proposition 2.2.2. The action of $\mathrm{Gal}(f)$ on the roots of f in L defines an injective homomorphism $\mathrm{Gal}(f) \hookrightarrow S_n$. The orbits of this action are the roots of irreducible factors of f. In particular, if f is irreducible, then the action is transitive, i.e. there is only one orbit.

Proof. Write $L = k(\alpha_1, \dots, \alpha_n)$ and $f(x) = \prod_{i=1}^n (x - \alpha_i)$. If $g\alpha_i = \alpha_i \forall i$ then g fixes the whole L, so $g = e \in \mathrm{Gal}(L/k) = \mathrm{Gal}(f)$.

Now let g be an irreducible factor of f and write $g(x) = \prod_{i=1}^m (x - \beta_i)$. We want to show that for any $i = 2, \dots, m$, there is a $g \in \mathrm{Gal}(f) : g(\beta_1) = \beta_i$. One has $K = k[x]/(g) \cong k(\beta_1) \cong k(\beta_i)$, so one has an embedding $K \hookrightarrow L$ where the image of x in K is sent to β_1, and another embedding sends it to β_i. Since L/k is normal, these two embeddings differ by an automorphism of L over k, so $\exists g \in \mathrm{Gal}(f) : \beta_i = g(\beta_1)$ as desired. □

We now need to understand subgroups of S_n and which of them are transitive. Naively, it could be all of S_n but we will see restrictions imposed by the coefficients of the polynomial such that the Galois group of the polynomial is a proper subgroup of S_n.

2.3 Low-degree polynomials

Suppose f is separable.

2.3.1 Degree 2

Write $f(t) = t^2 + bt + c = 0$ where $b, c \in k$. If f has a root in k then $\mathrm{Gal}(f) = \{e\}$ is trivial, otherwise it's irreducible and $\mathrm{Gal}(f) \cong C_2$.

2.3.2 Degree 3

1. If f complete splits in k, then again $\mathrm{Gal}(f) = \{e\}$.
2. If f is a product of a linear polynomial and an irreducible quadratic, then by above $\mathrm{Gal}(f) \cong C_2$
3. If f is irreducible, recall that the nontrivial transitive subgroup of S_3 are $C_3 = \{e, (123), (132)\}$ and S_3, so how do we decide which one it is?

Definition 2.3.1. The *discriminant* of $f(x) = \prod_{i=1}^{n}(x - \alpha_i)$ is

$$\Delta_f := \prod_{i<j}(\alpha_i - \alpha_j)^2,$$

clearly f is separable $\iff \Delta_f \neq 0$.

Now consider the Vandermonde matrix and its determinant

$$\det \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-2} & \cdots & \alpha_n^{n-1} \end{pmatrix} = \prod_{i<j}(\alpha_j - \alpha_i),$$

and since the Galois groups permutes the roots, it acts on this matrix by swapping its columns. By linear algebra, this multiplies the determinant by -1, and hence Δ_f is invariant under every element of $\mathrm{Gal}(f)$, so by 2.1.6, $\Delta_f \in k$. Let $\sqrt{\Delta_f} = \pm\prod_{i<j}(\alpha_i - \alpha_j) \in L$ and consider the tower $k \subset k\left(\sqrt{\Delta_f}\right) \subset L$.

Proposition 2.3.2. If $\mathrm{char}\, k \neq 2$ and $f \in k[x]$ is separable, then $\mathrm{Gal}(f) \subset A_n \iff \sqrt{\Delta_f} \in k$.

Proof. For $\sigma \in \mathrm{Gal}(f)$, $\sigma\left(\sqrt{\Delta_f}\right) = \mathrm{sign}(\sigma)\sqrt{\Delta_f}$, so again by 2.1.6,

$$\sqrt{\Delta_f} \in k \iff \mathrm{sign}(\sigma) = 1\ \forall \sigma \in \mathrm{Gal}(f) \iff \mathrm{Gal}(f) \subset A_n.$$

□

For $f(t) = t^2 + bt + c$, $\Delta_f = b^2 - 4c$ as usual. But how do we deal with higher degree polynomials in general? Recall that $\Delta_f = 0 \iff f$ is not separable $\iff \gcd(f, f') \neq 1$ by 1.4.2.

Definition 2.3.3. Let $f(x) = a\prod_{i=1}^{n}(x - \alpha_i)$ and $g(x) = b\prod_{i=1}^{m}(x - \beta_i)$ with $a, b \neq 0, \alpha_i, \beta_j \in L$ where L is a splitting field of fg. The *resultant* of f and g is

$$\mathrm{Res}(f, g) = a^m b^n \prod_{i,j}(\alpha_i - \beta_j).$$

Proposition 2.3.4. 1.

$$\mathrm{Res}(f, g) = (-1)^{mn}\,\mathrm{Res}(g, f) = a^m \prod_{i=1}^{n} g(\alpha_i),$$

2. $\mathrm{Res}(f, g) = 0 \iff \gcd(f, g) \neq 1$, i.e. they have a common root in L.
3. If at least one of f and g is separable, then $\mathrm{Res}(f, g) \in k$.

Week 7, lecture 3, 15th November

Proof. 1. This follows immediately from the definition.

2. $\mathrm{Res}(f, g) = 0 \iff \alpha_i = \beta_j$ for some $i, j \iff f, g$ have a common root α_i.
3. Write $K = k(\alpha_1, \alpha_n) \subset L$, a splitting field of f. Suppose f is separable, then K/k is Galois, and elements of $\mathrm{Gal}(f)$ permute $\alpha_1, \ldots \alpha_n$, hence they permute $g(\alpha_1), \ldots, g(\alpha_n)$, so $\prod_{i=1}^{n} g(\alpha_i)$ is fixed by $\mathrm{Gal}(f)$, so by 2.1.6 $\prod_{i=1}^{n} g(\alpha_i) \in k$.

□

Proposition 2.3.5. Let $f \in k[x]$ be monic. Then

$$\Delta_f = (-1)^{\frac{n(n-1)}{2}} \operatorname{Res}(f, f') = (-1)^{\frac{n(n-1)}{2}} \operatorname{Res}(f', f).$$

Proof. By product rule,

$$f'(x) = \sum_{i=1}^{n} \prod_{j \neq i} (x - \alpha_j) = (x - \alpha_2)(x - \alpha_3) \cdots (x - \alpha_n) + (x - \alpha_1)(x - \alpha_3) \cdots (x - \alpha_n) + \cdots,$$

so

$$\operatorname{Res}(f, f') = \prod_{i=1}^{n} f'(\alpha_i) = \prod_{i=1}^{n} \prod_{j \neq i} (\alpha_i - \alpha_j) = (-1)^{\frac{n(n-1)}{2}} \prod_{i<j} (\alpha_i - \alpha_j)^2 = (-1)^{\frac{n(n-1)}{2}} \Delta_f.$$

□

Remark 2.3.6. Note that if we write $g = hf + r$, then $g(\alpha_i) = r(\alpha_i)$, so $\operatorname{Res}(f, g) = a^{m-m_1} \operatorname{Res}(f, r)$ where $m_1 = \deg r$, so the way one calculates $\operatorname{Res}(f, g)$ is similar to Euclidean algorithm.

