MA3D5 Galois theory :: Lecture notes

Lecturer: Gavin Brown

April 26, 2024

Contents

Week 1, lecture 1: a mixture of review and teaser, giving the essential idea behind how Galois showed quintic was not solvable

Week 1, lecture 2 starts here

1 Field extension

Definition 1.0.1. $\varphi : K \to L$ where K, L fields is a *(field) homomorphism* if it is a ring homomorphism.

Proposition 1.0.2. Let $\varphi : K \to L$ be a homomorphism. Then φ is injective.

Proof. Suppose $a, b \in K : \varphi(a) = \varphi(b)$. Then $\varphi(a-b) = \varphi(a) - \varphi(b) = 0$. It then suffices to prove that the only element $c \in K : \varphi(c) = 0$ is $c = 0$. Suppose $c \neq 0$. Then $c^{-1} \in K$ and $\varphi(c)\varphi(c^{-1}) = \varphi(cc^{-1}) = \varphi(1) = 1$, so $\varphi(c) \neq 0$, a contradiction. □

Definition 1.0.3. A *field extension* is a (ring) homomorphism $\varphi : K \to L$, denoted L/K.

Remark.

1. Any subfield $K \subset L$ gives a field extension L/K.
2. If $\varphi : K \to L$, then it is injective by above, and we can write $\varphi : K \to K' = \varphi(K) \subset L$. So if we are not given a inclusion map, then K and K' are basically the same field (they are certainly isomorphic), and K' is just a copy of K sitting somehow inside L. Mostly we simply think of L/K as $K \subset L$.

1.1 Field extensions as vector spaces

Proposition 1.1.1. Let L/K be a field extension. Then L is a vector space over K, or K-vector space.

If we want to do scalar multiplication, i.e. multiply an element in L by an element λ in K, we just use φ to bring λ to K', consistent with remark above.

Definition 1.1.2. The *degree* of L/K, denoted $[L : K]$, is the dimension of L as a K-vector space. L/K is a *finite extension* if $[L : K]$ is finite. Otherwise, it's an *infinite extension.*

Note that if $[L : K] = 1$ then $L = K$.

Theorem 1.1.3 (Tower law)**.** If M/L and L/K are field extensions, then M/K is an extension, and if both M/L and L/K are finite, then

$$[M : K] = [M : L][L : K].$$

If either is infinite then so is M/K.

Proof sketch. Let $a_1, \ldots, a_n \in L$ be a basis of L as a K-vector space, and $b_1, \ldots, b_m \in M$ be a basis of M as a L-vector space. It suffices to prove that

$$\{a_i b_j \in M : 1 \leq i \leq n,\ 1 \leq j \leq m\}$$

is a basis of M as a K-vector space. □

Definition 1.1.4. If $K \subset L \subset M$, then L is an *intermediate field* of M/K.

1.2 Adjoining a square root to a subfield of $\mathbb{C}$

Suppose $s \in K$ is not a square in K. Choose $K \not\ni \alpha = \sqrt{s} \in \mathbb{C}$. Define $K(\alpha)$ to be the smallest subfield of $\mathbb{C}$ that contains K and α. Formally, it's

$$\left\{\frac{p(\alpha)}{q(\alpha)} : p, q \in K[x],\ q(\alpha) \neq 0\right\}.$$

Consider any $\xi = \dfrac{p(\alpha)}{q(\alpha)} \in K(\alpha)$. If we see α^2 we replace by s, α^3 by αs, α^4 by s^2 and so on, i.e. there won't be α of degree higher than 1, i.e. $\exists a, b, c, d \in K : \xi = \dfrac{a + b\alpha}{c + d\alpha}$ where $c + d\alpha \neq 0$. So

$$\xi = \frac{a + b\alpha}{c + d\alpha}\frac{c - d\alpha}{c - d\alpha} = \frac{ac - bds}{c^2 - d^2 s} + \frac{bc - ad}{c^2 - d^2 s},$$

which tells us that $1, \alpha$ span $K(\alpha)$, and of course they are linearly independent since if $e + f\alpha = 0$ where $e, f \in K$ then $e = f = 0$ since otherwise it would mean that $\alpha \in K$ which is assumed at first to be false. One concludes that $[K(\alpha) : K] = 2$.

Week 2, lecture 1 starts here

2 A brief review

3 things first:

1. Consider the (principal) ideal $(f) = \{fg : g \in \mathbb{R}[x]\}$ and the quotient ring $\mathbb{R}[x]/(f) = \{g + (f) : g \in \mathbb{R}[x]\}$. (**The golden rule:** $g_1 + (f) = g_2 + (f) \Leftrightarrow g_1 - g_2 \in (f)$. When we lazily omit '$+(f)$' and simply write g in place of $g + (f)$, we must remember that two polynomials g_1, g_2 define exactly the same element of quotient ring $\mathbb{R}[x]/(f)$ iff $g_1 - g_2 \in (f)$, i.e. $g_2 = g_1 + hf$ where $h \in \mathbb{R}[x]$.

   Consider $f = x^2 + 1 \in \mathbb{R}[x]$ and let $g = x^3 + 2x^2 + 3$. Then $g + (f) \in \mathbb{R}[x]/(f)$, and add, subtract g by multiple of f won't change the coset, and note $x^3 + 2x^2 + 3 - x(x^2 + 1) - 2(x^2 + 1) = 1 - x$. Now let $g = x^2$ then $g = g - f = -1$.

   $\mathbb{R}[x]/(f)$ in this case is $\cong \mathbb{C}$.

   Proof. Let $\varphi : \mathbb{R}[x] \to \mathbb{C}$ be defined by $x \mapsto i$. This is surjective since $\varphi(ax + b) = ai + b$. We claim $\ker\varphi = (x^2 + 1)$.

   Clearly $x^2 + 1 \in \ker\varphi$ since $\varphi(x^2 + 1) = \varphi(x)^2 + 1 = i^2 + 1 = 0$, so $(f) \subseteq \ker\varphi$.

   If $g \in \ker\varphi$, apply division algorithm:

   $$\text{given } f, g \in K[x] \text{ where } K \text{ field, } \exists! q, r \in K[x] : f = gq + r \text{ where } \deg r < \deg g$$

   $\exists h, r \in \mathbb{R}[x] : g = fh + r$ and $\deg r < \deg f = 2$, so we can write $r = ax + b$. Then $\varphi(g) = 0 = \varphi(f)\varphi(h) + \varphi(r) = \varphi(r) = ai + b \Leftrightarrow a = b = 0$. So $g = fh \in (f)$, hence $\ker\varphi \subseteq (f)$.

   This desired then follows by the first isomorphism theorem. □

2. **Easier context.** Let K be a field, then $\exists!$ ring homomorphism $\varphi : \mathbb{Z} \to K$. We can agree that either
   (a) $\ker \varphi = (0) = \{0\}$ (we say K has characteristic 0, denoted $\operatorname{char} K = 0$) and $\mathbb{Q} \subset K$ or
   (b) $\ker \varphi = (n) = n\mathbb{Z}$ for some $n > 0$, then n must be prime p, and $\operatorname{char} K = p$ and $\mathbb{Z}/p\mathbb{Z} \subset K$

   and it can't be that both are true and the p in (b) is unique, e.g. $K = \mathbb{Q}(\sqrt{2}) \supset \mathbb{Q}$ so $\operatorname{char} K = 0$ and $K = \mathbb{F}_7(t) \supset \mathbb{F}_7$ so $\operatorname{char} K = 7$.

   Sanity check.
   (a) If $\frac{a}{b} \in \mathbb{Q}$, define $\varphi\left(\frac{a}{b}\right) = \frac{\varphi(a)}{\varphi(b)}$. Since $b \neq 0$, $\varphi(b) \neq 0$. Now
   $$\varphi\left(\frac{a}{b}\right) = \varphi\left(\frac{c}{d}\right) \Rightarrow \varphi(ad - bc) = 0 \Rightarrow ad - bc = 0 \Rightarrow \frac{a}{b} = \frac{c}{d},$$
   so injective.
   (b) If $n = pq$ then $0 = \varphi(n) = \varphi(p)\varphi(q)$ but $\varphi(p), \varphi(q) \neq 0$ since $p, q < n$, so n must be prime.

3. Let K be a field and $f \in K[x]$ monic of degree d. **Motto:** working in $K[x]/(f)$ is the same as working in $K[x]_{<d}$ and letting $f = 0$ wherever required (or equivalently, using f to substitute $x^d = -a_{d-1}x^{d-1} - \cdots - a_1 x - a_0$ wherever multiplication results in degree $\geq d$). The point is, considering division algorithm, working in $\mathbb{K}[x]/(f)$ is the same as working with the remainder r.

Week 2, lecture 2 starts here (Matteo takes over)

3 Quadratic and cubic formula

3.1 Quadratic

Consider $x^2 + ax + b$. To find the root we Babylonian it: let $x = y - \frac{a}{2}$, then
$$\left(y - \frac{a}{2}\right)^2 + a\left(y - \frac{a}{2}\right) + b = 0$$
which gives $y^2 - c = 0$ where c is the discriminant $\frac{a^2-4b}{4}$ and $y = \pm\sqrt{c}$.

3.2 Cubic

Now consider $x^3 + ax^2 + bx + c$. We do a similar thing: let $x = y - \frac{a}{3}$ (complete the cube) and
$$\left(y - \frac{a}{3}\right)^3 + a\left(y - \frac{a}{3}\right)^2 + b\left(y - \frac{a}{3}\right) + c$$
gives
$$y^3 + px + q \text{ where } p = -\frac{a^3}{3} + b,\ q = \frac{2a^3}{27} - \frac{ab}{3} + c.$$

Now let $y = z - \frac{p}{3z}$, we get $z^6 + qz^3 - \frac{p^3}{27}$ and it's a quadratic in the variable z^3, so we have

$$z^3 = \frac{-q \pm \sqrt{q^2 + \frac{4p^3}{27}}}{2},$$

We then let discriminant $D := q^2 + \frac{4p^3}{27}$ and we let $\alpha =: \sqrt{D}$, and $\beta = \sqrt[3]{\frac{-q+\alpha}{2}}$, $\gamma = \sqrt[3]{\frac{-q-\alpha}{2}}$ are two candidates of roots. Note

$$(\beta\gamma)^3 = \left(\frac{-q+\alpha}{2}\right)\left(\frac{-q-\alpha}{2}\right) = \frac{1}{4}(q^2 - \alpha^2) = \frac{1}{4}\left(q^2 - \left(q^2 + \frac{4p^3}{27}\right)\right) = \left(-\frac{p}{3}\right)^3,$$

so by choosing β, γ as the roots, $\beta\gamma = -\frac{p}{3}$. Also, if we multiply z on both sides of the substitution formula,

$$z^2 - yz - \frac{p}{3},$$

this is a quadratic and we know $y = \beta + \gamma$ and $-\frac{p}{3} = \beta\gamma$ by Vieta's.
We now claim $\beta + \gamma,\ \omega\beta + \omega^2\gamma,\ \omega^2\beta + \omega\gamma$ where ω is the cubic root of unity are the three roots. By plugging them in we can verify. To write them explicitly,

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

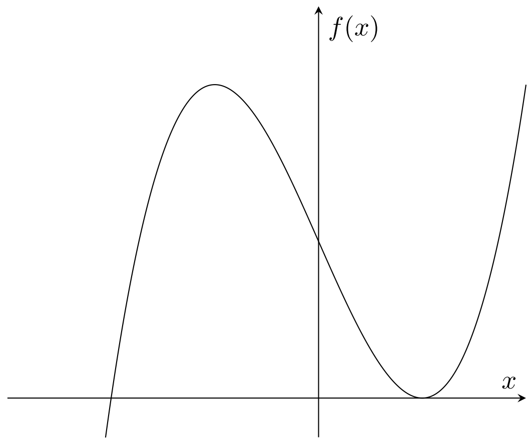
and one can then write the formulae in terms of the original a, b, c but that would be too long.

