Math 370 - Notes

Leart Ajvazaj

January 2020

Lecture 1

Abstract Algebra Recap

Polynomials over $\mathbb{C}$.

Definition 1. Let $f \in \mathbb{C}[x]$ be the polynomial $f = a_n x^n + \cdots + a_1 x + a_0$ where $a_n \neq 0$. We say that the **degree** of f is $\partial f = n$.
The degree function has the following properties:

(a) $\partial(f+g) \leq \max(\partial f, \partial g)$

(b) $\partial(fg) = \partial f + \partial g$

Recall the fundamental theorem of algebra.

Theorem 1: Fundamental Theorem of Algebra

If $f \in \mathbb{C}[x]$ with $\partial f \neq 0$, then $\exists z \in \mathbb{C}$ such that $f(z) = 0$. i.e. $\exists k, z_1, \ldots, z_n \in \mathbb{C}$ such that $f = k(x - z_1)(x - z_2)\ldots(x - z_n)$.

Recall the division algorithm:
Let R be a Euclidean domain with norm N. For any $a, b \in R$, $b \neq 0$, $\exists q, r$ such that $a = qb + r$ such that $r = 0$ or $N(r) < N(b)$.

Lecture 2

Exercise 1. Factor $x^3 + 5x^2 + 15x + 18$.

Solution. Notice that -2 is a root $x^3 + 5x^2 + 15x + 18$. Thus $x + 2 \mid x^3 + 5x^2 + 15x + 18$. This yields $x^3 + 5x^2 + 15x + 18 = (x+2)(x^2 + 3x + 9)$. □

Exercise 2. Is $f = x^3 + 2x + 2$ irreducible?

Solution. Suppose $f = gh$ and wlog $\deg(g) = 1, \deg(h) = 2$. So $g = x + a$ and $h = x^2 + bx + c$ thus $(x + a)(x^2 + bx + c) = x^3 + (a + b)x^2 + (c + ab)x + ac = x^3 + 2x + 2$. We must have that $2 \mid a, b, c$. However, this implies that $4 \mid ac$ but this is a contradiction. Hence f is irreducible. □

This example inspires the following result.

Theorem 2: Eisenstein Criterion

Let $f \in \mathbb{Z}[x]$ be a polynomial $f = a_n x^n + \cdots + a_0$. Suppose that for some prime p

(a) $p \nmid a_n$.

(b) $p \mid a_i$ for all $i < n$.

(c) $p^2 \nmid a_0$.

Then f is irreducible over $\mathbb{Q}$.

Proof. By way of contradiction, suppose $f = gh \in \mathbb{Z}[x]$ where g, h are non-constant. We have $\overline{f} \equiv \overline{g}\overline{h} \equiv \overline{a_n}x^n \pmod p$. This implies that $\overline{f}$ and $\overline{g}$ are monomials (why is it not possible to have lower degree terms cancel out when multiplying $\overline{g}$ and $\overline{h}$?) This implies that $p \mid \overline{g}(0), \overline{h}(0) \Rightarrow p^2 \mid a_0$. Which is a contradiction. □

Corollary

If p is prime, $f = x^{p-1} + \cdots + x + 1 \in \mathbb{Z}[x]$ is irreducible.

Proof. We perform a little trick to turn f into something we can apply Eisenstein to. Since $f(x) = x^{p-1} + \cdots + x + 1$ we shifty by one to get

$$xf(x+1) = (x+1)^p - 1 = \sum_{i=0}^{p} x^i \binom{p}{i} - 1$$

Since $p \mid \binom{p}{i}$ for $i \neq 0, p$ we can apply the Eisenstein criterion to get that f is irreducible. □

Example: We can try to find irreducible polynomials over $\mathbb{F}_2$. We do this by looking at degrees:

$$\underline{\text{Degree 1:}}\ \underbrace{x, x+1}_{\text{irreducible}}$$

$$\underline{\text{Degree 2:}}\ \underbrace{x^2 + x + 1}_{\text{irreducible}}, \underbrace{x^2, x^2 + 1, x^2 + x}_{\text{reducible}}$$

$$\underline{\text{Degree 3:}}\ \underbrace{x^3 + x + 1, x^3 + x^2 + 1}_{\text{irreducible}}, \underbrace{x^3 + 1, x^3, x^3 + x^2 + x + 1, \ldots}_{\text{reducible}}$$