Exercise 2.3.7. Show that for $f(x) = x^n + ax + b,\ a, b \in k$,

$$\Delta_f = (-1)^{\frac{n(n-1)}{2}} \left((-1)^{n-1} (n-1)^{n-1} a^n + n^n b^{n-1} \right).$$

In particular, if $n = 3$ and $f(x) = x^3 + px + q$, one has $\Delta_f = -4p^3 - 27q^2$. (This is the general (Weierstrass) form of cubic polynomials when $\operatorname{char} k \neq 3$.)

We can now finally finish part 3 of determining of Galois group of a cubic:

3. (a) If Δ_f is a square in k, then $\operatorname{Gal}(f) \cong C_3$,
   (b) otherwise $\operatorname{Gal}(f) \cong S_3$.

2.3.3 Degree 4

We first need some group theory since S_4 is a next layer of complexity than S_3. Up to conjugation, elements of S_n are given by their cycle types, and in particular in S_4 one has the conjugacy classes e, transpositions, 3-cycles, 4-cycles and double transpositions. The transitive subgroups of S_4 are

1. C_4 (generated by a 4-cycle), note that $C_4 \not\subset A_4$ and it's not normal,
2. the Klein 4-group V_4 (can be written as $\{e, (12)(34), (13)(24), (14)(23)\}$), note that $V_4 \subset A_4$, it's normal and $S_4/V_4 \cong S_3$ since S_4 acts transitively on $V_4 \backslash \{e\}$ by conjugation,
3. dihedral group D_8 generated by (1234) and (13). Again $D_8 \not\subset A_4$ and not normal,
4. A_4 which is clearly normal, and
5. S_4.

Since we have 5 and not 2 transitive subgroups, Δ_f is not enough to determine $\operatorname{Gal}(f)$, but at least we know

1. Δ_f is a square in $k \iff \operatorname{Gal}(f) \cong V_4$ or A_4,
2. Δ_f is not a square in $k \iff \operatorname{Gal}(f) \cong C_4,\ D_8$ or S_4.

Definition 2.3.8. Let $f \in k[x]$ be separable and monic of degree 4 with a splitting field L. Write $f(x) = \prod_{i=1}^{4} (x - \alpha_i)$. Define $a = \alpha_1\alpha_2 + \alpha_3\alpha_4,\ b = \alpha_1\alpha_3 + \alpha_2\alpha_4,\ c = \alpha_1\alpha_4 + \alpha_2\alpha_3$. The polynomial $g(x) = (x-a)(x-b)(x-c)$ is called the *resolvent cubic* of f.

Proposition 2.3.9. The resolvent cubic g is separable and $\Delta_f = \Delta_g$. If $\operatorname{char} k \neq 2$, the fields

$$k \subset k\left(\sqrt{\Delta_f}\right) \subset k(a, b, c) = K \subset L$$

are the fixed subfields of the normal subgroups

$$\operatorname{Gal}(f) \supset \operatorname{Gal}(f) \cap A_4 \supset \operatorname{Gal}(f) \cap V_4 \supset \{e\}$$

respectively. Moreover, $g \in k[x]$.

Proof. By direct calculation,

$$a-b=(\alpha_1-\alpha_4)(\alpha_2-\alpha_3),\quad b-c=(\alpha_1-\alpha_2)(\alpha_3-\alpha_4),\quad a-c=(\alpha_1-\alpha_3)(\alpha_2-\alpha_4),$$

so $\Delta_f=\Delta_g$, and in particular, it follows from f is separable that g is separable. Again for any $\sigma\in\mathrm{Gal}(f)\leq S_4$, $\sigma\left(\sqrt{\Delta_f}\right)=\mathrm{sign}(\sigma)\cdot\sqrt{\Delta_f}$, so $\sqrt{\Delta_f}$ is fixed by every $\sigma\in\mathrm{Gal}(f)\cap A_4$, hence $k\left(\sqrt{\Delta_f}\right)=L^{\mathrm{Gal}(f)\cap A_4}$. Equivalently, $\mathrm{Gal}(f)\cap A_4=\mathrm{Gal}\left(L/k\left(\sqrt{\Delta_f}\right)\right)$.

Now if $\sigma\in\mathrm{Gal}(f)\cap V_4$, then σ fixes each of a,b,c. To see this, let's look at a: (12)(34) clearly preserves each monomial $\alpha_1\alpha_2$ and $\alpha_3\alpha_4$, and the other two double transposition exchanges the two. Hence σ fixes every element of $K=k(a,b,c)$.

It remains to prove conversely that if σ fixes a,b,c, then $\sigma\in V_4$. Now S_4 permutes $\alpha_1,\alpha_2,\alpha_3,\alpha_4$, hence it naturally and transitively permutes a,b,c. We claim the stabiliser of $b=\alpha_1\alpha_3+\alpha_2\alpha_4$ is the subgroup of S_4 generated by (1234) and (13). One exchanges two monomials and the other preserves, so their products also fix b. This group is isomorphic to D_8, and it cannot be any bigger since the stabiliser must be of order 8 by the orbit–stabiliser theorem and that the action is transitive (so the orbit of b is the whole $\{a,b,c\}$).

Now a permutation $\sigma\in S_4$ fixes each of $a,b,c\iff\sigma\in\bigcap$ stabilisers of $a,b,c\iff\sigma\in\bigcap_{g\in S_4}gD_8g^{-1}$ (since again the action is transitive). But this intersection is exactly V_4, since it has to be a normal subgroup of S_4, so it can only be A_4 or V_4, but $|A_4|>|D_8|$ so it can only be V_4.

Finally, $\mathrm{Gal}(f)$ permutes a,b,c, hence acts trivially on the coefficients of g. By 2.1.6, $g\in k[x]$. □

Proposition 2.3.10. Assume $\mathrm{char}\,k\neq 2$, then a a general quartic can be reduced to $f(x)=x^4+px^2+qx+r,\quad p,q,r\in k$. The resolvent cubic of f is then $g(t)=t^3-pt^2-4rt+(4rp-q^2)$.

Algorithm for determining $\mathrm{Gal}(f)$ **where** f **is an irreducible quartic.**

- If $\Delta_f=\Delta_g$ is a square in k, then $\mathrm{Gal}(f)\subset A_4$.
  - $\mathrm{Gal}(f)=A_4$ if g has no roots in k, and
  - $\mathrm{Gal}(f)=V_4$ if g has a root in k.

  Indeed, $\mathrm{Gal}(g)=\mathrm{Gal}(f)/\left(\mathrm{Gal}(f)\cap V_4\right)$, so if g has no roots in k then $\mathrm{Gal}(g)$ is not trivial, and if it has a root then it is trivial.
- If $\Delta_f=\Delta_g$ is not a square in k, then $\mathrm{Gal}(f)\not\subset A_4$.
  - If g has a root in k, then $\mathrm{Gal}(f)=D_8$ if f remains irreducible over K
  - If g has a root in k, then $\mathrm{Gal}(f)=C_4$ if f is a product of two quadratics over K
  - $\mathrm{Gal}(f)=S_4$ if g has no roots in K

Remark 2.3.11. How did the resultant cubic appear historically? Again consider $f(x)=x^4+px^2+qx+r$ and write it as

$$\left(x-\frac{1}{2}t\right)^2-\left((t-p)x^2-qx+\left(\frac{1}{4}t^2-r\right)\right)$$

one can check that the t's cancel out. Let t be a new variable. It would be great that the above is a difference of two squares, i.e. the second quadratic has discriminant 0. The condition is then $q^2-4(t-p)\left(\frac{1}{4}t^2-r\right)=0$, which is the resolvent cubic! Now take $t=t_0$, a root of the resolvent, then $f(x)=\left(x-\frac{1}{2}t_0\right)^2-(t_0-p)(\cdots)^2$, which one can then use to solve the quartic.