Week 2, lecture 3 starts here

3.2.1 Real solutions for real cubics

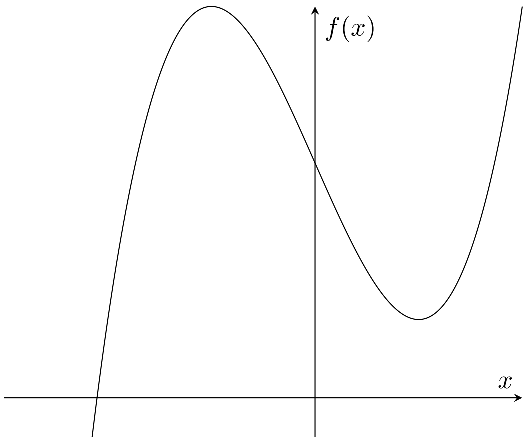
As in the context of above and let $p, q \in \mathbb{R}$.

1. When $D = 0$, $q^2 = -\frac{4p^3}{27} \Rightarrow p < 0$. Also $\beta = \gamma = \sqrt[3]{\frac{-q}{2}}$. (Check:$\beta\gamma = \sqrt[3]{\frac{q^2}{4}} = \frac{-p}{3}$) So $y_1 = 2\beta$ and $y_2 = y_3 = \beta(\omega + \omega^2) = -\beta$. Note that all roots are real.
   e.g. $f = x^3 - 3x + 2$, $x_1 = -2$, $x_2 = x_3 = 1$ are roots.



2. When $D > 0$, $\sqrt{D} \in \mathbb{R}$ then at least $\beta, \gamma \in \mathbb{R}$ but only $y_1 = \beta + \gamma$ is real and $y_2 = \omega\beta + \omega^2\gamma$, $y_3 = \omega^2\beta + \omega\gamma$ are complex conjugates.

   e.g. $f = x^3 - 3x + 3$, $x_1 = -2$ is a real root.

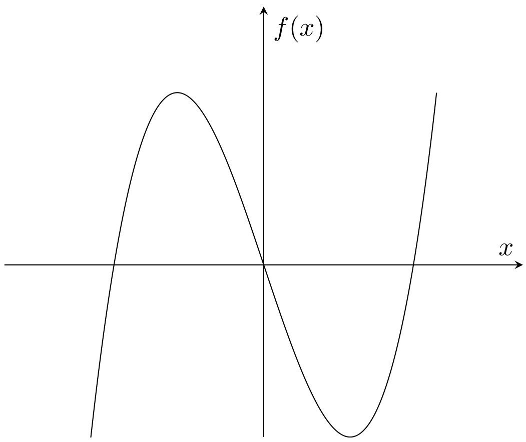


3. When $D < 0$, then $\sqrt{D} =: \alpha \in \mathbb{C}\backslash\mathbb{R}$. But note that

$$\beta^3 = \frac{-q + i|\alpha|}{2}, \quad \gamma^3 = \frac{-q - i|\alpha|}{2}$$

   are conjugates, hence β, γ are conjugates as well since $\beta\gamma = \frac{-p}{3}$. Now $y_1 = \beta + \overline{\beta}$, $y_2 = \omega\beta + \overline{\omega\beta}$ and $y_3 = \omega^2\beta + \overline{\omega^2\beta}$ are all reals. The problem is we cannot avoid complex computations during the process (in algebra jargon, this means you need the field extension $\mathbb{Q}(\alpha, \beta, \omega)/\mathbb{Q}$), so people back in the days thought this was bad. (Casus irreducibilis)

   e.g. $f = x^3 - 3x$, $x_1 = 0$, $x_{2,3} = \pm\sqrt{3}$ are roots.



3.2.2 Trigonometric

We know

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta$$

which can be treated as a cubic by letting $y := \cos\theta$

$$y^3 - \frac{3}{4}y - \frac{1}{4}\cos 3\theta = 0$$

and we immediately have solutions $y_1 = \cos\theta,\ y_2 = \cos\left(\theta + \frac{2\pi}{3}\right),\ y_3 = \cos\left(\theta + \frac{4\pi}{3}\right)$.
This can be adapted to solve $y^2 + px + q = 0$ in general as long as $q \in \left[-\frac{1}{4}, \frac{1}{4}\right]$.

Week 3, lecture 1 starts here

4 Factorisation

Recall that a field K gives a UFD $K[x]$, i.e. a commutative ring with no zero divisors and every element in which can be uniquely written as a product of irreducible elements up to reordering and multiplication by units. $f \in K[x]$ is *reducible* if $\deg f > 0$ and $\exists g, h \in K[x] : \deg g, h > 0$ and $f = gh$.
The question of whether $f \in K[x]$ is irreducible is generally really hard (and depends on K).

4.1 Roots

Definition 4.1.1. $\alpha \in K$ is a *root* of $f \in K[x]$ if $f(\alpha) = 0 \in K$.

Corollary 4.1.2. The following are equivalent:

1. α is a root of f
2. $(x - \alpha) \mid f$
3. $\exists g \in K[x] : f = (x - \alpha)g$ (g can be constant)

Proof. 2 and 3 are equivalent by definition.

$3 \Rightarrow 1$: $f(x) = (x - \alpha)g(x)$ so $f(\alpha) = (\alpha - \alpha)g(\alpha) = 0 \cdot g(\alpha) = 0$.

$1 \Rightarrow 3$: Since $K[x]$ is a UFD we can do Euclidean division, i.e. $\exists g, r \in K[x] : f(x) = (x-\alpha)g(x) + r(x)$ where $\deg r < \deg x - \alpha = 1$, so $r \in K$. Since $0 = f(\alpha) = r(x)$, one has what's desired.

□

Remark. Being reducible is not equivalent to having a root, e.g. $x^4 + 3x^2 + 2 \in \mathbb{Q}[x]$ is reducible to $(x^2 + 1)(x^2 + 2)$ but has no roots. This is only true when we are in an algebraically closed field (e.g. $\mathbb{C}$) or $\deg f \leq 3$ so that when it's reduced we are guaranteed to have a linear term.

4.2 $\mathbb{C}[x]$ vs $\mathbb{Q}[x]$

Theorem 4.2.1 (Fundamental theorem of algebra)**.** Any $f \in \mathbb{C}[x]$ factorises into linear factors:

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

where $n = \deg f$ and $\alpha_i \in \mathbb{C}$.

This does not hold in $\mathbb{Q}[x]$, e.g. x^2+1. So in terms of factorisation, $\mathbb{Q}[x]$ is harder to work with. To make the situation better we go in $\mathbb{Z}[x]$. Clearly $\mathbb{Z}$ is not a field but still $\pm 1 \in \mathbb{Z}[x]$ and it's a UFD (not a PID), so conclusions about factorisations apply.

Lemma 4.2.2 (Gauss')**.** Let $f = a_m x^m + \cdots + a_0 \in \mathbb{Z}[x]$ suppose $\gcd(a_0, \ldots, a_m) = 1$ (*primitive*). If $f = gh$ where $g, h \in \mathbb{Q}[x],\ \deg g, h > 1$ then $\exists b \in \mathbb{Q}^* : bg, b^{-1}h \in \mathbb{Z}[x]$.

This is just common sense: one can clear denominators of quotients to get integers (let's still do a proof later though). The real punchline of the lemma is:

Corollary 4.2.3. If f is irreducible in $\mathbb{Z}[x]$ then it's irreducible in $\mathbb{Q}[x]$.

Week 3, lecture 2 starts here

Remark. We didn't define irreducibility in $\mathbb{Z}[x]$ since $\mathbb{Z}$ is not a field. But note that a non-1 $n \in \mathbb{Z}$ is not a unit in $\mathbb{Z}[x]$, so we consider it as irreducible. Hence the assumption that f is irreducible in $\mathbb{Z}[x]$ implies f is primitive since if we can factor out a non-1 integer then it's reducible. It's only because of this that we can apply Gauss' lemma.

4.3 $\mathbb{Z}[x]$

4.3.1 Rational root test

Recall that if $f \in \mathbb{Q}[x]$ with $\deg f = 2, 3$ is reducible then f has a root in $\mathbb{Q}$.

Lemma 4.3.1. If $f = a_m x^m + \cdots + a_0 \in \mathbb{Z}[x]$ and $f(a) = 0,\ a \in \mathbb{Z}$ then $a \mid a_0$.

Proof. One has $f(a) = a_m a^m + \cdots + a_1 a + a_0 = 0$ and $a \mid a_m a^m + \cdots + a_1 a,\ a \mid 0$, so $a \mid a_0$. $\square$

Proposition 4.3.2 (Rational root test)**.** If $f = a_m x^m + \cdots + a_0 \in \mathbb{Z}[x],\ a_m \neq 0$ and $\frac{r}{s} \in \mathbb{Q}$ is a root of f, then $r \mid a_0,\ s \mid a_m$.

Proof. In $\mathbb{Q}[x]$ one has

$$f(x) = \left(x - \frac{r}{s}\right) g(x).$$

By Gauss'

$$\exists b \in \mathbb{Q}^\times : b(sx - r), \frac{g(x)}{bs} \in \mathbb{Z}[x],$$

which makes the desired obvious. $\square$

Example 4.3.3. Is $f = x^3 - 4x + 5$ irreducible in $\mathbb{Q}[x]$? Again $\deg f = 3$ so if it's not irreducible (so reducible) then it's of the form $f = gh$ where WLOG $\deg g = 1,\ \deg f = 2$, so it would have a rational root satisfying rational root test. The only possibility for a root x_i is then $x_i = \pm 1,\ \pm 5$, but $f(x_i) \neq 0\ \forall i$, hence f is irreducible in $\mathbb{Q}[x]$.

4.3.2 Eisenstein's criterion

Proposition 4.3.4. If $f = a_m x^m + \cdots + a_0 \in \mathbb{Z}[x]$ and $\exists$ a prime $p \in \mathbb{Z} : p \nmid a_m,\ p \mid a_i\ \forall i = 1, \ldots, m-1$ and $p^2 \nmid a_0$ (i.e. f is *Eisenstein at prime* p) then f is irreducible in $\mathbb{Z}[x]$ (and therefore $\mathbb{Q}[x]$).

Week 3, lecture 3 starts here

Proof. Suppose $f = gh$ where $g, h \in \mathbb{Z}[x]$ and $\deg g, h > 0$, $g = \sum^H b_i x^i$, $h = \sum^k c_i x^i$ (where $H, k < m$). Then $a_0 = b_0 c_0$. Since $p \mid a_0$, WLOG $p \mid b_0$ and $p \nmid c_0$. Also $a_m = b_H c_k$, so since $p \nmid a_m$, p does divide all b_i. Choose b_j to be the coefficient such that $p \nmid b_j$ and j is minimal. But note that

$$a_j = b_0 c_j + b_1 c_{j-1} + \cdots + b_j c_0$$

and $p \mid a_j$, $p \mid b_{0,\ldots,j-1}$, $p \nmid c_0$, so p must divide b_j, a contradiction. $\square$

Example 4.3.5. Is $f = \frac{1}{2}x^3 + x^2 - \frac{4}{3}x + \frac{5}{9}$ irreducible in $\mathbb{Q}[x]$? First one makes it a polynomial in $\mathbb{Z}[x] : 18f = 9x^2 + 18x^2 - 24x + 10$. $p = 3$ is not a candidate since $3 \mid 9$, and since $18 = 2 \times 3^2$, one can only choose $p = 2$. Indeed, $2 \nmid 9$, $2 \mid 18$, $2 \mid 24$, $2 \mid 10$, $4 \nmid 10$, so $18f$ is irreducible in $\mathbb{Z}[x]$, so $\mathbb{Q}[x]$, and since $18 \in \mathbb{Q}^*$, f is irreducible in $\mathbb{Q}[x]$.