Notice that we can calculate how many irreducible polynomials of degree n there are if we know how many irreducible polynomials of degrees less than n there are. There are 2^4 degree 4 polynomials over $\mathbb{F}_2$. We can calculate the number of reducible polynomials by seeing in how many ways we can combine polynomials of degrees $1, 2$ and 3 to obtain polynomials of degree 4. The calculation goes as follows:

- $1+1+1+1$. Product of four degree 1 irreducible polynomials: 5 choices.
- $1+1+2$. Product of two degree 1 irreducibles and one degree 2 irreducible: 3 choices.
- $2+2$. Product of two degree 2 irreducibles: 1 choice
- $1+3$. Product of one degree 1 irreducible and one degree 1 irreducible: 4 choices.

Adding all these up we have 13 irreducible polynomials of degree 4 over $\mathbb{F}_2$. Hence there are $16-13=3$ irreducibles of degree 4.

Definition 2. A polynomial $f \in \mathbb{Z}[x]$ is **primitive** if $f = a_nx^n + \cdots + a_0$ if $a_n \geq 1$ and $\gcd(a_0, \ldots, a_n) = 1$.

Lemma

Let $f \in \mathbb{Q}[x]$, then $\exists! c \in \mathbb{Q}$ such that $f = cf_0$ and $f_0 \in \mathbb{Z}[x]$ is primitive.

Proof. Multiply with the lcm of the denominators of all coefficients of f and then divide by the gcd of the new coefficients to get a primitive polynomial. □

The following result is going to be quite important down the line. People refer to different results by the name "Gauss Lemma," but the one we'll give that name to is the following.

Theorem 3: Gauss' Lemma

Let $f, g \in \mathbb{Z}[x]$ be primitive polynomials then fg is primitive.

Proof. There are several proofs of this. I think you can do this using Bézout's identity. □

Corollary

If $f, g \in \mathbb{Z}[x]$ and g is primitve. If $g \mid f$ in $\mathbb{Q}[x]$, then $g \mid f$ in $\mathbb{Z}[x]$.

Proof. Suppose $f = gh \in \mathbb{Q}[x]$. Factor $h = ch_0$ where h_0 is primitive and $c \in \mathbb{Q}$ Then $f = c \cdot gh_0 \in \mathbb{Z}$. By Gauss' lemma, gh_0 is primitive. This implies that $c \in \mathbb{Z}$ therefore $h = ch_0 \in \mathbb{Z}[x]$. □

Lemma

If f is irreducible in $\mathbb{Z}[x]$, then it is irreducible in $\mathbb{Q}[x]$.

Proof. □

Lecture 3

Field Extensions (in $\mathbb{C}$)

Definition 3. Let $K, L \subset \mathbb{C}$ be fields. A **field extension** is an injection of fields $K \hookrightarrow L$.

Definition 4. Let $S \subset \mathbb{C}$ be a subset, $F \subset \mathbb{C}$ is a subfield

$$F(S) := \text{smallest subfield of } \mathbb{C} \text{ containing F \& S.}$$

Examples:

- $$\begin{tikzcd} \mathbb{Q}(i) \arrow[d, dash] \\ \mathbb{Q} \end{tikzcd}$$ You need $i \in \mathbb{Q}(i)$, therefore you'll get $a + bi \in \mathbb{Q}(i)$. Note that $(a + bi)^{-1} = \dfrac{a - bi}{a^2 + b^2}$ so $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$

- $$\begin{tikzcd} \mathbb{Q}(\sqrt[3]{2}) \arrow[d, dash] \\ \mathbb{Q} \end{tikzcd}$$ Let $\omega = \sqrt[3]{2}$. We get $\{a + b\omega + c\omega^2 \mid a, b, c \in \mathbb{Q}\} = \mathbb{Q}(\sqrt[3]{2})$. We need to show the linear independence over $\mathbb{Q}$ of $\{1, \omega, \omega^2\}$ and we get that $\mathbb{Q}(\sqrt[3]{2})$ is a 3 dimensional vector space over $\mathbb{Q}$.