2.4 Biquadratic equations

Assume $\mathrm{char}\,k\neq 2$. The main question: what is a quadratic extension (i.e. extension of degree 2) of a quadratic extension? Let's first review some easy facts about quadratic extensions:

Lemma 2.4.1. Let K be a field and $a,b\in K^\times$.

1. If a is not a square in K, then the kernel of the natural homomorphism $K^\times/K^{\times 2} \to K\left(\sqrt{a}\right)^\times/K\left(\sqrt{a}\right)^{\times 2}$ (where $K^{\times 2}$ is the subgroup of $K^\times$ that contains squares in $K^\times$) consists of the classes of 1 and a.
2. $K\left(\sqrt{b}\right) = K\left(\sqrt{a}\right) \iff$ the class of ab in $K^\times/K^{\times 2}$ is trivial.
3. $K\left(\sqrt{b}, \sqrt{a}\right) = K\left(\sqrt{a}\right) \iff b$ or ab is a square in K.
   If $K\left(\sqrt{a}, \sqrt{b}\right) \neq K\left(\sqrt{a}\right) \neq K$, then $\mathrm{Gal}\left(K\left(\sqrt{a}, \sqrt{b}\right)/K\right) \cong C_2 \times C_2$.
4. Suppose b is not a square in K. If $K\left(\sqrt{x+y\sqrt{b}}\right) = K\left(\sqrt{b}\right)$ for some $x, y \in K$, then $x^2 - by^2$ (norm of $x + y\sqrt{b}$) is a square in K.

Proof. 1. Squares of $K\left(\sqrt{a}\right)^\times$ are of the form

$$\left(z + w\sqrt{a}\right)^2 = z^2 + aw^2 + 2zw\sqrt{a},$$

for this to be in K, $2zw = 0$ so either $z = 0$ or $w = 0$. If $z = 0$ then out element is aw^2, so its image in the quotient group $K^\times/K^{\times 2}$ is a as desired. If $w = 0$ then our element is $z^2 \in K^{\times 2}$.

2. The case that a or b is a square in K is trivial, so suppose not. If $K\left(\sqrt{b}\right) = K\left(\sqrt{a}\right)$, then by 1, the kernels of $K^\times/K^{\times 2} \to K\left(\sqrt{a}\right)^\times/K\left(\sqrt{a}\right)^{\times 2}$ and $K^\times/K^{\times 2} \to K\left(\sqrt{b}\right)^\times/K\left(\sqrt{b}\right)^{\times 2}$ both consist of the classes 1 and a, so b has to be of the class a and hence $ab = a^2$ is trivial.

   If the class of ab is trivial in $K^\times/K^{\times 2}$ then so is the class of $\frac{a}{b} = ab\frac{1}{b^2}$, so the class of a is the same as the class of b, i.e. $a^2 = b^2$, so $K\left(\sqrt{b}\right) = K\left(\sqrt{a}\right)$.

3. If $K\left(\sqrt{a}, \sqrt{b}\right) = K\left(\sqrt{a}\right)$ then b is a square in $K(\alpha)$, so by 1, either b is a square in K or $b = aw^2$ for some $w \in K$, so $ab = a^2w^2 \in K^{\times 2}$.

   If b is a square in K then of course $K\left(\sqrt{a}, \sqrt{b}\right) = K\left(\sqrt{a}\right)$. If ab is a square in K, write $ab = c^2$, but in $K\left(\sqrt{a}\right)$ one has $a = \left(\sqrt{a}\right)^2$, hence $b = \left(\frac{c}{\sqrt{a}}\right)^2 \in K\left(\sqrt{a}\right)^{\times 2}$.

   By above, we have the inequality $K\left(\sqrt{a}, \sqrt{b}\right) \neq K\left(\sqrt{a}\right) \neq K$ precisely when neither a, b nor ab is a square in K, so $\mathrm{Gal}\left(K\left(\sqrt{a}, \sqrt{b}\right)/K\right) \cong C_2 \times C_2$ has two generators: the first one changes the sign of $\sqrt{a}$, the second one $\sqrt{b}$.

4. One has $K\left(\sqrt{x+y\sqrt{b}}\right) = K\left(\sqrt{b}\right)$ precisely when $x + y\sqrt{b}$ is a square in $K\left(\sqrt{n}\right)$, i.e. $x + y\sqrt{b} = \left(z + w\sqrt{b}\right)^2$, so $x - y\sqrt{b} = \left(z - w\sqrt{b}\right)^2$ and hence $x^2 - by^2 = \left(x + y\sqrt{b}\right)\left(x - y\sqrt{b}\right) = \left(z^2 - bw^2\right)^2 \in K^{\times 2}$.

□

Let K be a field and $a, b \in K^\times$. Suppose b is not a square in K. Consider $L = K\left(\sqrt{a+\sqrt{b}}, \sqrt{a-\sqrt{b}}\right)$. This is a splitting field of

$$\begin{aligned} f(x) &= \left(x - \sqrt{a+\sqrt{b}}\right)\left(x + \sqrt{a+\sqrt{b}}\right)\left(x - \sqrt{a-\sqrt{b}}\right)\left(x + \sqrt{a-\sqrt{b}}\right) \\ &= x^4 - 2ax^2 + (a^2 - b) = (x^2 - a)^2 - b. \end{aligned}$$

Write $c = a^2 - b$. This is not zero since b is not a square. Observe that

- f is separable: $f'(x) = 4x^3 - 4ax = 4x\left(x - \sqrt{a}\right)\left(x + \sqrt{a}\right)$ which has roots $0, \pm\sqrt{a}$, which are not roots of f.
- f has no roots in K since $\sqrt{b} \notin K$.
- If furthermore c is not a square, then f is irreducible. Indeed, if f is reducible, then since it doesn't have a root in K, it must be a product of two irreducible quadratics, so either $a \pm \sqrt{b} \in K$, which contradicts that b is not a square, or $\sqrt{a^2 - b} = \sqrt{c} \in K$, i.e. c is a square in K.
- Observe that

$$\left(\sqrt{a+\sqrt{b}} + \sqrt{a-\sqrt{b}}\right)^2 = 2a + 2\sqrt{c},$$

so $K\left(\sqrt{c}\right) \subset L$. Also, $\sqrt{2\left(a \pm \sqrt{c}\right)} \subset L$, so $K\left(\sqrt{2\left(a+\sqrt{c}\right)}, \sqrt{2\left(a-\sqrt{c}\right)}\right) \subset L$. In fact, we claim it's the whole of L, since

$$\left(\sqrt{2(a+\sqrt{c})}, \sqrt{2\left(a-\sqrt{c}\right)}\right)^2 = 4a + 4\sqrt{a^2-c} = 4(a+\sqrt{b}),$$

implying $K\left(\sqrt{2\left(a+\sqrt{c}\right)}, \sqrt{2\left(a-\sqrt{c}\right)}\right)$ contains $\sqrt{a \pm \sqrt{b}}$. Thus L is also a splitting field of the *companion polynomial*

$$\begin{aligned} g(x) &= \left(x - \sqrt{2\left(a+\sqrt{c}\right)}\right)\left(x + \sqrt{2\left(a+\sqrt{c}\right)}\right)\left(x - \sqrt{2\left(a-\sqrt{c}\right)}\right)\left(x + \sqrt{2\left(a-\sqrt{c}\right)}\right) \\ &= x^4 - 4ax^2 + 4b, \end{aligned}$$

so one can think of b and c as having a sort of symmetry.