Example 4.3.6 (Prime cyclotomic)**.** $f = x^{p-1} + \cdots + 1 = \frac{x^p - 1}{x-1} \in \mathbb{Q}[x]$ has pth roots of unity except 1 as its complex roots. One can't apply Eisenstein since all coefficients are 1, but one can substitute by $x = y + 1$ which is an automorphism of $\mathbb{Q}[x]$ and

$$f = p + \frac{p!}{2!(p-2)!}y + \cdots + y^{p-1}$$

which is clearly Eisenstein at p, so f is irreducible.

4.3.3 Reduction modulo prime p

Proposition 4.3.7. Let $f = a_m x^m + \cdots + a_0 \in \mathbb{Z}[x]$, a prime $p \in \mathbb{Z} : p \nmid a_m$, and $\overline{f} = \overline{a_m} x^m + \cdots + \overline{a_0} \in \mathbb{F}_p[x]$ the reduction of f mod p. If $\overline{f}$ is irreducible in $\mathbb{F}_p[x]$ then f is irreducible in $\mathbb{Z}[x]$ (and therefore $\mathbb{Q}[x]$).

Proposition 4.3.8. Suppose $f = gh$ where $g, h \in \mathbb{Z}[x]$ and $\deg g, h > 0$, $g = \sum^H b_i x^i$, $h = \sum^k c_i x^i$. Then $\overline{f} = \overline{g}\overline{h}$. It then suffices to see that $\deg g, h = \deg \overline{g}, \overline{h}$. Indeed, since $p \nmid a_m = b_H c_k$, $p \nmid b_H$ nor c_k.

Example 4.3.9. Which of these are irreducible in $\mathbb{Q}[x]$?

1. $f = x^3 + 9x + 6$
   (a) Eisenstein: indeed, f is Eisenstein at $p = 3$, so irreducible
   (b) Rational root test: if f is reducible, the only possible roots are $\pm 1, \pm 2, \pm 3, \pm 6$, each of which is not a root, so irreducible
   (c) Reduction modulo 2: $\overline{f} = x^3 + x = x(x^2 + 1) = x(x+1)^2 \in \mathbb{F}_2[x]$, so inconclusive
2. $x^7 + 15x^2 + 9x - 3$
   (a) Rational root test: if f has a root $\frac{r}{s}$ then $r \mid 3$, so $r = \pm 1, \pm 3$, each of which does not give a root
   (b) Eisenstein: indeed, f is Eisenstein at $p = 3$, so irreducible
   (c) Reduction modulo 2: $\overline{f} = x^7 + x^2 + x + 1$ is reducible in $\mathbb{F}_2[x]$ since 1 is a root, so inconclusive

Week 4, lecture 1 starts here

Proof of Gauss' lemma. Suppose $f \in \mathbb{Z}[x] : f = gh$ where $g, h \in \mathbb{Q}[x]$.

1. We know $\exists a, b \in \mathbb{Q} : g = ag_1,\ h = bh_1$ where $g_1, h_1 \in \mathbb{Z}[x]$ and are primitive.
2. It remains to see that $a = b^{-1}$. Write $f = gh = abg_1h_1$ and $ab = \frac{r}{s} \in \mathbb{Q}$ where $\gcd(r, s) = 1,\ s > 0$.
   (a) Case 1: $s = 1$, then $r \mid a_i\ \forall i$, but f is primitive, so $r = \pm 1$, hence indeed $a = b^{-1}$
   (b) Case 2: $s > 1$, then one has p prime such that $p \mid s,\ p \nmid r$, so p divides all coefficients of g_1h_1. We claim that in this case, p divides all coefficients of g_1 or h_1. Suppose there exists a coefficient b_i of g_1 that's not divisible by p with i minimal, and a coefficient c_k of h_1 that's not divisible by p with k minimal. Now set $N = j + k$, then the coefficient $d_N = b_0c_N + \cdots + b_jc_k + \cdots + b_Nc_0$ of g_1h_1 is divisible by p, a contradiction.

□

Example 4.3.10 (Using reduction modulo prime p)**.** $f = x^3 + ax + b \in \mathbb{Z}[x],\ a, b$ odd. Then $\overline{f} = x^3 + x + 1 \in \mathbb{F}_2[x]$. One can check that it has no roots easily by going through all elements of $\mathbb{F}_2$, i.e. 0 and 1. So $\overline{f}$ is irreducible in $\mathbb{F}_2[x]$, hence irreducible in $\mathbb{Z}[x]$, hence irreducible in $\mathbb{Q}[x]$.

Example 4.3.11. Is $f = x^4 - 7x^2 + 12$ irreducible?

1. Rational root test: possible roots $\frac{r}{s}$ satisfy $r = \pm 1, \pm 2, \pm 3, \pm 4, \pm 6$, too much calculation
2. Eisenstein: there is no prime we can try since 7 is prime and $7 \nmid 12$, so inconclusive
3. Reduction modulo 2: $\overline{f} = x^4 + x^2$ is clearly reducible, so again inconclusive

Well... in fact f is pretty easy to decompose since $-3 - 4 = -7$ and $(-3)(-4) = 12$, so $f = (x^2 - 3)(x^2 - 4) = (x^2 - 3)(x + 2)(x - 2)$, so in our mind we know it's reducible.

Week 4, lecture 2 starts here (Gavin is back)

5 Continuation of chapter 1

5.1 Simple extension

Definition 5.1.1. L/K is simple if $\exists \alpha \in L : K(\alpha) = L$.

Lemma 5.1.2. Given L/K and $\alpha \in L$,

$$\begin{aligned} \mathrm{ev}_\alpha : K[x] &\to L \\ g &\mapsto g(\alpha) \end{aligned}$$

is a ring homomorphism uniquely defined by $K \to L$ and $x \mapsto \alpha$.

Proof. We write e for ev_α:

1. $e(1) = 1$
2. $e(f + g) = (f + g)(\alpha) = f(\alpha) + g(\alpha) = e(f) + e(g)$

3. $e(fg) = (fg)(\alpha) = f(\alpha)g(\alpha) = e(f)e(g)$

Now suppose φ is also a homomorphism with $\varphi(x) = \alpha$ and $\varphi|_K$ is $K \to L$. Then

$$\varphi(bx^n) = \varphi(b)\varphi(x)^n = b\alpha^n = \mathrm{ev}_\alpha(bx^n).$$

$\square$

Proposition 5.1.3. *L/K, $\alpha \in L$ and ev_α as above. Exactly one of the following occurs:*

1. *ev_α is injective, then it extends to*

$$\widetilde{\mathrm{ev}_\alpha} : K(x) \to K(\alpha) \subset L.$$

2. *(much more interesting) ev_α is not injective, then $\ker(\mathrm{ev}_\alpha) = (f)$ where $f \in K[x]$ is irreducible and $\deg f \geq 1$, i.e. $f(\alpha) = 0$ and for any $g : g(\alpha) = 0,\ f \mid g$. Moreover, ev_α induces an isomorphism $K[x]/(f) \cong K[\alpha] = K(\alpha) \subset L$ (1st isomorphism theorem).*

Proof. The injective case is boring since it's same as for $\mathbb{Z}$.
Now $K[x]$ is a PID, so $\ker \mathrm{ev}_\alpha = (f)$ for some $f \in K[x]$. It remains to prove f is irreducible. If $f = gh$ where $1 < \deg g, h < \deg f$, then WLOG $g(\alpha) = 0$, so $g \in (f)$, so $f \mid g$, a contradiction. $\square$

Definition 5.1.4. L/K and $\alpha \in L$. If $\exists$ monic $f \in K[x] : f(\alpha) = 0$ then α is *algebraic* over K. If not, then α is *transcendental* over K.

Remark (A miraculous proof of $K[\alpha] = K(\alpha)$ where K field not using conjugates)**.** By the 1st isomorphism theorem, $K[x]/(f) \cong K[\alpha]$. But f is irreducible, so (f) is prime, so $K[x]/(f)$ is a field. Hence $K[\alpha]$ is also a field and it must be the same field as $K(\alpha)$.

When α is algebraic, the monic polynomial f of smallest degree such that $f(\alpha) = 0$ is called the *minimal polynomial* of α over K.

Proposition 5.1.5. *$K \subset K(\alpha)$ is a simple extension by algebraic α with minimal polynomial $f \in K[x]$ and $n := \deg f > 1$. Then $1, \alpha, \alpha^2, \ldots, \alpha^{n-1} \in K(\alpha)$ is a K-basis for $K(\alpha)$ and so $[K(\alpha) : K] = n$.*

Proof. Let $V := K[x]_{<n}$, $W := K[x]/(f) \cong K(\alpha)$ as a K-vector space and define $L : V \to W$ by $h \mapsto h + (f)$.

1. Surjective: given $h + (f) \in W$, write $h = qf + r$ where $\deg r < \deg f$, then $L(r) = r + (f) = r + qf + (f) = h(f)$.

2. Injective: uniqueness of r.

So L is bijective, and since V has $1, x, x^2, \ldots, x^{n-1}$ as a basis, we can map it to get the desired basis of $K(\alpha)$. $\square$

Week 4, lecture 3 starts here

5.2 Adjoining a root of a polynomial

Theorem 5.2.1. $f \in K[x]$ monic, irreducible and $\deg f \geq 2$. Then $\exists L/K$ and $\alpha \in L : L = K(\alpha)$ is simple and $f(\alpha) = 0$. Moreover, f is minimal polynomial of α over K, so $[L : K] = \deg f$.

In other words, if you have an irreducible polynomial, there *is* a bigger field in which it has a root.

Proof. Set $L = K[x]/(f)$.

1. This is indeed a field since f is irreducible.
2. $K \hookrightarrow K[x] \twoheadrightarrow K[x]/(f) = L$ is injective by Proposition 1.0.2.
3. Set $\alpha = x + (f) \in L$, then general elements of L of the form $h + (f)$ are exactly $h(\alpha)$.
4. $f(\alpha) = f + (f) = 0 + (f) = 0_L$.
5. Since f is monic, irreducible and vanishes α it's minimal. By Proposition 5.1.5 $[L : K] = \deg f$.

□

Corollary 5.2.2. Let $f \in K[x]$ by any polynomial with $\deg f \geq 1$. Then $\exists L/K$ and $\alpha \in L$: $f(\alpha) = 0,\ L = K(\alpha)$.

Proof. Pick any irreducible factor of f and apply theorem above. □

5.3 Algebraic extension / finite extension

Definition 5.3.1. L/K is *algebraic* if any $\alpha \in L$ is algebraic over K.

Proposition 5.3.2. Finite extensions are algebraic.

Proof. Suppose $[L : K] = n \geq 1$. If $\alpha \in L$, consider $n + 1$ elements $1, \alpha, \alpha^2, \ldots, \alpha^n$ in the n-dimensional K-vector space L. This means there is a linear dependence relation

$$c_0 + c_1\alpha + c_1\alpha^2 + \cdots + c_n\alpha^n = 0 \text{ where not all } c_i \text{ are zero.}$$

Set $s := \max\{i : c_i \neq 0\}$ and write

$$f(x) := \frac{c_0}{c_s} + \frac{c_1}{c_s}x + \cdots + \frac{c_{s-1}}{c_s}x^{s-1} + x^s.$$

Then f is monic and $f(\alpha) = 0$. □

5.4 Maps between fields

Definition 5.4.1. Suppose L/K and M/K are two extensions of the same field. A K-homomorphism $\varphi : L \to M$ is a homomorphism that fixed all elements of K, i.e. $\varphi(\alpha) = \alpha\ \forall \alpha \in K$.

Definition 5.4.2 (Main object of study)**.**

$$\mathrm{Emb}_K(L, M) := \{\varphi : L \to M : \varphi \text{ is a } K\text{-homomorphism}\}.$$

Remark. This is not a group because if one has two maps from L to M one cannot compose them because M might not be equal to L. Even it is, φ is certainly injective because it's a map of fields, but if L, M are infinite dimensional there's no reason why it needs to be surjective. But, if $L = M$ are finite extensions of K then $\mathrm{Emb}_K(L, M)$ is a group, called the *Galois group* $\mathrm{Gal}(L/K)$. Otherwise, it's just a set and has no real structure.