- Let $\beta = 1 + \sqrt{2} \in \mathbb{C}$ and $\alpha \in \mathbb{C}$. Then $$\begin{tikzcd} \mathbb{Q}(\beta) = \mathbb{Q}(\alpha) \arrow[d, dash] \\ \mathbb{Q} \end{tikzcd}$$ $\mathbb{Q}(\alpha)$ comes from adjoining to $\mathbb{Q}$ a root of $x^2 - 2 = 0$.
  $\mathbb{Q}(\beta)$ comes from a adjoining to $\mathbb{Q}$ a root of $x^2 - 2x - 1 = 0$. The extensions are the same; however, the polynomials look quite differrent. How can we tell from polynomials that attaching roots from the two polynomials will give the same extensions? This will be discussed later.

- $$\begin{tikzcd}\mathbb{Q}(i,\sqrt{2}) \arrow[d, dash, "2"] \\ \mathbb{Q}(\sqrt{2}) \arrow[d, dash, "2"] \\ \mathbb{Q}\end{tikzcd}$$ Splitting up the extensions makes stuff easier. A basis for $\mathbb{Q}(i,\sqrt{2})$ over $\mathbb{Q}$ is $\{1, i, \sqrt{2}, i\sqrt{2}\}$. The following is the diagram of all intermediate fields between $\mathbb{Q}(i,\sqrt{2})$ and $\mathbb{Q}$.

  $$\begin{tikzcd} & \mathbb{Q}(i,\sqrt{2}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\ \mathbb{Q}(i) \arrow[dr, dash] & \mathbb{Q}(\sqrt{2}) \arrow[d, dash] & \mathbb{Q}(i\sqrt{2}) \arrow[dl, dash] \\ & \mathbb{Q} & \end{tikzcd}$$

  Can we find β such that $\mathbb{Q}(\beta) = \mathbb{Q}(i,\sqrt{2})$? Yes! Take $\beta = i+\sqrt{2}$ and this works. β is a root of $x^4 - 2x^2 + 9$. There are infinitely choices for β. So how do you find a polynomial whose root can be one such β if you know the minimal polynomials of $i, \sqrt{2}$? Miki said that there's no good way of doing this and I will cry. I'm not convinced.

Definition 5. A field extension K/F is **simple** if $\exists \alpha \in K$ so $K = F(\alpha)$.

Definition 6. An **isomorphism** of a field extension $K/F \overset{\sim}{\to} K'/F'$ is a pair of field isomorphisms $\lambda : K \to K', \mu : F \to F'$ so $\lambda|_F = \mu$.

$$\begin{tikzcd} K \arrow[r, "\lambda"] & K' \\ F \arrow[u, hook] \arrow[r, "\mu"] \arrow[ur, phantom, "\circlearrowright"] & F' \arrow[u, hook] \end{tikzcd}$$

Example:

- $$\begin{tikzcd}\mathbb{Q}(i) \arrow[r, "i\mapsto -i"] & \mathbb{Q}(i) \\ \mathbb{Q} \arrow[u, dash] \arrow[r, "id"] & \mathbb{Q} \arrow[u, dash]\end{tikzcd}$$ We can also change i with $\sqrt{2}$.

Definition 7. If K/F, K'/F' an **F-morphism** is a field homomorphism $\lambda : K \to K'$ so $\lambda|_F = id$.

Definition 8. Let K/F be a field extension. We say $\alpha \in K$ is **algebraic** over F if there exists $f \in F[x]$ such that $f(\alpha) = 0$. If not algebraic, an element is called **transcendental**. Example: π is transcendental over $\mathbb{Q}$.

Definition 9. An extension K/F is **algebraic** if $\forall k \in K$ is algebraic over F. Example: $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is an algebraic extension.

Example:

- Let $\alpha \in \mathbb{Q}(\sqrt{2})$ be arbitrary. Then $1, \alpha, \alpha^2$ is a linearly dependent set. Thus there's a polynomial one of whose roots is α.