Week 8, lecture 3, 22nd November

The task now is to compute $\mathrm{Gal}(L/K) = \mathrm{Gal}(f)$. Note that there are lots of symmetries in f so its Galois group clearly can't be the whole of S_4.

Proposition 2.4.2. $\mathrm{Gal}(f)$ is a subgroup of D_8.

Proof. Consider the square

$$\begin{array}{ccc} \sqrt{a-\sqrt{b}} & \text{———} & \sqrt{a+\sqrt{b}} \\ \Big| & & \Big| \\ -\sqrt{a+\sqrt{b}} & \text{———} & -\sqrt{a-\sqrt{b}} \end{array}$$

(this means nothing we are just ordering the roots in a certain way), and note that opposite vertices are negatives, so if one goes to another then the other vertices are preserved: it's a reflection. If a vertex goes to the one next to it, which is of the same sign, then $\sqrt{b} \mapsto -\sqrt{b}$, so every vertex goes to the one next to it: it's a rotation. We conclude that $\mathrm{Gal}(f)$ fixes the square, and so does D_8. □

Theorem 2.4.3. Let K be a field of $\mathrm{char}\, K \neq 2$ and $a, b \in K^\times : b$ is not a square in K. As before, write $c = a^2 - b$ and $f(x) = x^4 - 2ax^2 + c$. Then

1. If bc and c are not squares in K, then $\mathrm{Gal}(f) \cong D_8$.
2. If bc is a square (hence c is not a square), then $\mathrm{Gal}(f) \cong C_4$.
3. If c is a square and
   (a) neither $2\left(a+\sqrt{c}\right)$ nor $2\left(a-\sqrt{c}\right)$ is a square, then $\mathrm{Gal}(f) \cong V_4 \cong C_2 \times C_2$.
   (b) one of $2\left(a \pm \sqrt{c}\right)$ is a square, then $\mathrm{Gal}(f) \cong C_2$.

Proof. The resolvent cubic of f is $t^3+2at^2-4ct-8ac = (t+2a)(t^2-4c)$ with discriminant c up to a multiplication by a square in K and splitting field $K\left(\sqrt{c}\right)$.

Assume that c is a square in K, then recall $L = K\left(\sqrt{2\left(a+\sqrt{c}\right)}, \sqrt{2\left(a-\sqrt{c}\right)}\right)$. Note that $2\left(a+\sqrt{c}\right)2\left(a-\sqrt{c}\right) = 4(a^2-c) = 4b$ is not a square, so either one of $\sqrt{2\left(a+\sqrt{c}\right)}$ and $\sqrt{2\left(a-\sqrt{c}\right)}$ is not square or both of them aren't. The desired now follows from 2.4.1.

Now for the first case, consider the tower $K \subset K\left(\sqrt{b}\right) \subset K\left(\sqrt{a+\sqrt{b}}\right) \subset L$. Clearly $\left[K\left(\sqrt{b}\right) : K\right] = 2$, and $\left[K\left(\sqrt{a+\sqrt{b}}\right) : K\right] = 2$ as well since if $a+\sqrt{b}$ is a square in $K\left(\sqrt{b}\right)$, but then by the last part of 2.4.1, $c = a^2 - b$ is a square, a contradiction. Hence by tower law, $\left[K\left(\sqrt{a+\sqrt{b}}\right) : K\right] = 2 \times 2 = 4$. Now again by 2.4.1, $K\left(\sqrt{a+\sqrt{b}}\right) = K\left(\sqrt{a-\sqrt{b}}\right) \iff \left(a+\sqrt{b}\right)\left(a-\sqrt{b}\right) = a^2 - b = c$ is a square, hence $[L : K] \geq 8$, and by 2.4.2 it must be $\mathrm{Gal}(f)$ is the whole of D_8.

Finally, if $bc \in K^{\times 2}$, then $c \notin K^{\times 2}$ as observed and $K\left(\sqrt{b}\right) = K\left(\sqrt{c}\right)$. Now $f(x) = \left(x^2 - \left(a+\sqrt{b}\right)\right)\left(x^2 - \left(a-\sqrt{b}\right)\right)$ is a product of two quadratics over $K\left(\sqrt{c}\right)$, both are irreducible since $a \pm \sqrt{b}$ is not a square (if it is then c is a square). By the algorithm for quartics, in this case $\mathrm{Gal}(f) \cong C_4$. □

Remark 2.4.4. f is irreducible in cases 1, 2 and 3a, but not in 3b.

Example 2.4.5. $f(x) = x^4 - 2$ over $\mathbb{Q}$. In the notation above, $a = 0, b = 2$ and $c = -2$, so bc and c are not squares in $\mathbb{Q}$, hence $\mathrm{Gal}(f) \cong D_8$.

Example 2.4.6. $f(x) = x^4 - 4x^2 + 2$ over $\mathbb{Q}$, then $a = b = c = 2$, so $bc = 4$ is a square, hence $\mathrm{Gal}(f) \cong C_4$. Curiously enough, the splitting field of f is $L = \mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right)$ and we don't need to write the extra $\sqrt{2-\sqrt{2}}$, since

$$\left(\sqrt{2+\sqrt{2}}\right)\left(\sqrt{2-\sqrt{2}}\right) = \sqrt{4-2} = \sqrt{2} \in \mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right).$$

Week 9, lecture 1, 26th November

3 Frobenius lifting

The aim is to know how to calculate the Galois group of a polynomial with integer coefficients.

3.1 Finite fields

Let K be a finite field. Recall that there is exactly one homomorphism $\varphi : \mathbb{Z} \to K$ since one must have $\varphi(1) = 1$ and the rest is determined. Now since $|K| < \infty$, one must have $\ker\varphi \neq 0$. Since K is a field, $\ker\varphi$ is a maximal ideal of $\mathbb{Z}$ so it's of the form $p\mathbb{Z}$ where p is a prime. In this case we say $\mathrm{char}\, K = p$, and note that $\mathrm{im}\,\varphi = \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$, so K is a finite-dimensional vector space over $\mathbb{F}_p$, hence $|K| = p^d$ for some $d \geq 1$.

Proposition 3.1.1. There is a unique finite field with p^d elements for every prime p and every $d \geq 1$.

Proof. All fields of size p^d are isomorphic. Indeed, $K^\times$ is a group of order $p^d - 1$. By Lagrange, each $x \in K$ is a root of $x^{p^d} - x = x(x^{p^d-1} - 1)$. But by the fundamental theorem of algebra, this has at most p^d roots, which must be precisely the whole K without multiplicities. Equivalently, K is a splitting field of $x^{p^d} - x$, so the desired follows from 1.3.2.

Conversely, a field with p^d elements does exist: consider the set of roots M in the splitting field L of $x^{p^d} - x \in \mathbb{F}_p[x]$. Then $\mathrm{char}\, L = \mathrm{char}\,\mathbb{F}_p = p$, so one has M is a field; in particular if $\alpha, \beta \in M$ then $(\alpha\beta)^{p^d} = \alpha^{p^d}\beta^{p^d} = \alpha\beta$, $(\alpha+\beta)^{p^d} = \alpha^{p^d} + \beta^{p^d} = \alpha + \beta$ (by binomial theorem and that coefficients between are divisible by p). If $p = 2$ then $(-\alpha)^{p^d} = \alpha^{p^d} = \alpha = -\alpha$, and if p is odd then $(-\alpha)^{p^d} = -\alpha^{p^d} = -\alpha$. The multiplicative inverses are clear. Then $L = M$ since we already have all the roots by construction. □

Definition 3.1.2. Let $q = p^d$ with $d \geq 1$. Define $\mathbb{F}_q$ as the field of size $q = p^d$ (which we can by above).