Example 5.4.3. $L = \mathbb{C}$, $K = \mathbb{R}$, then complex conjugation $\mathbb{C} \to \mathbb{C}$ by $z \mapsto \overline{z}$ is a K-homomorphism (also a $\mathbb{Q}$-homomorphism, a $\mathbb{Q}\left(\sqrt{2}\right)$-homomorphism).

Big idea 5.4.4. Suppose $\varphi \in \mathrm{Emb}_K(L, M)$. If $\alpha \in L$ is a root of $f \in K[x]$, then $\varphi(\alpha)$ is a root of f in M.

Proof. Write $f = a_n x^n + \cdots + a_1 x + a_0$ where $a_i \in K$. Then

$$\begin{aligned} f(\varphi(\alpha)) &= a_n \varphi(\alpha)^n + \cdots + a_1 \varphi(\alpha) + a_0 \\ &= \varphi(a_n)\varphi(\alpha)^n + \cdots + \varphi(a_1)\varphi(\alpha) + \varphi(a_0) \\ &= \varphi(f(\alpha)) = \varphi(0) = 0. \end{aligned}$$

□

Proposition 5.4.5. L/K with $f \in K[x]$ irreducible and $\alpha, \beta \in L$ roots of f. Then $\exists$ a K-isomorphism $K(\alpha) \xrightarrow{\cong} K(\beta)$ with $\alpha \mapsto \beta$.

Proof.

$$\begin{array}{ccccc} K(\alpha) & \xleftarrow{\cong} & K[x]/(f) & \xrightarrow{\cong} & K(\beta) \\ \alpha & \leftarrow\!\shortmid & x & \mapsto & \beta \end{array}$$

□

Corollary 5.4.6. L/K with $f \in K[x]$ irreducible and $\alpha \in L$ a root of f. Then

$$\begin{aligned} \mathrm{Emb}_K(K(\alpha), L) &\to \{\beta \in L : f(\beta) = 0\} \\ \varphi &\mapsto \varphi(\alpha) \end{aligned}$$

is a bijection. In particular, $|\mathrm{Emb}_K(K(\alpha), L)| =$ number of roots of f in L.

Proof. Big idea 5.4.4 says it's well defined. Any K-homomorphism $\varphi : K(\alpha) \to L$ is determined by $\varphi(\alpha)$, so it's injective. Proposition 5.4.5 says if $\beta \in L$ is a root of f then there is a K-isomorphism $K(\alpha) \to K(\beta) \subset L$, so it's surjective. □

Week 5, lecture 1 starts here

Theorem 5.4.7. Let L/K be finite and M/K any extension. Then

$$|\mathrm{Emb}_K(L, M)| \le [L : K].$$

Proof. If $L = K(\alpha)$ is a simple extension with minimal polynomial f of α. Then

$$[L : K] = \deg f \ge \#\text{roots of } f \text{ in } M = |\mathrm{Emb}_K(L, M)|.$$

If not, do induction on $[L:K]$. Pick $\alpha \in L\backslash K$ and consider $L \subsetneqq K(\alpha) \subset L$ and the map of sets

$$\begin{aligned} \rho : \mathrm{Emb}_K(L, M) &\to \mathrm{Emb}_K(K(\alpha), M) \\ \varphi &\mapsto \varphi|_{K(\alpha)} \end{aligned}$$

For any $\varphi \in \mathrm{Emb}_K(K(\alpha), M)$,

$$\rho^{-1}(\varphi) = \{\tilde{\varphi} : L \to M : \tilde{\varphi}|_{K(\alpha)} = \varphi\}.$$

If $\tilde{\varphi} \in \rho^{-1}(\varphi)$ then it can be considered as a $K(\alpha)$-homomorphism where $M/K(\alpha)$ is given by $\varphi : K(\alpha) \to M$, i.e. $\tilde{\varphi} \in \mathrm{Emb}_{K(\alpha)}(L, M)$. Since $[L : K(\alpha)] < [L : K]$ by tower law, by inductive hypothesis we have

$$|\rho^{-1}(\varphi)| \leq [L : K(\alpha)].$$

Hence

$$\begin{aligned} |\mathrm{Emb}_K(L, M)| &\leq \max\{|\rho^{-1}(\varphi)| : \varphi \in \mathrm{Emb}_K(K(\alpha), M)\} \cdot |\mathrm{Emb}_K(K(\alpha), M)| \\ &\leq [L : K(\alpha)] \cdot [K(\alpha) : K] \\ &= [L : K]. \end{aligned}$$

□

6 Automorphism group of a field

Definition 6.0.1. An *automorphism* of a field L is a bijective ring homomorphism $L \to L$. The set of all of them, denoted $\mathrm{Aut}(L)$, is a group.
If $K < L$ is a subfield, then a K*-automorphism* is $\varphi : L \to L$ such that $\varphi(\alpha) = \alpha \ \forall \alpha \in K$. Again

$$\mathrm{Aut}_K(L) := \{K\text{-automorphism } \varphi : L \to L\}$$

is a group and is a subgroup of $\mathrm{Aut}(L)$.

6.1 Fixed field

Definition 6.1.1. Let L be a field and $\sigma \in \mathrm{Aut}(L)$. The *fixed field* of σ is

$$L^\sigma = \{\alpha \in L : \sigma(\alpha) = \alpha\}.$$

(If $\Sigma \subset \mathrm{Aut}(L)$, define $L^\Sigma = \{\alpha \in L : \sigma(\alpha) = \alpha \ \forall \sigma \in \Sigma\}$).

Example 6.1.2. Let σ be complex conjugating of $\mathbb{C}$. Then

$$\mathbb{C}^\sigma = \{z \in \mathbb{C} : \overline{z} = z\} = \mathbb{R}.$$

Note that $[\mathbb{C} : \mathbb{R}] = 2$ and $|\langle\sigma\rangle| = 2$.
Now let $L = \mathbb{Q}(\alpha, i)$ where $\alpha^2 = 5, \ i^2 = -1$. Then $[L : \mathbb{Q}] = 4$ with $\mathbb{Q}$-basis $\{1, \alpha, i, i\alpha\}$. For the same σ (this is indeed an automorphism since it's injective and $\dim L = \dim L$),

$$L^\sigma = \{a + b\alpha + ci + di\alpha : a + b\alpha - ci - di\alpha = a + b\alpha + ci + di\alpha\} = \langle 1, \alpha\rangle = \mathbb{Q}(\alpha).$$

Note again $[L : \mathbb{Q}(\alpha)] = |\langle\sigma\rangle| = 2$.

Lemma 6.1.3. Let $G \leq \mathrm{Aut}(L)$ be a finite subgroup. Then $[L : L^G] \leq |G|$.

Proof. Let $G = \{\sigma_1, \dots, \sigma_n\}$ and WLOG $\sigma_1 = \mathrm{id}$. Suppose $a_1, \dots, a_{n+1} \in L$ and set $K = L^G$. It suffices to prove to find a nontrivial linear dependence relation among the a_i's. Consider

$$v_i = \begin{pmatrix} \sigma_1(a_i) \\ \vdots \\ \sigma_n(a_i) \end{pmatrix} \in L^n \text{ for } i = 1, \dots, n+1.$$

So we have $v_1, \dots, v_{n+1} \in L^n$. Clearly $\dim_L L^n = n$, so $\exists$ a dependence relation $\sum x_i v_i = 0$ and not all $x_i = 0$.

Week 5, lecture 2 starts here

Choose a shortest such relation and after relabelling,

$$x_1 v_1 + x_2 v_2 + \cdots + x_k v_k = 0 \text{ where } x_i \neq 0,\ k \text{ minimal}.$$

Since we are in a field, WLOG $x_1 = 1$, i.e.

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_k \\ \sigma_2(a_1) & \sigma_2(a_2) & \cdots & \sigma_2(a_k) \\ \vdots & & & \\ \sigma_n(a_1) & & \cdots & \sigma_n(a_k) \end{pmatrix} \begin{pmatrix} x_1 = 1 \\ x_2 \\ \vdots \\ x_k \end{pmatrix} = \begin{pmatrix} 0 \\ \\ \vdots \\ 0. \end{pmatrix}$$

Apply any $\sigma \in G$ to the equations, then $\begin{pmatrix} \sigma(x_1) \\ \vdots \\ \sigma(x_n) \end{pmatrix}$ is still a solution. But they have to be the same, since if not their difference would be another solution that's smaller the minimal one, a contradiction. So $\sigma(x_i) = x_i\ \forall i$. ☐

Example 6.1.4. $f = x^3 - 2 \in \mathbb{Q}[x]$. Then $\alpha_1 = \alpha = \sqrt[3]{2},\ \alpha_2 = \alpha\omega,\ \alpha_3 = \alpha\omega^2 \in \mathbb{C}$ are the roots. The splitting field is then $L = \mathbb{Q}(\alpha, \omega)$. Let $K_i = \mathbb{Q}(\alpha_i)$, a simple extension. Note that L/K_1 is also simple. Clearly $[K_1 : \mathbb{Q}] = 3$. We also have $[L : K_1] = 2$ since one can write $f = (x - \alpha)(x^2 + \alpha x + \alpha^2)$ and the second factor must be irreducible, so it's the minimal polynomial. Hence by tower law we have $[L : \mathbb{Q}] = 6$, and naturally we have the basis $\{1, \alpha, \alpha^2, \alpha\omega, \alpha^2\omega, 2\omega\}$. We can write a better basis though: $\{1, \alpha, \alpha^2, \omega, \alpha\omega, \alpha^2\omega\}$. The tower structure is the same for K_2 and K_3 as well, i.e. $[K_i : \mathbb{Q}] = 3,\ [L : K_i] = 2\ \forall i$.

Now note that if $\varphi \in \mathrm{Emb}_{\mathbb{Q}}(L, L)$ then $\varphi(\alpha_i) \in \{\alpha_i\}$. So $\exists$ a injective group homomorphism

$$\begin{aligned} \mathrm{Emb}_{\mathbb{Q}}(L, L) &\hookrightarrow S_3 \\ \varphi &\mapsto \{i \mapsto j \text{ where } \varphi(\alpha_i) = \alpha_j\}. \end{aligned}$$

e.g., σ = complex conjugation $\in \mathrm{Emb}_{\mathbb{Q}}(L, L)$ has $\sigma(\alpha_1) = \alpha_1,\ \sigma(\alpha_2) = \alpha_3$ and $\sigma(\alpha_3) = \alpha_2$, i.e. σ corresponds to $(2, 3)$. In fact $\mathrm{Emb}_{\mathbb{Q}}(L, L) \cong S_3$ (one can hit arbitrary permutation in S_3 indirectly by 5.4.6). Let τ be corresponded to $(1, 2, 3)$.

Now $\mathrm{Aut}(L) = S_3$ has 6 elements, so $[L : L^{\mathrm{Aut}(L)}] = 6$, so $L^{\mathrm{Aut}(L)}$ must be $\mathbb{Q}$. Similarly, $L^{\langle\sigma\rangle} = K_1$ and $L^{\langle\tau\rangle} = \mathbb{Q}(\omega)$. In fact, every subfield of L is a fixed field of a subgroup of S_3.

Week 5, lecture 3 starts here

Corollary 6.1.5. $G \subset \mathrm{Aut}(L)$ is finite, then $[L : L^G] = |G|$.

Proof. Let $K = L^G,\ M = L$, then

$$[L : K] \le |G| \le |\mathrm{Aut}_K(L)| = |\mathrm{Emb}_K(L, L)| \le [L : K]$$

so it's all equal signs. □

Definition 6.1.6. The *splitting field* for $f \in K[x]$ is the field extension L/K such that $\exists \alpha_1, \dots, \alpha_n \in L : f = c(x - \alpha_1) \cdots (x - \alpha_n),\ c \in K$ and $L = K(\alpha_1, \dots, \alpha_n)$.

Remark.