Lecture 4

Proposition

If K/F is a finitely dimensional extension, then K/F is algebraic.

Consider $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \dots)$ over $\mathbb{Q}$. This is infinite-dimensional over $\mathbb{Q}$ but has no transcendental elements. So the converse of the proposition above does not hold.
Today we'll work in $\mathbb{C}$:

Definition 10. Take a field F ($\subseteq \mathbb{C}$) and $\alpha \in \mathbb{C}$ algebraic over F. Take a monic polynomial $m_\alpha \in F[x]$ with $m_\alpha(\alpha) = 0$ with smallest possible degree. This polynomial is unique and is called the **minimal polynomial** of α over F.
Example:

- $\alpha = \sqrt[4]{2} \in \mathbb{C}$.
  - Minimal polynomial over $\mathbb{Q}$: $x^4 - 2 = 0$.
  - Minimal polynomial over $\mathbb{Q}(\sqrt{2})$: $x^2 - \sqrt{2} = 0$.
  - Minimal polynomial over $\mathbb{Q}(\sqrt[4]{2})$: $x - \sqrt[4]{2} = 0$.

  So the ground field is important!

We need to establish the uniqueness of the minimal polynomial. This is quite easy. Assume there's two "minimal polynomials", take their difference and you've obtained a nonconstant polynomial of lower degree where α vanishes. This contradicts the minimality of the polynomials.

Proposition

(a) Any polynomial $p \in F[x]$ with $p(\alpha) = 0$ is a multiple of m_α.

(b) The minimal polynomial is irreducible.

Part (b) has a converse as follows: For any irreducible monic polynomial $m \in F[x]$ there exists $\alpha \in \mathbb{C}$ so that m is its minimal polynomial.

We would like to have a way of expressing field extensions $F(\alpha)$ through the minimal polynomial of α. This can be done. In particular, we'll show that

$$F[x]/(m_\alpha) \simeq F(\alpha).$$

Proposition : 0

If $K \subseteq \mathbb{C}$ is a subfield and $m \in K[x]$. $K[x]/(m)$ is a field if and only if m is irreducible.

Proof. We want to show that (m) is maximal if and only if m is maximal.
If m is reducible then $m = fg$ where $0 < \partial f < \partial m$. We then have $(m) \subsetneq (f) \subsetneq K[x]$. So (m) is not maximal.
For the other direction, assume (m) is not maximal then we know that there exists an ideal I such that $(m) \subsetneq I \subsetneq K[x]$. Since $K[x]$ is a PID, we have $I = (h)$. *Finish it.* □

Proposition : 1

Let $K \subseteq \mathbb{C}$ be a subfield and $\alpha \in \mathbb{C}$ have minimal polynomial m_α over K. There exists a homomorphism $K[x] \overset{\varphi}{\to} \mathbb{C}$ sending $x \mapsto \alpha$ with $\ker \varphi = (m_\alpha)$.

Proof. □

Proposition : 2

φ is surjective onto $K[\alpha] \subseteq \mathbb{C}$.

Proof. □

Proposition : 3

$$K[x]/(m_\alpha) \simeq K[\alpha].$$

Proof. □

From propositions 0 and 3 we have that $K[\alpha]$ is a field so $K[\alpha] = K(\alpha)$.
Example:

- $\mathbb{Q}[x]/(x^2 + 1) \simeq \mathbb{Q}(i)$.

Corollary

Let $K \subseteq \mathbb{Q}$ be a subfield. If $\alpha, \beta \in \mathbb{C}$ with the same minimal polynomial m over K. Then $K(\alpha)/K \simeq K(\beta)/K$.

Example:

- $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q} \xrightarrow{\sim} \mathbb{Q}(\sqrt[3]{2}\zeta_3)/\mathbb{Q}$ where $\zeta_3 = e^{2\pi i/3}$.