Definition 3.1.3. Let K be a field with $\mathrm{char}\, K = p$. Then the *Frobenius map* $\mathrm{Frob}_p : K \to K$ is given by $x \mapsto x^p$. More generally, $\mathrm{Frob}_{p^d} : x \mapsto x^{p^d} = (\mathrm{Frob}_p)^d$.

By the proof of the proposition above, Frob is a field homomorphism.

Remark 3.1.4. Like any other field homomorphism, Frob is injective, but it's not always surjective. Take $K = \mathbb{F}_p(x) = \left\{\frac{f(x)}{g(x)} : f, g \in \mathbb{F}_p[x], g \neq 0\right\}$. Then

$$(a_n x_n + \cdots + a_0)^p = a_n^p (x^p)^n + \cdots + a_1^p x^p + a_0^p = a_n (x^p)^n + \cdots + a_1 x^p + a_0$$

by Fermat's little theorem, so one never gets powers of x lower than p, i.e. $\mathrm{im}\,\mathrm{Frob}_p = \mathbb{F}_p(x^p) \neq \mathbb{F}_p(x)$.

Proposition 3.1.5. Let K be a finite field with $q = p^d$ elements. Then Frob_p is surjective (i.e. Frob_p is an automorphism of K) and the order of Frob_p (the least time that Frob_p composes with itself to get to the identity) is $d = [K : \mathbb{F}_p]$.

Proof. Clearly if a map from a finite set to itself is injective then it's surjective.

Now since $|K| = p^d$, again every element of K is a root of $x^{p^d} - x$, hence $(\mathrm{Frob}_p)^d = \mathrm{id}$. It remains to show that $(\mathrm{Frob}_p)^m = \mathrm{id}$ for $m < d$ cannot happen. Indeed, if so, then every element of K is a root of $x^{p^m} - x$, which has at most $p^m < p^d = |K|$ roots, an absurdity. □

Proposition 3.1.6. Let $K \subset L$ be an extension of finite fields of degree d. Then L is Galois over K with Galois group $\mathrm{Gal}(L/K) \cong C_d$ generated by Frob_q where $q = |K|$. Moreover, $K = L^{\mathrm{Frob}_q}$ is the unique subfield of L of size q.

Proof. The reason we are interested in Frob_q is that Frob_p only fixes $\mathbb{F}_p$ but could act nontrivially on K, but Frob_q does fix K (i.e. $\mathrm{Frob}_q \in \mathrm{Aut}_K(L)$) if we take $q = |K|$ by proposition above. Now $\mathrm{Frob}_p : L \to L$ has order $[L : \mathbb{F}_p] = [L : K][K : \mathbb{F}_p] = d[K : \mathbb{F}_p]$, so $\mathrm{Frob}_q = (\mathrm{Frob}_p)^d$ has order d and so generates C_d. Now $C_d \subset \mathrm{Aut}_K(L)$, but $|\mathrm{Aut}_K(L)| \leq [L : K] = d$, so $\mathrm{Aut}_K(L) \cong C_d$, and in particular L/K is Galois by the remark after 2.1.1. By Galois correspondence, $K = L^{\mathrm{Gal}(L/K)} = L^{\mathrm{Frob}_q}$.

If $K' \subset L$ is another field of size q, then every element of K' is fixed by Frob_q, so $K' \subset L^{\mathrm{Frob}_q} = K$, so $K' = K$ since $|K'| = |K|$. □

Corollary 3.1.7. Let K be a field with q elements, $f \in K[x]$ be irreducible, and L/K be a finite extension such that f completely splits in L. Then Frob_q acts on roots of f in L as an n-cycle where $n = \deg f$.

Proof. $\mathrm{Gal}(L/K)$ is generated by Frob_q, but f is irreducible, hence Frob_q acts on the roots transitively by 2.2.2. □

Week 9, lecture 2, 29th November

Consider a separable $f(x) = f_1(x) \cdots f_m(x) \in \mathbb{F}_p[x]$ with $\deg f_i = n_i$. Then Frob_p is a permutation of cycle shape $(n_1)(n_2) \cdots (n_m)$.

Theorem 3.1.8. Let $f \in \mathbb{Z}[x]$ be separable of degree n, p be a prime and $f_p \in \mathbb{F}_p[x]$ the reduction of f mod p. Suppose $\deg f_p = n$ and f_p is separable. Let $K \supset \mathbb{Q}$ be a splitting field of f and $F \supset \mathbb{F}_p$ a splitting field of f_p. Let Z be the set of roots of f in K and Z_p the set of roots of f_p in F. Then there is a bijection $\psi : Z \to Z_p$ such that under this identification, $\mathrm{Gal}(f_p)$ is a subgroup of $\mathrm{Gal}(f)$. More formally, there is a cyclic subgroup $C \subset \mathrm{Gal}(f)$ and an isomorphism of groups $\iota : C \to \mathrm{Gal}(f_p)$ such that each $g \in C$ satisfies $\iota(g)\psi = \psi g$.

Corollary 3.1.9. Let f be separable of degree n. If f_p is separable of degree n and is a product of irreducible factors of degree $n_1, \ldots, n_m$ with $n_1 + \cdots + n_m = n$, then the image of $\mathrm{Gal}(f)$ in S_n contains a permutation of cycle shape $(n_1) \cdots (n_m)$.

Remark 3.1.10. Only finitely many primes don't satisfy our assumptions; write $f(x) = a_n x^n + \cdots + a_0$, then $\deg f_p = n$ as long as $p \nmid a_n$, and f_p is separable as long as $\Delta_{f_p} \neq 0$ (i.e. $p \nmid \Delta_f$).

We now require some easy group theory lemmas about the structure of S_n.

Recall that every permutation is a product of disjoint cycles, and a cycle is a product of transpositions. This implies transpositions generate S_n. In fact, $(12), (23), \ldots, (n-1, n)$ already do (since for example $(13) = (23)(12)(23)$).

Also, (12) and $\sigma = (12 \cdots n)$ generate S_n, since $(i, i+1) = \sigma^{i-1}(12)\sigma^{1-i}$. Note that (13) and (1234) generate $D_4 \subsetneq S_4$.

But if n is prime, then any transposition and a n-cycle does generate S_n: indeed, after relabelling we have the transposition (12) and a n-cycle σ, but some power σ^i sends 1 to 2, and it's still a n-cycle by Lagrange (C_n doesn't have any other nontrivial subgroup), so we have (12) and $(12 \cdots)$ which generate S_n.

Week 9, lecture 3, 29th November

Example 3.1.11. What's $\mathrm{Gal}(f)$ for $f(x) = x^5 - x - 1 \in \mathbb{Q}[x]$?

Modulo 2 the polynomial $f_2 \in \mathbb{F}_2[x]$ looks the same, and it has no roots in $\mathbb{F}_2$. Now if $f_2'(x_0) = x_0^4 - 1 = 0$, then $f_2(x_0) = x_0 - x_0 - 1 = -1 \neq 0$, so f_2 is separable over $\mathbb{F}_2$.