1. Consider $f = x^3 - x^2 - 2x + 2 = (x - 1)(x^2 - 2) \in \mathbb{Q}[x]$. Then splitting field is $\mathbb{Q}\left(1, \sqrt{2}, -\sqrt{2}\right) = \mathbb{Q}\left(\sqrt{2}\right)$.
2. Same f but $f \in \mathbb{Q}\left(\sqrt{3}\right)[x]$. Then $\mathbb{Q}(\sqrt{2})$ is no longer splitting field, which now should be $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$.
3. If $K \subset \mathbb{C}$ is a subfield and f has roots α_i, then splitting field is always $K(\alpha_i)$.

Proposition 6.1.7 (Splitting fields exist)**.** $f \in K[x]$ with $\deg f = n$. Then $\exists$ splitting field L/K with $[L : K] \le n!$.

Proof. Factorise f in $K[x]$ and let $k = \#$ linear factors. If $k = n$ then f already splits, so done. Else, choose an irreducible factor $g_1 \in K[x]$ and let $L_1 = K[x]/(g_1)$ and α_1 is a root of g_1 in L_1. Now let $k_1 = \#$ linear factors of f in $L_1[x]$. Note that $k < k_1 \le n$ since $(x - \alpha_1)$ is now one of them.

We proceed inductively and get $K \subset L_1 \subset L_2 \subset \cdots L_s := L$ where f splits completely in L. By tower law,

$$\begin{aligned}[L : K] &= [L : L_1][L_1 : K] = [L : L_{s-1}][L_{s-1} : L_{s-2}] \cdots [L_2 : L_1][L_1 : K] \\ &\le 2 \cdot 3 \cdots (n-1)n = n!.\end{aligned}$$

□

Theorem 6.1.8. L/K splitting field for $f \in K[x]$. If $M/K : f$ splits in M then $\exists K$-homomorphism $L \to M$.

Proof. We know $L = K(\alpha_1, \dots, \alpha_s)$ where α_i are (some of) the roots of f. Do induction on s. Let $m \in K[x]$ be minimal polynomial of α_1. Note that $m \mid f$, so m splits in M, i.e. all its roots are in M. Choose $\beta_1 \in M$ be one of them. Then $\exists K$-homomorphism $L \supset K(\alpha_1) \xrightarrow{\cong} K(\beta_1) \subset M$. For notation, set $L_1 = K(\alpha_1)$. Then $L = L_1(\alpha_2, \dots, \alpha_s)$ is a splitting field for $g = \frac{f}{(x - \alpha_1)} \in L_1[x]$. By induction, $\exists L_1$-homomorphism $L \to M$. □

Corollary 6.1.9 (A splitting field is unique up to isomorphism)**.** If $L/K, L'/K$ are both splitting fields for $f \in K[x]$, then $\exists K$-isomorphism $L \to L'$.

Proof. We know $\exists K$-homomorphism $L \to L'$ and $\exists K$-homomorphism $L' \to L$. They are both injective, so $\dim_K L \le \dim_K L' \le \dim_K L$, so by linear algebra (and since dimensions are finite) they are surjective, so bijective. □

Theorem 6.1.10. L/K splitting field for $f \in K[x]$ and $g \in K[x]$ be irreducible with ≥ 1 roots in L. Then g splits completely in $L[x]$, i.e. all its roots are in L.

Proof. Regard $g \in L[x]$ and let M/L be splitting field of g. Suppose $\alpha \in M$ is a root of g. Then $L(\alpha)$ is a splitting field for $f \in K(\alpha)[x]$. Tower law says

$$[L(\alpha) : L][L : K] = [L(\alpha) : K(\alpha)][K(\alpha) : K].$$

If $\beta \in M$ is another root of g then the same is true for β and $K(\alpha) \cong K(\beta)$. But note that then $L(\beta)$ is also a splitting field for $f \in K(\alpha)[x]$, so $L(\alpha) \cong L(\beta)$. Hence if $\alpha \in L$ is a root, $[L(\alpha) : L] = 1$, so $[L(\beta) : L] = 1$ for all other roots β, so $L(\beta) = L$, so $\beta \in L$.

$$\begin{tikzcd}
K(\alpha) \arrow[r, hook] & L(\alpha) \arrow[dr, hook] & \\
K \arrow[u, hook] \arrow[r, hook] & L \arrow[u, hook] \arrow[r, hook] & M
\end{tikzcd}$$

□

Week 6, lecture 1 starts here

6.2 Normal extension

Definition 6.2.1. A field extension is L/K is *normal* if the following holds: a irreducible $g \in K[x]$ has roots in $L \Rightarrow g$ splits completely in L.

Corollary 6.2.2. If L/K is finite then the following are equivalent:

1. L/K is normal
2. L/K is a splitting field of some $f \in K[x]$

Proof. $2 \Rightarrow 1$ is Theorem 6.1.10.

For $1 \Rightarrow 2$, write $L = K(\alpha_1, \ldots, \alpha_n)$. Let m_i be minimal polynomial of α_i over K. Since $m_i(\alpha_i) = 0$, they all split completely in L. Now let $f = m_1 m_2 \cdots m_n$ which also split completely in L. Then L/K is a splitting field of f over K. □

Corollary 6.2.3. If L/K is finite then $\exists N/L$ normal (called the *normal closure*) (and therefore N/K is normal).

Proof. Write $L = K(\alpha_1, \ldots, \alpha_n)$. Let m_i be minimal polynomial of α_i over K. Let N be splitting field for $f = m_1 m_2 \cdots m_n \in L[x]$. □

Corollary 6.2.4. Let L/K be finite and normal and $K \subset M \subset L$. If $\xi : M \to L$ is a K-homomorphism, then $\exists \varphi : L \to L$ such that $\varphi|_M = \xi$.

Proof. Suppose L is splitting field for $f \in K[x]$. Since ξ fixes K, $\xi(f) = f$, so L/M is a splitting field for f and $K/\xi(M)$ is a splitting field for $\xi(f)$. Hence by uniqueness of splitting field we have the isomorphism. □

Corollary 6.2.5. If L/K is finite and normal and irreducible $f \in K[x]$ has roots $\alpha, \beta \in L$, then $\exists \varphi \in \mathrm{Aut}_K(L)$ such that $\varphi(\alpha) = \beta$.

Proposition 6.2.6. Let L/K be finite and normal. If M/L is finite then

1. If $\varphi : L \to M$ is a K-homomorphism then $\varphi(L) = L$ (N.B. this is not saying $\varphi(l) = l \, \forall l \in L$).
2. If $\tau \in \mathrm{Aut}_K(M)$ then $\tau(L) = L$.

6.3 Separable

Definition 6.3.1. $f \in K[x]\backslash\{0\}$ is *separable* over K if it has $n = \deg f$ distinct roots in a splitting field. Otherwise it is *inseparable*.

Remark (Handwavy teaser)**.** Suppose $K \subset \mathbb{C}$, $f \in K[x]$ and $n = \deg f \geq 2$. We know over $\mathbb{C}$, $f = c\prod_{i=1}^{s}(x-\alpha_i)^{m_i}$. We claim if f is irreducible over K then all $m_i = 1$ and $s = n$ and f is separable over K. Consider $f' = \frac{df}{dx}$ with $\deg f' < \deg f$. So $\gcd(f, f') = 1$. Write $f = (x-\alpha_1)^{m_1}g$ But now

$$f' = m_1(x-\alpha_1)^{m_1-1}g + (x_{-}\alpha_1)^{m_1}g'$$

so if WLOG $m_1 \geq 2$, $(x-\alpha_1) \mid f'$ so $(x-\alpha_1) \mid \gcd(f, f')$, a contradiction.

Week 6, lecture 2 starts here

Example 6.3.2.
1. $x^3 - 2 = x^3 + 1 = (x+1)^3 \in \mathbb{F}_3[x]$ is inseparable since it only has 1 distinct root.
2. $f = x^p - t \in K[x]$ where $p > 2$ and $K = \mathbb{F}_p(t)$. This is irreducible. If α is a root, write $L = K(\alpha)$ then $(x-\alpha)^p = x^p - \alpha^p = x^p - t$. So this is inseparable, but $f' = px^{p-1} - t = 0$ so it doesn't contradict previous remark.

Definition 6.3.3.
1. α is *separable* if minimal polynomial of α is separable.
2. L/K is separable if every $\alpha \in L$ is separable.

Definition 6.3.4. The *formal derivative* of $f \in K[x]$ is

$$Df := a_1 + 2a_2x + \cdots + na_nx^{n-1}$$

Theorem 6.3.5. If $f \in K[x]$ is irreducible then f is inseparable iff char $K = p$ and $f = a_0 + a_1x^p + \cdots + a_nx^{pn}$.

Lemma 6.3.6. $f \in K[x]\backslash\{0\}$ is separable over K iff $\gcd(f, Df) = 1$, i.e. f is inseparable iff $\gcd(f, Df) \neq 1$.

Proof. Let L/K be splitting field of f. If $f = c\prod_{i=1}^{n}(x-\alpha_i)$ where $c \in K$, $\alpha_i \in L$, $n = \deg f$ is separable, then α_i are distinct and

$$Df = c\sum_{j=1}^{n}\prod_{k\neq j}(x-\alpha_k),$$

and observe that $x - \alpha_i$ cannot be a common factor.
Now suppose f is inseparable then write $f = (x-\alpha)^m g$ where α is a repeated root (i.e. $m \geq 2$). Then

$$Df = m(x-\alpha)^{m-1}g + (x-\alpha)^m Dg$$

so $(x-\alpha)$ is a common factor, so $\gcd(f, Df) \neq 1$ in $L[x]$. But then it must be that $\gcd(f, Df) \neq 1$ in $K[x]$. $\square$

Theorem 6.3.7. If $L = K(\alpha_1, \ldots, \alpha_n)$ then L/K is separable if α_i are all separable.

7 Galois theory

Definition 7.0.1. The *Galois group* of L/K is $\mathrm{Gal}(L/K) := \mathrm{Aut}_K(L)$.

If $f \in K[x]$ is separable, let L/K be a splitting field of f over K. Then the *Galois group* of f is $\mathrm{Gal}(f) := \mathrm{Gal}(L/K)$ (defined up to isomorphism).

e.g. $f = x^3 - 2$ then $\mathrm{Gal}(f) \cong S_3$.

Definition 7.0.2. $H \subset S_n$ is *transitive* if $\forall i, j \in \{1, \ldots, n\},\ \exists \sigma \in H : \sigma(i) = j$.

Example 7.0.3. $H_1 = \langle (1,2) \rangle = \{\mathrm{id}, (12)\}$ is not transitive.

$H_2 = \langle (123) \rangle = \{\mathrm{id}, (123), (132)\}$ is transitive.

Lemma 7.0.4. If $f \in K[x]$ is irreducible and $\deg f = n$, then $\mathrm{Gal}(f)$ is isomorphic to a transitive subgroup of S_n.

Week 6, lecture 3 starts here

7.1 Galois extension

Definition 7.1.1. An extension L/K is *Galois* if it's the splitting field of a separable polynomial, or equivalently it's finite, normal and separable.

Lemma 7.1.2. If $K \subset M \subset L$ and L/K is Galois, then L/M is Galois.

Remark. M/K is not necessarily Galois, e.g. $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(\sqrt[3]{2}, \omega)$.

Theorem 7.1.3. L/K Galois, then $[L : K] = |\mathrm{Gal}(L/K)|$.

Proof. We prove by induction on $n = [L : K]$. Indeed when $n = 1$, $L = K$ and $\mathrm{Gal}(L/K) = \{\mathrm{id}\}$. Now suppose $n > 1$ and let L/K be the splitting field of a separable $f \in K[x]$. So $d = \deg f > 1$ and pick $\alpha \in L \backslash K$ a root of f and let m be minimal polynomial of α over K (so m is a irreducible factor of f in $K[x]$).

Now $[L : K(\alpha)] < [L : K]$ since $[K(\alpha) : K] > 1$, and by previous lemma, $L/K(\alpha)$ is Galois, so by inductive hypothesis $[L : K(\alpha)] = |\mathrm{Gal}(L/K(\alpha))|$.

f is separable implies m is separable, so now

$$[K(\alpha) : K] = \deg m = \#\text{roots of } m = |\mathrm{Emb}_K(K(\alpha), L)|.$$

Consider restriction $\mathrm{res}_\alpha : \mathrm{Gal}(L/K) \to \mathrm{Emb}_K(K(\alpha), L)$ by $\sigma \mapsto \sigma|_{K(\alpha)}$. This is surjective: by Corollary 6.2.4 given $\iota : K(\alpha) \to L$, $\exists : \sigma \in \mathrm{Gal}(L/K) : \sigma|_{K(\alpha)} = \iota$. Suppose $\tau \in \mathrm{Gal}(L/K) : \mathrm{res}_\alpha(\tau) = \iota$. Then $\tau^{-1}\sigma = \mathrm{id}$ on $K(\alpha)$, i.e. $\tau^{-1}\sigma \in \mathrm{Gal}(L/K(\alpha))$. Now we can consider $\mathrm{Gal}(L/K(\alpha))$ as a subgroup of $\mathrm{Gal}(L/K)$, then τ, σ are in the same left coset and one has

$$\frac{|\mathrm{Gal}(L/K)|}{|\mathrm{Gal}(L/K(\alpha))|} = |\mathrm{Emb}_K(K(\alpha), L)|.$$

So finally

$$\begin{aligned} |\mathrm{Gal}(L/K)| &= |\mathrm{Gal}(L/K(\alpha))| \times |\mathrm{Emb}_K(K(\alpha), L)| \\ &= [L : K(\alpha)] \times [K(\alpha) : K] \\ &= [L : K]. \end{aligned}$$

□

Corollary 7.1.4. L/K Galois, then

$$L^{\mathrm{Gal}(L/K)} = K.$$

Proof. One has

$$K \subset L^{\mathrm{Gal}(L/K)} \subset L$$

and by Corollary 6.1.5

$$|\mathrm{Gal}(L/K)| = \left[L : L^{\mathrm{Gal}(L/K)}\right]$$

so by tower law $\left[L^{\mathrm{Gal}(L/K)} : K\right] = 1$ and thus desired. $\square$

Proposition 7.1.5. L/K Galois, $K \subset M \subset L$. Then M/K is normal iff $\mathrm{Gal}(L/M) \leq \mathrm{Gal}(L/K)$ is normal.

Proof. Let $G = \mathrm{Gal}(L/K)$ and $H = \mathrm{Gal}(L/M)$. M/K is normal implies $\sigma(M) = M$ $\forall \sigma \in G$ by Proposition 6.2.6. Suppose $h \in H$ and $\sigma \in G$. We want to show $\sigma h \sigma^{-1} \in H$. Let $\alpha \in M$ and set $\beta := \sigma^{-1}(\alpha) \in M$. Then

$$\sigma h \sigma^{-1}(\alpha) = \sigma h(\beta) = \sigma(\beta) = \alpha.$$

Now suppose $H \trianglelefteq G$. Let $\alpha \in M$ with minimal polynomial $g \in K[x]$. We want to prove g splits completely in M. Let $\beta \in L$ be any other root, then by Corollary 6.2.5 $\exists : \sigma \in G : \sigma(\alpha) = \beta$. If $h \in H$ then $h(\alpha) = \alpha \in M$. So

$$\sigma h \sigma^{-1}(\beta) = \sigma h(\alpha) = \sigma(\alpha) = \beta,$$

and since all elements of H are of the form $\sigma h \sigma^{-1}$, $\beta \in L^H$. But $L^H = M$ since L/M is Galois, so $\beta \in M$. $\square$

Week 7, lecture 1 starts here

7.2 Lattice map

Definition 7.2.1. A *lattice* is a collection of vertices (usually labelled) joined by directed lines (usually indicating relations between vertices).
Given L/K finite, the *subfield lattice* of L/K is $\mathcal{F}_{L/K} := \{M \subset L : M \text{ a subfield, } M/K \text{ an extension}\}$, a partially ordered set by inclusion, simply denoted $\mathcal{F}$ when context is clear.
Given G a finite group, the *subgroup lattice* of G is $\mathcal{G}_G =: \{H \subset G : H \text{ a subgroup}\}$, partially ordered by inclusion.

Note that $\mathrm{Gal}(L/K)$ acts on $\mathcal{F}$ by the natural way and G acts in $\mathcal{G}$ by conjugation. Normal extensions get mapped to themselves by Proposition 6.2.6, normal subgroups get mapped to themselves by group theory.

Definition 7.2.2. Define two order reserving maps between lattices $\dagger : \mathcal{G}_G \to \mathcal{F}_{L/K}$ by $H \mapsto H^\dagger := L^H$ and $* : \mathcal{F}_{L/K} \to \mathcal{G}_G$ by $M \mapsto M^* := \mathrm{stab}_G(M)$.

Lemma 7.2.3 (Polarity).

1. $H_1 \subset H_2 \subset G \Rightarrow H_2^\dagger \subset H_1^\dagger$.
2. $K \subset M_1 \subset M_2 \subset L \Rightarrow M_2^* \subset M_1^*$.

3. $H \leq G \Rightarrow H \subset \left(H^\dagger\right)^*$.

4. $K \subset M \subset L \Rightarrow M \subset (M^*)^\dagger$.

Proof. 3. $h \in H \Rightarrow h \in \mathrm{Gal}(L/H^*) \Rightarrow h \in \left(H^\dagger\right)^*$.

4. Similar.

□

7.3 Galois correspondence

Theorem 7.3.1 (Galois correspondence)**.** Let L/K be Galois, $\mathcal{F} = \mathcal{F}_{L/K}$, $G = \mathrm{Gal}(L/K)$ and $\mathcal{G} = \mathcal{G}_G$. Then

1. $*, \dagger$ are mutually inverse bijection, giving inclusion reserving bijection $\mathcal{F} \leftrightarrow \mathcal{G}$.

2. If $K \subset M \subset L$ then $[L : M] = |M^*|$ and therefore $[M : K] = \frac{|\mathrm{Gal}(L/K)|}{|M^*|}$.

3. M/K is normal iff $M^* \trianglelefteq \mathrm{Gal}(L/K)$. In this case, $\mathrm{Gal}(M/K) \cong \mathrm{Gal}(L/K)/M^*$.

Proof. 1. Let $M \in \mathcal{F}$. Note L/M is Galois by Lemma 7.1.2, so by Corollary 6.1.5 and Theorem 7.1.3,

$$\left[L : (M^*)^\dagger\right] = |M^*| = [L : M].$$

Since $M \subset (M^*)^\dagger$, one has $M = (M^*)^\dagger$, i.e. $\dagger \circ *$ is identity.

Now let $H \subset \mathcal{G}$. Then

$$|H| = \left[L : H^\dagger\right] = \left|\mathrm{Gal}\left(L/H^\dagger\right)\right| = \left|\left(H^\dagger\right)^*\right|.$$

Since $H \subset \left(H^\dagger\right)^*$, one has $H = \left(H^\dagger\right)^*$.

2. By 7.1.3 and tower law.

3. By Proposition 7.1.5. Isomorphism by 1st isomorphism theorem and considering the map $\mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K) : \sigma \mapsto \sigma|_M$.

□

Week 7, lecture 2 starts here

7.4 Biquadratic extension

Let K be a field with $\mathrm{char}\, K \neq 2$, $a, b \in K : b(a^2 - b) \neq 0$ where b is not a square in K. Consider $f = (x^2 - a)^2 - b = x^4 - 2ax^2 + (a^2 - b)$. Let L/K be a splitting field of f. Such extensions are called *biquadratic.*

1. Consider $\beta : \beta^2 = b$. Then $x^2 - a = \pm\beta$. Set $\alpha : \alpha^2 = a + \beta$ and $\alpha' : \alpha'^2 = a - \beta$, so f has 4 distinct roots $\pm\alpha, \pm\alpha'$, i.e. f is separable and $L = K(\alpha, \alpha')$.

2. Now one has

$$[L:K] = [L:K(\alpha)][K(\alpha):K(\beta)][K(\beta):K] \leq 2 \times 2 \times 2 = 8,$$

so it's 2 or 4 or 8.

3.

Lemma 7.4.1. (a) $a^2 - b$ not a square in $K \Rightarrow [K(\alpha):K] = [K(\alpha'):K] = 4$.
(b) If also $b(a^2-b)$ not a square in K then $[L:K] = 8$.

Proof. (a) We show $[K(\alpha):K(\beta)] = 2$. Suppose $\alpha \in K(\beta)$, i.e. $a+\beta$ is a square in $K(\beta)$, then

$$a+\beta = (c+d\beta)^2 = (c^2+d^2b) + 2cd\beta, \; a-\beta = (c^2+d^2b) - 2cd\beta = (c-d\beta)^2,$$

so

$$a^2 - b = \left(c^2 - d^2b\right)^2,$$

so $a^2 - b$ is a square, a contradiction.

(b) Similar.

□

4.

Lemma 7.4.2. Now suppose $[K(\alpha):K] = [K(\alpha'):K] = 4$. Then

(a) $q = x^2 - (a+\beta)$, $q' = x^2 - (a-\beta)$ are the minimal polynomials of α, α' over $K(\beta)$.

(b) If $\sigma \in \mathrm{Gal}(L/K)$ then the only 8 possibilities are:

$$\begin{array}{lccccccccc}
 & & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\
\sigma(\beta) & & \beta & \beta & \beta & \beta & -\beta & -\beta & -\beta & -\beta \\
\sigma(\alpha) & = & \alpha & \alpha & -\alpha & -\alpha & \alpha' & \alpha' & -\alpha' & -\alpha' \\
\sigma(\alpha') & & -\alpha' & \alpha' & \alpha' & -\alpha' & \alpha & -\alpha & \alpha & -\alpha
\end{array}$$

i.e. $\mathrm{Gal}(L/K)$ is a subgroup of a group of order 8.

5. If $[L:K] = 2^3 = 8$, then $|\mathrm{Gal}(L/K)| = [L:K] = 8$ so it has to be the whole thing above, which is $D_8 \leq S_4$: indeed, let σ be #6 above and τ be #1 above.

6. Subgroup lattice of D_8:

$$\begin{tikzcd}
 & & \{\mathrm{id}\} \arrow[dll, no head] \arrow[dl, no head] \arrow[d, no head] \arrow[dr, no head] \arrow[drr, no head] & & \\
\langle\tau\rangle \arrow[dr, no head] & \langle\sigma^2\tau\rangle \arrow[d, no head] & \langle\sigma^2\rangle \arrow[dl, no head] \arrow[d, no head] \arrow[dr, no head] & \langle\sigma^3\tau\rangle \arrow[d, no head] & \langle\sigma\tau\rangle \arrow[dl, no head] \\
 & \langle\sigma^2,\tau\rangle \arrow[dr, no head] & \langle\sigma\rangle \arrow[d, no head] & \langle\sigma^2,\sigma\tau\rangle \arrow[dl, no head] & \\
 & & D_8 & &
\end{tikzcd}$$

7. Subfield lattice by Galois correspondence:

$$\begin{tikzcd}
 & & L \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
L^{\tau} \arrow[dr, dash] & L^{\sigma^2\tau} \arrow[d, dash] & L^{\sigma^2} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & L^{\sigma^3\tau} \arrow[d, dash] & L^{\sigma\tau} \arrow[dl, dash] \\
 & L^{\langle\sigma^2,\tau\rangle} \arrow[dr, dash] & L^{\langle\sigma\rangle} \arrow[d, dash] & L^{\langle\sigma^2,\sigma\tau\rangle} \arrow[dl, dash] & \\
 & & L^{\langle\sigma,\tau\rangle} & &
\end{tikzcd}$$

Week 7, lecture 3 starts here

8. What actually are these fixed fields? Let $\gamma = \alpha\alpha'$, $\delta = \alpha + \alpha'$, $\delta' = \alpha - \alpha'$. By checking how α, α' and β are fixed by σ and τ and considering tower law, one has

$$\begin{tikzcd}
 & & L = K(\alpha,\alpha') \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
K(\alpha) \arrow[dr, dash] & K(\alpha') \arrow[d, dash] & K(\beta,\delta) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & K(\delta') \arrow[d, dash] & K(\delta) \arrow[dl, dash] \\
 & K(\beta) \arrow[dr, dash] & K(\beta\gamma) \arrow[d, dash] & K(\gamma) \arrow[dl, dash] & \\
 & & K & &
\end{tikzcd}$$

9.