To see if f_2 is irreducible or not, one needs to check if it has a factor of degree 2. A complete list of degree 2 polynomials in $\mathbb{F}_2[x]$ is $x^2, x^2+1, x^2+x, x^2+x+1$, and one does have $x^5 + x + 1 = (x^2 + x + 1)(x^3 + x^2 + 1)$. This tells us $\mathrm{Gal}(f)$ contains a permutation σ of 2, 3-cycle type, and σ^3 is a transposition.

Modulo 3 the polynomial still looks the same and has no roots. But f_3 is irreducible: a complete list of irreducible degree 2 polynomials in $\mathbb{F}_3[x]$ is x^2+1, x^2+x+2, x^2+2x+2, and f_3 is not divisible by any of these. Hence $\mathrm{Gal}(f)$ contains a 5-cycle, so $\mathrm{Gal}(f) = S_5$.

Proposition 3.1.12. Let $f \in \mathbb{Q}[x]$ be irreducible of prime degree p. If f has exactly $p-2$ real roots (i.e. has exactly one complex conjugate pair as roots) then $\mathrm{Gal}(f) = S_p$.

Proof. Let L be a splitting field of f and $\alpha \in L$ a root of f. Since f is irreducible, $\mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(f)$ with $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg f = p$, so by tower law, $p \mid [L : \mathbb{Q}] = |\mathrm{Aut}_{\mathbb{Q}}(L)| = |\mathrm{Gal}(f)|$, so by Cauchy, $\mathrm{Gal}(f)$ contains an element of order p, i.e. a p-cycle. The complex conjugation (which interchanges the two complex roots and fixes every other root) is a transposition in $\mathrm{Gal}(f)$. Hence $\mathrm{Gal}(f) \cong S_p$. □

Lemma 3.1.13. If $G \subset S_n$ is a transitive subgroup containing a transposition and an $n-1$-cycle, then $G = S_n$.

Proof. After relabelling, suppose the transposition is $\tau = (12)$. If σ is the $n-1$-cycle that doesn't contain 1, then after relabelling write $\sigma = (23\cdots n)$, so $\tau\sigma = (12\cdots n)$ and we are done. If σ contains 1 and 2, again after relabelling $\sigma = (23\cdots n)$ and $\tau = (2m)$ with $m \neq 1$. Since G is transitive, $\exists g \in G : g(2) = 1$, so $g\tau g^{-1} = (1m')$, then this element together with σ we are again in the first case. □

Example 3.1.14. $f(x) = x^6 - 12x^4 + 15x^3 - 6x^2 + 16x + 12$ is Eisenstein at $p = 3$, so f is irreducible.

Modulo 2, $f_2(x) = x^6 + x^3 + x = x(x^5 + x^2 + 1)$ where $x^5 + x^2 + 1$ is irreducible, so $\mathrm{Gal}(f)$ contains a 5-cycle.

Modulo 5, $f_5(x) = x^6 - 2x^4 - x^2 + 2 = (x^2-1)(x^2+1)(x^2-2) = (x-1)(x+1)(x-2)(x+2)(x^2-2)$, so $\mathrm{Gal}(f)$ contains a transposition, so by lemma above $\mathrm{Gal}(f) \cong S_6$.

Week 10, lecture 1, 3rd December

3.2 Dedekind's theorem

Definition 3.2.1. A *semigroup* S is a set with a associative binary operation. A *homomorphism* of semigroups $S_1 \to S_2$ is a map preserving this binary operation. If S has a unit element 1 satisfying $1 \cdot x = x \cdot 1 = x \ \forall x \in S$, then it's a *monoid*. A homomorphism of monoids is a homomorphism of semigroups sending 1 to 1.

Example 3.2.2. Every group is a monoid.

Every ring is a monoid under multiplication.

$\{n \in \mathbb{Z} : n \geq 0\}$ is a monoid under addition.

$\{n \in \mathbb{Z} : n > 0\}$ is a monoid under multiplication.

Every field is a monoid under multiplication.

Definition 3.2.3. Let S be a semigroup and K a field. Then semigroup homomorphisms $S \to K$ are called *characters* of S with values in K.

Example 3.2.4. If S is a group, then a character is known as a 1-dimensional representation of S over K.

A field homomorphism $K \to K$ is a character.

The zero function $S \to K$ that sends everything to 0 is always a character. Same for the one sending everything to 1.

Theorem 3.2.5 (Linear independence of characters, by Dedekind)**.** Let S be a semigroup and K be a field. Let $\chi_1, \ldots, \chi_n : S \to K$ be pairwise different and nonzero characters. Then $\chi_1, \ldots, \chi_n$ are linearly independent over the K-vector space of functions $S \to K$.

Proof. We prove by induction on n. The case $n = 1$ is clear since χ_1 is nonzero. Suppose the statement is proved for $n \leq N$ and for a contradiction suppose it's false for $N+1$, i.e. there are $\lambda_i \in K, i = 1, \ldots, N+1$, not all zero, such that $\sum_{i=1}^{N+1} \lambda_i \chi_i = 0$. Though by inductive hypothesis, all λ_i's are nonzero. Also, if one has another relation $\sum_{i=1}^{N+1} \mu_i \chi_i = 0$, then one can scale some λ_i and μ_i and subtract one from another, obtaining a relation that again contradicts the inductive hypothesis (unless $\lambda_i = \mu_i \ \forall i = 1, \ldots, N+1$); hence the λ_i's are unique up to scaling.

Since $\chi_1 \neq \chi_2$, there is some $c \in S : \xi_1(c) \neq \xi_2(c)$. But since χ_i's are characters, $\chi_i(cx) = \chi_i(c)\chi_i(x) \ \forall x \in S$, so since $\sum_{i=1}^{N+1} \lambda_i \chi_i(x) = 0$, one has $\sum_{i=1}^{N+1} \lambda_i \chi_i(c)\chi_i(x) = 0 \ \forall x \in S$, i.e. $\sum_{i=1}^{N+1} \lambda_i \chi_i(c)\chi_i = 0$ contradicting uniqueness of λ_i's. □

Definition 3.2.6. An *algebraic integer* is a root of a monic polynomial with integer coefficients.

An *algebraic number* is a root of a polynomial with rational coefficients.

Every element of a finite extension of $\mathbb{Q}$ is an algebraic number, but not necessarily an algebraic integer.

Proposition 3.2.7. An element of a finite extension of $\mathbb{Q}$ is an algebraic integer iff its minimal polynomial has integer coefficients.

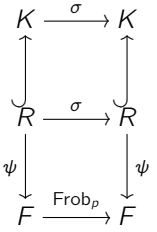
Proof. The "if" part is clear by definition, so suppose $f \in \mathbb{Z}[x]$ is monic such that $f(\alpha) = 0$. Let $g \in \mathbb{Q}[x]$ be the minimal polynomial of α. Then $g \mid f$, and by Gauss' lemma one has $g \in \mathbb{Z}[x]$. □

Proposition 3.2.8. If α, β are algebraic integers, then $\alpha + \beta, \alpha\beta$ are also algebraic integers.