Example 7.4.3. $K = \mathbb{Q}$.

(a) $a = 0,\ b = 2,\ a^2 - b = 2$ and $b(a^2 - b) = -4$ are not squares in $\mathbb{Q}$. Then $\mathrm{Gal}(f) \le D_8$ and note that $f = x^4 - 2$ has 4 distinct roots $\alpha = \sqrt{0 + \sqrt{2}} = \sqrt[4]{2}, -\alpha, \alpha' = i\alpha, -\alpha$. The β as above is $\sqrt{2}$. Then we have the subfield lattice

$$\begin{tikzcd}
 & & L = \mathbb{Q}(\alpha,i) \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
\mathbb{Q}(\alpha) \arrow[dr, dash] & \mathbb{Q}(i\alpha) \arrow[d, dash] & \mathbb{Q}(i\sqrt{2}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \mathbb{Q}((1-i)\alpha)) \arrow[d, dash] & \mathbb{Q}((1+i)\alpha) \arrow[dl, dash] \\
 & \mathbb{Q}(\sqrt{2}) \arrow[dr, dash] & \mathbb{Q}(i) \arrow[d, dash] & \mathbb{Q}(i\sqrt{2}) \arrow[dl, dash] & \\
 & & \mathbb{Q} & &
\end{tikzcd}$$

by above.

(b) $a = 1,\ b = 3,\ a^2 - b = -2$ and $b(a^2 - b) = -6$ are not squares in $\mathbb{Q}$. Then similarly f has 4 distinct roots $\pm\alpha = \pm\sqrt{1+\sqrt{3}}$ and $\pm\alpha' = \pm i\sqrt{\sqrt{3}-1}$.

10. Now suppose $\sqrt{b(a^2-b)} \in K$. Then observe that

$$(\beta\alpha\alpha')^2 = b(a+\beta)(a-\beta) = b(a^2-b),$$

so $\beta\alpha\alpha' \in K$, hence

$$\alpha' = \frac{\text{something in } K}{\beta\alpha} \in K(\alpha,\beta) = K(\alpha),$$

so $K(\alpha,\alpha') = K(\alpha)$ is a splitting field, and

$$[L : K] = [K(\alpha) : K(\beta)][K(\beta) : K] = 2 \times 2 = 4 = |\mathrm{Gal}(L/K)|.$$

11. We now observe that $f = (x^2 - a)^2 - b$ is then irreducible. Use a similar method you've seen before to verify (first suppose there is a root, then suppose split into quadratics). So by Lemma 7.0.4, $\mathrm{Gal}(f)$ is a transitive subgroup of D_8. In particular, $\exists \sigma \in \mathrm{Gal}(f) : \sigma(\alpha) = \alpha'$ and $\langle\sigma\rangle \leq \mathrm{Gal}(f)$. By the 8 possibilities we listed, $\sigma(\beta) = -\beta$, and since σ fixed K, one has

$$\sigma(\beta\alpha\alpha') = \sigma(\beta)\sigma(\alpha)\sigma(\alpha') = -\beta\alpha'\sigma(\alpha') = \beta\alpha\alpha',$$

so $\sigma(\alpha') = -\alpha$. Now by σ,

$$\begin{gathered} \alpha \mapsto \alpha' \mapsto -\alpha \mapsto -\alpha' \mapsto \alpha \\ \alpha' \mapsto -\alpha \mapsto -\alpha' \mapsto \alpha \mapsto \alpha' \end{gathered}$$

so $\sigma^4 = \mathrm{id}$ and $\{\mathrm{id}, \sigma, \sigma^2, \sigma^3\} \subset \mathrm{Gal}(f)$, and since $\mathrm{Gal}(f) = 4$, $\langle\sigma\rangle$ is in fact the whole $\mathrm{Gal}(f)$ and we have the subgroup-subfield lattice correspondence:

$$\begin{array}{ccc} \langle\sigma\rangle = C_4 & \qquad & L = K(\alpha) \\ | & & | \\ \langle\sigma^2\rangle = C_2 & & K(\beta) \\ | & & | \\ \{\mathrm{id}\} & & K \end{array}$$

Week 8, lecture 1 starts here

8 Finite field

Definition 8.0.1. A *finite field* is a field with finite elements.

Proposition 8.0.2. If K is a finite field then $\operatorname{char} K = p > 0$ and $|K| = p^n$ for some $n \in \mathbb{N}$.

Proof. Consider the unique homomorphism $\varphi : \mathbb{Z} \to K$. Since K is a field, in particular a domain, $\ker\varphi$ is a prime ideal, so is of the form $p\mathbb{Z}$. By 1st isomorphism theorem, $\mathbb{Z}/p\mathbb{Z} \cong \operatorname{im}\varphi \subset K$, so $\operatorname{char} K = p$. But now note that K is a finite dimensional $\mathbb{Z}/p\mathbb{Z}$-vector space, so $|K| = p^n$ where n is its dimension. $\square$

Theorem 8.0.3. Given prime p and $n \in \mathbb{N}$, set $q = p^n$, then splitting field L of $x^q - x \in \mathbb{F}_p[x]$ is a field with $|L| = q$. Moreover, $L/\mathbb{F}_p$ is Galois and any two fields with q elements are isomorphic.

Proof. Write $f = x^q - x$. Then $Df = qx^{q-1} - 1 = -1 \in \mathbb{F}_p[x]$, so f and Df are coprime, so f is separable by 6.3.6 and $L/\mathbb{F}_p$ is then by definition Galois.

Let $M \subset L$ be the set of roots of f, i.e. $M = \{\alpha \in L : \alpha^q = \alpha\}$. We claim M is a field. Indeed, if $\alpha, \beta \in M$ then $(\alpha\beta)^q = \alpha^q \beta^q = \alpha\beta$ so $\alpha\beta \in M$, and $(\alpha+\beta)^q = \alpha^q + \beta^q = \alpha + \beta$ so $\alpha + \beta \in M$. Since L is defined to be the smallest field that contains M, $M = L$, hence $|L| = |M| = q$.

Suppose $N/\mathbb{F}_p$ is another field with q elements. Consider $N^* = N\backslash\{0\}$, a group with $q-1$ elements. If $\beta \in N^*$ then $|\beta| \mid q-1$ and in particular $\beta^{q-1} = 1$, so $\forall \beta \in N$ one has $\beta^q = \beta$, i.e. every element of N is a root of f. This means N is a splitting field of $f \in \mathbb{F}_p$, and by 6.1.9 N is isomorphic to L. □

Notation. We've seen $\mathbb{F}_p$ quite many times before. Now that we have the theorem, we define $\mathbb{F}_{p^n}$ to be the unique field of size p^n (so not $\mathbb{Z}/p^n\mathbb{Z}$ which is generally not a field).

8.1 Frobenius map

Definition 8.1.1. Let K be a field (not necessarily finite) with $\operatorname{char} K = p > 0$. The *Frobenius map* is the homomorphism $\varphi_p : K \to K : \alpha \mapsto \alpha^p$.

Proposition 8.1.2. Write φ for φ_p in context above. Then

1. φ is indeed a homomorphism
2. $M := \{\alpha \in K : \varphi(\alpha) = \alpha\} = \mathbb{F}_p$
3. K is finite $\Rightarrow \varphi$ is surjective, so $\varphi \in \operatorname{Aut}_{\mathbb{F}_p}(K)$ and $K^\varphi = \mathbb{F}_p$.

Proof.

1. One has $(\alpha\beta)^p = \alpha^p\beta^p$, $1^p = 1$ and $(\alpha+\beta)^p = \alpha^p + \beta^p$.
2. M is a subfield, so $\mathbb{F}_p \subset M$ and in particular $|M| \geq p$. But $M = \{\text{roots of } x^p - x \in \mathbb{F}_p[x]\}$, so $|M| \leq p$, hence $|M| = p$ and $M = \mathbb{F}_p$.
3. φ is surjective by its injectivity (K is a field) and rank–nullity theorem. The rest follows from definition.

□

Example 8.1.3. $K = \mathbb{F}_3(t) = \left\{\frac{A}{B} : A, B \in \mathbb{F}_3[t],\ B \neq 0\right\}$. Then $\operatorname{char} K = 3$. This is not infinite, and note that φ is not surjective (you can't hit t).

Theorem 8.1.4 (Galois group)**.** Given a finite field K with $\operatorname{char} K = p > 0$ and $|K| = p^n$, one has $\operatorname{Gal}(K/\mathbb{F}_p) = \langle \varphi_p \rangle \cong \mathbb{Z}/n\mathbb{Z}$.

Week 8, lecture 2 starts here

Proof. Since $K/\mathbb{F}_p$ is Galois, by 7.1.3 one has $|\operatorname{Gal}(K/\mathbb{F}_p)| = [K : \mathbb{F}_p] = n$. It suffices to prove $|\varphi_p| = n$. Suppose $\varphi_p^m = \mathrm{id}$ for some $m \leq n$, i.e. $\alpha^{p^m} = \alpha\ \forall \alpha \in K$, i.e. α is a root of $g = x^{p^m} - x$. This means $p^n = |K| \leq p^m$, so $n \leq m$, so $m = n$. □

Remark. Note that any subgroup of $\mathrm{Gal}(K/\mathbb{F}_p)$ is then of the form $\langle \varphi_p^m \rangle$ where $m \mid n$ which has $\frac{n}{m}$ elements. By 6.1.5, $[L : L^H] = |H| = \frac{n}{m}$, so $|L^H| = p^m$ and hence $L^H \cong \mathbb{F}_{p^m}$. We can therefore draw the subgroup/subfield lattice quite easily.

Example 8.1.5. Let $p = 7$ and $n = 12$.
Subgroup lattice of $\mathrm{Gal}(L/\mathbb{F}_p) \cong C_{12}$:

$$\begin{tikzcd}
 & & \{\mathrm{id}\} = \langle \varphi^{12} \rangle \arrow[dl, dash] \arrow[dr, dash] & \\
 & \langle \varphi^6 \rangle \cong C_2 \arrow[dl, dash] \arrow[dr, dash] & & \langle \varphi^4 \rangle \cong C_3 \arrow[dl, dash] \\
\langle \varphi^3 \rangle \cong C_4 \arrow[dr, dash] & & \langle \varphi^2 \rangle \cong C_6 \arrow[dl, dash] & \\
 & \langle \varphi \rangle \cong C_{12} & &
\end{tikzcd}$$

so by Galois correspondence one has subfield lattice:

$$\begin{tikzcd}
 & & L = \mathbb{F}_{13841287201} \arrow[dl, dash] \arrow[dr, dash] & \\
 & L^{\langle \varphi^6 \rangle} = \mathbb{F}_{117649} \arrow[dl, dash] \arrow[dr, dash] & & L^{\langle \varphi^4 \rangle} = \mathbb{F}_{2401} \arrow[dl, dash] \\
L^{\langle \varphi^3 \rangle} = \mathbb{F}_{343} \arrow[dr, dash] & & L^{\langle \varphi^2 \rangle} = \mathbb{F}_{49} \arrow[dl, dash] & \\
 & L^{\langle \varphi \rangle} = \mathbb{F}_7 & &
\end{tikzcd}$$

which seems insane to derive from scratch but now almost comes for free.

Week 8, lecture 3 starts here

9 Radical solution of a polynomial

Recall section 3.2.

Definition 9.0.1. A field extension M/K is *radical* if $\exists$ a sequence of subfields $K = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_s = M$ with $F_i = F_{i-1}(\alpha_i)$ and $\alpha_i^{n_i} \in F_{i-1}$.

Example 9.0.2. Let $\omega^3 = 1,\ \omega \neq 1$. Then $\mathbb{Q}(\omega)/\mathbb{Q}$ is radical, since ω is a root of $x^3 - 1 \in \mathbb{Q}[x]$.

Example 9.0.3. $f = x^3 - 3x - 3 \in \mathbb{Q}[x]$ is Eisenstein at 3 so irreducible. The discriminant D is

$$q^2 + \frac{4p^3}{27} = 9 + \frac{4(-27)}{27} = 5.$$

Let $\alpha = \sqrt{5}$, $\beta = \sqrt[3]{\frac{-q+\alpha}{2}} = \sqrt[3]{\frac{3+\sqrt{5}}{2}}$ and $\gamma = \sqrt[3]{\frac{3-\sqrt{5}}{2}}$, subject to $\beta\gamma = -\frac{p}{3} = 1$. Choose $\beta, \gamma \in \mathbb{R}$ and one has $\gamma = \frac{1}{\beta}$. Roots of f are $\alpha_0 = \beta + \gamma$, $\alpha_1 = \omega\beta + \omega^2\gamma$, $\alpha_2 = \omega^2\beta + \omega\gamma = \overline{\alpha_1}$. Splitting field is $\mathbb{Q}(\alpha_0, \alpha_1, \alpha_2)$. Note that one has

$$\begin{aligned} F_0 = \mathbb{Q} \subset F_1 &= \mathbb{Q}(\sqrt{5}) \\ \subset F_2 &= \mathbb{Q}(\sqrt{5}, \beta) \\ \subset F_3 &= \mathbb{Q}(\beta, \omega) =: M, \end{aligned}$$

so $M/\mathbb{Q}$ is radical since

$$5 \in \mathbb{Q}, \quad \frac{3+\sqrt{5}}{2} \in \mathbb{Q}(\sqrt{5}), \quad 1 \in \mathbb{Q}(\sqrt{5}, \beta).$$

Now we know if $L/\mathbb{Q}$ is a splitting field then $[L : \mathbb{Q}] = 3$ or 6 and $L \subset M$. We claim that $[F_2 : F_1] = 3$, since

$$\begin{tikzcd}
F_3 \arrow[r, equal] \arrow[d, dash, "2"'] & M \arrow[d, dash] \arrow[ddd, dash, bend left, "\text{divisible by 3}"] \\
F_2 \arrow[d, dash, "\text{at most 3}"'] & L \arrow[dd, dash, "\text{3 or 6}"'] \\
F_1 \arrow[d, dash, "2"'] & \\
F_0 \arrow[r, equal] & \mathbb{Q}.
\end{tikzcd}$$

So in particular $[M : \mathbb{Q}] = 12$ hence $L \subsetneq M$. In fact, $\sqrt{5}, \beta, \gamma, \omega \notin L$.

Definition 9.0.4. L/K is *soluble* if $\exists M/K$ radical with $L \subset M$.

A polynomial $f \in K[x]$ is *soluble by radicals* if its splitting field L/K is soluble.

Proposition 9.0.5. Suppose $\operatorname{char} K = 0$ and L/K radical. Then $\exists$ a finite extension M/L : M/K is radical and Galois.

Compare this with 6.2.3.

Proof. Let M/L be normal closure. One has

$$K = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_s = L$$

with $F_i = F_{i-1}(\alpha_i)$ where α_i is a root of $x^{n_i} - b_i \in F_{i-1}[x]$. Let m_i be minimal polynomial of α_i over K.

Let $\widetilde{F_i} = F_{i-1}(\text{roots of } m_i) \subset M$ (so $\widetilde{F_1}/K$ is normal since it's a splitting field).

$b_1 \in K$ so it's fixed by $\mathrm{Gal}(M/K)$. m_1 is irreducible over K so if β_1 is another root, $\exists \sigma \in \mathrm{Gal}(M/K) : \sigma(\alpha_1) = \beta_1$, so β_1 is a root of $x^{n_1} - \sigma(b_1) = x^{n_1} - b_1$, hence β_1 is a radical, i.e. $\widetilde{F_1}/K$ is radical.

Now let β_2 be a another root of m_2. Then $\exists \sigma \in \mathrm{Gal}(M/K) : \sigma(\alpha_2) = \beta_2$, and α_2 is a root of $x^{n_2} - b_2 \in F_1[x] \subset \widetilde{F_1}[x]$; β_2 is a root of $x^{n_2} - \sigma(b_2) \in \widetilde{F_1}[x]$ since $\widetilde{F_1}/K$ is normal and so $b_2 \in \widetilde{F_1}$ by 6.2.6. Hence β_2 is a radical, i.e. $\widetilde{F_2}/K$ is radical.

The proof is finished by induction and definition of normal closure. $\square$

Week 9, lecture 1 starts here

Definition 9.0.6. A group G is *soluble* if $\exists$ a chain of subgroups

$$\{\mathrm{id}\} \subset G_0 \subset G_1 \subset \cdots \subset G_s = G$$

with each $G_i \subset G_{i+1}$ being normal subgroups (called a *subnormal series*) and G_{i+1}/G_i abelian $\forall i = 0, \ldots, s-1$.

Remark. When G is finite and soluble, there is a subnormal series with all quotients being cyclic of prime order since we know structure of finite abelian groups.

Definition 9.0.7. For $g, h \in G$, the *commutator* of g, h is $[g, h] = ghg^{-1}h^{-1}$.

Example 9.0.8. Abelian groups are soluble.

S_3, S_4 are soluble. S_5 is not, and in fact A_5 is already not since it's simple and nonabelian.

Every element of $A_5 = \{\mathrm{id}, (i,j,k), (i,j)(k,l), (i,j,k,l,m)\}$ is a commutatator. Indeed,

$$\begin{aligned}(i,j,k) &= [(i,k,l),(i,k,m)]\\ (i,j)(k,l) &= [(i,j,k),(i,j,l)]\\ (i,j,k,l,m) &= [(i,j)(k,m)(i,m,l)].\end{aligned}$$

Now suppose A_5 is soluble with H normal and A_5/H abelian and forget we know it's simple. Then $\exists$ a homomorphism $\pi : A_5 \twoheadrightarrow A_5/H$, but commutators are mapped to commutators by homomorphisms, and since A_5/H is abelian, it's trivial, i.e. $H = A_5$.

Proposition 9.0.9. Let G be a group and $H \subset G$ a subgroup.

1. G soluble $\Rightarrow$ H soluble.
2. If H is normal, then G soluble $\Leftrightarrow$ H and G/H soluble.

Example 9.0.10. $f = x^5 - 10x + 5$ is not soluble by radicals.

f is irreducible since it's Eisenstein at $p = 5$ (so it's separable). We claim it has 3 distinct real roots and a complex conjugate pair of roots. Note that $f' = 5x^4 - 10 = 5(x^4 - 2)$ has two real roots $\pm\sqrt[4]{2}$ (and two imaginary roots $\pm i\sqrt[4]{2}$), and that $f(-\sqrt[4]{2}) > 0$, $f(\sqrt[4]{2}) < 0$, so by IVT and MVT we have three real roots. We have the complex conjugates since $f \in \mathbb{Q}[x]$. Name them $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{R}$, $\beta, \overline{\beta} \in \mathbb{C}\backslash\mathbb{R}$ and one has splitting field $L = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \beta, \overline{\beta})$.

Complex conjugation $\sigma(z) = \overline{z}$ is an automorphism of L, so $\sigma \in \mathrm{Gal}(L/\mathbb{Q}) = \mathrm{Gal}(f)$, which corresponds to $(4,5) \in S_5$.

Now by tower law and Galois correspondence, 5 divides $\mathrm{Gal}(L/\mathbb{Q})$, which divides $120 = |S_5|$ by Lagrange's and Lemma 7.0.4. So $5^2 \nmid \mathrm{Gal}(L/\mathbb{Q})$, and there is a 5 cycle in $\mathrm{Gal}(L/\mathbb{Q})$.

But S_5 is generated by $(4,5)$ and a 5-cycle, so $\mathrm{Gal}(L/\mathbb{Q}) \cong S_5$, a not soluble group.

Week 9, lecture 2 starts here

Lemma 9.0.11. $K \subset \mathbb{C}$, $\zeta \in \mathbb{C}$ a primitive pth root of 1 where p prime. Then $K(\zeta)/K$ is Galois and $\mathrm{Gal}(K(\zeta)/K)$ is abelian.

Proof. $K(\zeta)$ is a splitting field of the minimal polynomial of ζ, which is separable since it divides $x^p - 1$ which has p roots $1, \zeta, \zeta^2, \ldots, \zeta^{p-1}$. Hence $K(\zeta)/K$ is Galois.

If $\sigma, \tau \in \mathrm{Gal}(K(\zeta)/K)$ then we know $\sigma(\zeta) = \zeta^r$ and $\tau(\zeta) = \zeta^s$ for some $r, s \in \{1, \ldots, p-1\}$, so $\tau(\sigma(\zeta)) = \sigma(\tau(\zeta)) = \zeta^{rs}$. $\square$

Lemma 9.0.12. Suppose $\zeta \in K \subset \mathbb{C}$ where ζ is a primitive pth root of 1 where p prime. If $\alpha \in \mathbb{C}$ satisfies $\alpha^p = a \in K$ then $K(\alpha)/K$ is Galois and $\mathrm{Gal}(K(\alpha)/K)$ is abelian.

Proof. $K(\alpha)$ is a splitting field of $f = x^p - a \in K[x]$ where f is separable with roots $\alpha, \alpha\zeta, \alpha\zeta^2, \ldots, \alpha\zeta^{p-1}$, so $K(\alpha)/K$ is Galois.

Minimal polynomial m of α over K divides f so m splits in $K(\alpha)$ with roots of the form $\alpha\zeta^s$. Again elements of $\mathrm{Gal}(K(\alpha)/K)$ are determined by these roots, and if $\sigma(\alpha) = \alpha\zeta^s$ and $\tau(\alpha) = \alpha\zeta^r$ then $\sigma(\tau(\alpha)) = \sigma(\alpha\zeta^r) = \sigma(\alpha)\sigma(\zeta)^r = \alpha\zeta^s\zeta^r = \alpha\zeta^{r+s}$ and the result follows from the fact that $r + s = s + r$. $\square$

Corollary 9.0.13. $K \subset \mathbb{C}$, $\alpha \in \mathbb{C}$ satisfies $\alpha^p = a \in K$ where p prime. Let $L = K(\alpha, \zeta)$ and $M = K(\zeta)$. Then L/K is Galois and $\mathrm{Gal}(L/K)$ is soluble with $\{\mathrm{id}\} \subset \mathrm{Gal}(L/M) \subset \mathrm{Gal}(L/K)$ a soluble series.

Proof. $K(\alpha, \zeta)$ is a splitting field of $f = x^p - a$ which has roots $\alpha, \alpha\zeta, \ldots, \alpha\zeta^{p-1}$, so L/K is Galois. Also M/K is Galois by , so normal, so $\mathrm{Gal}(L/M) \lhd \mathrm{Gal}(L/K)$ with $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/M) \cong \mathrm{Gal}(M/K)$ by 7.3.1, which is abelian by . $\mathrm{Gal}(L/M)$ is abelian by 9.0.12. $\square$

Theorem 9.0.14. If L/K is radical Galois then $\mathrm{Gal}(L/K)$ is soluble.

Corollary 9.0.15. $K \subset \mathbb{C}$ and $f \in K[x]$ irreducible with splitting field L/K. If f is soluble in radicals then $\mathrm{Gal}(L/K)$ is soluble.

For proofs of the above two, see Gavin's notes.

Week 9, lecture 3, week 10, lectures 1 and 2 are cancelled

Week 10, lecture 3 is an overview