Proof. See algebraic number theory which uses a group theoretic proof. □

Theorem 3.2.9. Let f be a degree n, monic, separable polynomial with coefficients in $\mathbb{Z}$ with a splitting field K. Let $Z = \{\lambda_1, \dots, \lambda_n\} \subset K$ be the set of roots of f. Let p be prime and f_p the reduction of f mod p. Suppose $\deg f_p = n$ and f_p is separable. Let F be a splitting field of f_p and $Z_p \in F$ be the set of roots of f_p. Define $R = \mathbb{Z}[\lambda_1, \dots, \lambda_n] \subset K$. Then

1. There is a ring homomorphism $\psi : R \to F$ giving a bijection $Z \xrightarrow{\sim} Z_p$.
2. A function $\varphi : R \to F$ is a ring homomorphism iff $\varphi = \psi \circ \sigma$ for some $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(K)$.
3. There is a $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(K)$ such that $\mathrm{Frob}_p \circ \psi = \psi \circ \sigma$.



Week 10, lecture 2, 6th December

Proof. Claim 1: As a group under addition, $R \cong \mathbb{Z}^r$ for some r by the structure of finitely generated abelian groups. Indeed, since $f(\lambda_i) = 0$, λ_i^n is a $\mathbb{Z}$-linear combination of $1, \lambda_i, \dots, \lambda_i^{n-1}$, so every monomial $\lambda_1^{a_1} \cdots \lambda_n^{a_n}$ is a $\mathbb{Z}$-linear combination of monomials with $a_1 \leq n-1$. Hence the abeian group R is finitely generated. Moreover, R is torsion-free as a subring of K, a field of characteristic 0.

Claim 2: A $\mathbb{Z}$-basis $u_1, \dots, u_d$ of R is also a basis of the $\mathbb{Q}$-vector space K.

Indeed; clearly $\mathrm{span}(u_1, \dots, u_d) = K$, and u_i's are linearly independent since a $\mathbb{Q}$-dependence relation gives a $\mathbb{Z}$-dependence relation by clearing denominators, contradicting that they form a $\mathbb{Z}$-basis.

1. By 3.2.8, each element of R is an algebraic integer. Now $\frac{1}{p} \in \mathbb{Q}$ is not an algebraic integer with minimal polynomial $x - \frac{1}{p}$, so $\frac{1}{p} \notin R$, i.e. p is not invertible in R. Recall that $(p) = R \iff p \in R^\times$, so $(p) \neq R$. By Claims 1 and 2, $R \cong \mathbb{Z}^d$ where $d = [K : \mathbb{Q}]$, so $R/(p) \cong (\mathbb{Z}/p\mathbb{Z})^r$ is finite. Take any maximal ideal in $R/(p)$, then its inverse image in R is a maximal ideal $\mathfrak{m} \subset R$ containing (p).

   Let $F = R/\mathfrak{m}$ (we'll show that F is a splitting field of f_p) and $\psi : R \to R/\mathfrak{m}$ be the canonical map. Since $\mathfrak{m}$ is maximal, it's a field. Note that $\mathbb{Z} \subset R \implies \psi(\mathbb{Z}) \subset \psi(R) = F$, and since $p \in \mathfrak{m} = \ker \psi$, one has $\psi(\mathbb{Z}) = \mathbb{F}_p$. Hence F is a finite extension of $\mathbb{F}_p$. Extend ψ to a homomorphism $R[x] \to F[x]$ with $x \mapsto x$, Then $f(x) = \prod_{i=1}^n (x - \lambda_i)$ is sent by ψ to $f_p(x) = \prod_{i=1}^n (x - \psi(\lambda_i))$. Since f_p is separable,the roots $\psi(\lambda_i), \dots \psi(\lambda_n)$ are distinct, so ψ does induce a bijection $Z \xrightarrow{\sim} Z_p$.

   Now we prove F is a splitting field of f_p, which is clear: as a ring R is generated by $\lambda_1, \dots \lambda_n$. so $\psi(R) = F$ is generated by $\psi(\lambda_1), \dots, \psi(\lambda_n)$ over $\mathbb{F}_p$.

2. $K/\mathbb{Q}$ is a Galois extension. Let $G = \mathrm{Gal}(K/Q) = \mathrm{Aut}_{\mathbb{Q}}(K)$. Each $\sigma \in G$ acts on R. Then $\psi \circ \sigma : R \xrightarrow{\sigma} R \xrightarrow{\psi} F$ is a ring homomorphism. Now $|G| = [K : \mathbb{Q}] = d$, so write $G = \{\sigma_1, \dots, \sigma_d\}$ and $\psi_i = \psi \circ \sigma_i$. To prove statement 2, for a contradiction suppose ψ_{d+1} is a ring homomorphism $R \to F$ not equal to any $\psi_i, i = 1, \dots, d$. Recall that $u_1, \dots, u_d$ is a $\mathbb{Z}$-basis of R. Consider the system of d linear equations in $x_1, \dots, x_{d+1}$ (variables with values in F)
$$\sum_{i=1} \psi_i(u_j) x_i = 0.$$
   By linear algebra, we have more variables than equations, so $\exists x_1, \dots, x_{d+1} \in F$ not all 0 satisfying the system, i.e. $\sum_{i=1}^{d+1} x_i \psi_i = 0$ at each $u_1, \dots, u_d$, hence $\sum_{i=1}^{d+1} x_i \psi_i = 0$ on R, so also on K. This contradicts 3.2.5.

3. Let φ be $\mathrm{Frob}_p \circ \psi$ and apply 2.

□

Week 10, lecture 3, 6th December

4 Complements on field extensions

4.1 Primitive element theorem

We've seen that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$, i.e. one only needs one element to generate this extension. It turns out this is true for all finite extensions of $\mathbb{Q}$.

Theorem 4.1.1 (Primitive element theorem)**.** Let $F \supset K$ be a finite field extension. Write $F = K(\alpha_0, \ldots, \alpha_n)$ such that the minimal polynomials of $\alpha_1, \ldots, \alpha_n$ are separable. Then $F = K(\gamma)$ for some $\gamma \in F$.

Proof. Suppose K is a finite field, then $F^\times$ is a cyclic group, so take γ to be a generator of $F^\times$.

Now suppose K is infinite. It suffices to show the statement for $n = 1$ by iterating inductively. Let f be the minimal polynomial of α_0 and g the minimal polynomial of α_1. Let $L \supset K$ be a splitting field of fg. Then $K \subset F(\alpha_0, \alpha_1) \subset L$. Since K is infinite, $\exists c \in K : \alpha_0 + c\alpha_1 \neq \alpha_0' + c\alpha_1'$ where $f(\alpha_0') = g(\alpha_1') = 0$ and $(\alpha_0', \alpha_1') \neq (\alpha_0, \alpha_1)$. Define $\gamma = a_0 + c\alpha_1$. We claim this is the γ we want. It suffices to show $\alpha_1 \in K(\gamma)$. Note that $f(\gamma - c\alpha_1) = f(\alpha_0) = 0$, i.e. $g(x)$ and $f(\gamma - cx)$ share the root α_1. But in fact α_1 is the only common root of $g(x)$ and $f(\gamma - cx)$ in L by our construction of c. This implies in L, the gcd of $g(x)$ and $f(\gamma - cx)$ is $x - \alpha_1$, but in $g(x), f(\gamma - cx) \in K(\gamma)[x]$ and calculating gcd works the same in different fields, so $x - \alpha_1 \in K(\gamma)[x]$, i.e. $\alpha_1 \in K(\gamma)$. □

Example 4.1.2. The proofs provides a constructive way to find the primitive element γ, e.g. for $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, one has $\sqrt{2} + c\sqrt{3} \neq -\sqrt{2} + c\sqrt{3}$ or $\sqrt{2} - c\sqrt{3}$ or $-\sqrt{2} - c\sqrt{3}$ when $c = 1$, so $F = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

Week 11, lecture 1, 10th December

4.2 Normal basis theorem

Definition 4.2.1. Let $L \supset K$ be a Galois extension of degree n and write $\mathrm{Gal}(L/K) = \{\sigma_1 = e, \sigma_2, \ldots, \sigma_n\}$. A *normal basis* of L over K is a basis of L as a K-vector space which is an orbit of $\mathrm{Gal}(L/K)$. Equivalently, we have $\alpha \in L$ such that $\sigma_1(\alpha) = \alpha, \sigma_2(\alpha), \ldots, \sigma_2(\alpha)$ is a basis of L over K.

Remark 4.2.2. We can then think of L as a representation of the finite group $\mathrm{Gal}(L/K)$ over K. (i.e. action of $\mathrm{Gal}(L/K)$ on L is by K-linear transformation). A normal basis, if it exists, gives L the structure of regular representation of $\mathrm{Gal}(L/K)$. (Recall that if G is a finite group and K a field, the regular representation of G over K is a vector space with basis the elements of G so that G acts on the basis vectors by left multiplication.)

Theorem 4.2.3. Every Galois extension admits a normal basis.

Proof for infinite fields. The primitive element theorem asserts the extension of $\alpha \in L$ such that $L = K(\alpha)$. Define $\alpha_i = \sigma_i(\alpha)$. (Then $\alpha_1 = \alpha$.) We claim $\alpha_i \neq \alpha_j$ if $i \neq j$. Indeed, if $\alpha_i = \alpha_j$, then $\sigma_i(\alpha) = \sigma_j(\alpha)$, i.e. α is fixed by $\sigma_j^{-1}\sigma_i$, hence fixed by the subgroup $H \neq \{e\}$ generated by it, so $K(\alpha) \subset L^H \subsetneq L$, a contradiction.

Let $f \in K[x]$ be the minimal polynomial of α. By construction, $\alpha_1, \ldots \alpha_n$ are n distinct roots of f in L, hence f is separable. Consider $g(x) = \frac{f(x)}{(x-\alpha)f'(\alpha)} \in L[x]$, which makes sense since $f'(\alpha) \neq 0$ (otherwise $(x - \alpha) \mid \gcd(f, f')$ and f wouldn't be separable). Define $g_i(x) = \sigma_i(g(x)) = \frac{f(x)}{(x-\alpha_i)f'(\alpha_i)} \in L[x]$ (applying σ_i to coefficients of g). Then $g_1 = g$. Also note $g_i(\alpha_j) = 0$ if $i \neq j$, and $g_i(\alpha_i) = \frac{\prod_{j\neq i}(\alpha_i - \alpha_j)}{\prod_{j\neq i}(\alpha_i - \alpha_j)} = 1$ (by product rule). In particular, $g(\alpha_1) = 1, g(\alpha_i) = 0$ for $i \neq 1$.

Let $A(x)$ be the $n \times n$ matrix with entries $A(x)_{ij} = (\sigma_i\sigma_j)(g(x))$ and define $D(x) = \det A(x)$. We claim $D(x)$ is a nonzero polynomial. It suffices to check $D(\alpha) \neq 0$. Calculate $A(\alpha)_{ij} = g_k(\alpha)$ where $\sigma_k = \sigma_i\sigma_j$. By above, $g_k(\alpha) = 1$ if $k = 1$ and $g_k(\alpha) = 0$ if $k \neq 1$, and $k = 1$ if $\sigma_i = \sigma_j^{-1}$. Hence every row of $A(\alpha)$ has a unique nonzero element and different rows have 1's in different columns (every element of a group has a unique inverse). So $A(\alpha)$ is the permutation matrix encoding $g \mapsto g^{-1}$ in $\mathrm{Gal}(L/K)$, and every permutation matrix has determinant ± 1, hence $D(\alpha) \neq 0$. Thus $D(x)$ has finitely many roots, so $\exists \beta \in K : D(\beta) \neq 0$.

Define $\gamma_i = g_i(\beta)$. We claim γ_i's form a desired normal basis. Indeed, $\gamma_i = \sigma_i(g(\beta))$ since β is fixed by $\mathrm{Gal}(L/K)$, so $\gamma_1, \ldots, \gamma_n$ is the $\mathrm{Gal}(L/K)$-orbit of $g(\beta)$. It remains to show $\gamma_1, \ldots, \gamma_n$ are linearly independent. For a contradiction, write $\sum_{j=1}^n x_j g_j(\beta) = 0$ for $x_1, \ldots, x_n \in K$ not all 0. Apply σ_i to this relation and obtain $\sum_{j=1}^n (\sigma_i\sigma_j)(g(\beta))x_j = 0$, i.e. $A(\beta)\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0$, but $D(\beta) \neq 0$, so $x_1 = \cdots = x_n = 0$, a contradiction. □

Week 11, lecture 2, 13th December

Proof for finite fields. Recall that if L/K is a (Galois) extension of finite fields, then $\mathrm{Gal}(L/K) \cong C_n$ where $n = [L : K]$, and it's generated by Frob_q where $q = |K|$. Observe that $\mathrm{Frob}_q : L \to L$ is a linear map of L as a K-vector space. By considering L as a $K[t]$-module via setting $t \cdot y = y^q = \mathrm{Frob}_q(y)$ for $y \in L$, one can

use structure of finitely generated modules over principal ideal domains (from Algebra 3): let f be the minimal polynomial of Frob_q and write $f(x) = \prod_{i=1}^{m} f_i(x)^{n_i}$ where each f_i is monic and irreducible and $n_i \geq 1$, then

$$L \cong \bigoplus_{i=1}^{m} \bigoplus_{a_{ij}} K[t]/(f_i(t)^{a_{ij}}) \qquad \text{where } \max(a_{ij}) = n_i.$$

We claim that (1) for each i, there is only one a_{ij}, namely n_i itself, and (2) $f(x) = x^n - 1$.

We first prove claim 2. Obviously Frob_q satisfies f since $|L| = q^n$. So $f \mid x^n - 1$. It remains to show $\deg f = n$, i.e. $(\mathrm{Frob}_q)^0 = \mathrm{id}, \mathrm{Frob}_q, \ldots, (\mathrm{Frob}_q)^{n-1}$ are linearly independent, which follows from 3.2.5 since they are distinct characters $L \to L$.

Now let $\chi(x)$ be the characteristic polynomial of Frob_q. Then $\deg \chi = n$, and Cayley–Hamilton says $\chi(\mathrm{Frob}_q) = 0$, so $\chi = f$, and claim 1 follows from $\chi(x) = \prod_{i=1}^{m} \prod_{a_{ij}} f_i(x)^{a_{ij}}$.

We can now write

$$L \cong \bigoplus_{i=1}^{m} K[t]/(f_i(t)^{n_i})$$

as a $K[t]$-module. Note that $f_i(t)^{n_i}$ and $f_j(t)^{n_j}$ are coprime for $i \neq j$, so by the Chinese remainder theorem, $L \cong K[t]/(f) = K[t]/(t^n - 1)$. Then the following is a basis of L as a K-vector space: $1, t, \ldots, t^{n-1}$, and clearly this is stable under multiplication by t. □

Week 11, lecture 3, 13th December: problem class

No mastery material.