PSET 2

Lecture 5

Let $F(\alpha)$ be an extension where α satisfies $f(\alpha) = a_n\alpha^n + \cdots + a_1\alpha + a_0 = 0$. Consider an F-morphism $F(\alpha) \xrightarrow{\varphi} K$. Then $\varphi(a_n\alpha^n + \cdots + a_0) = 0 \Rightarrow f(\varphi(\alpha)) = 0$. Hence roots are sent to roots.
Given any field F (in $\mathbb{C}$ or not) and an irreducible polynomial $m \in F[x]$. Adjoining a root α of m means $F(\alpha) := F[x]/(m)$.

Lemma

Let F be a field, $m \in F[x]$ an irreducible polynomial. Adjoin a root α of m then $F(\alpha)$ has basis $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ over F where $n = \partial m$.

The following theorem is going to be quite important hence the, pardon, a* name.

Theorem 4: The Extension Theorem

Let $i : K \xrightarrow{\sim} L$ be a field isomorphism and $m \in K[x]$ an irreducible polynomial. Let $i(m) =: m' \in L[x]$ and $K(\alpha)$ and $L(\beta)$ be extensions by attaching a root of m and m', respectively. Then we have that there exists $j : K(\alpha) \xrightarrow{\sim} L(\beta)$ such that $j|_K = i$.

In diagram the previous theorem is the following:

$$\begin{tikzcd}
K(\alpha) \arrow[r, dotted, "\underset{j}{\sim}" description] \arrow[d, dash, "m"] & L(\beta) \arrow[d, dash, "m'"] \\
K \arrow[r, "\underset{i}{\sim}" description] & L
\end{tikzcd}$$

Define j as $j(a_0 + \cdots + a_n\alpha^n) = i(a_0) + \cdots + i(a_n)\beta^n$. Since $K(\alpha) \simeq K[x]/(m)$ and $L(\beta) \simeq L[x]/(m')$ it is easy to see that $K[x]/(m) \simeq L[x]/(m')$ from which the proof follows.
Example:

- $K = L = \mathbb{Q}$, $i = \mathrm{id}$

$$\begin{tikzcd}
\mathbb{Q}(\sqrt{2}) \arrow[rr, "\sqrt{2}\mapsto-\sqrt{2}"] \arrow[dr, dash] & & \mathbb{Q}(-\sqrt{2}) \arrow[dl, dash] \\
& \mathbb{Q} &
\end{tikzcd}$$

$\alpha = \sqrt{2}, \beta = -\sqrt{2}, m = m' = x^2 - 2.$

- $$\begin{tikzcd}
\mathbb{Q}(\sqrt[4]{2}) \arrow[rr, dotted, "\sqrt[4]{2}\mapsto i\sqrt[4]{2}", "j"'] \arrow[d, dash, "m=x^2-\sqrt{2}"'] & & \mathbb{Q}(i\sqrt[4]{2}) \arrow[d, dash, "m'=x^2+\sqrt{2}"] \\
\mathbb{Q}(\sqrt{2}) \arrow[rr, "\sqrt{2}\mapsto-\sqrt{2}"] \arrow[dr, dash] & & \mathbb{Q}(-\sqrt{2}) \arrow[dl, dash] \\
& \mathbb{Q} &
\end{tikzcd}$$

Definition 11. Let K/F be a field extension. The extension **degree** $[K : F]$ is the dimension of K as an F-vector space.
Examples:

- $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$

- If $m \in K[x]$ is an irreducible polynomial and α is a root of m, then $[K(\alpha) : K] = \partial m$.

Theorem 5: Tower Law

Let L/K and K/F be field extensions. Then

$$[L : F] = [L : K] \cdot [K : F].$$

Proof. Linear algebra. Take a basis $\{\beta_1, \ldots, \beta_n\}$ for L/K and $\{\alpha_1, \ldots, \alpha_m\}$ for K/F. Then L/F has basis $\{\alpha_i\beta_j\}$. □

Example:

- $$\begin{tikzcd}
\mathbb{Q}(i,\sqrt{2}) \arrow[d, dash, "2"'] \arrow[dr, dash, "2"] \arrow[dd, dash, bend right=60, "4"'] & \\
\mathbb{Q}(\sqrt{2}) \arrow[d, dash, "2"'] & \mathbb{Q}(i) \arrow[dl, dash, "2"] \\
\mathbb{Q} &
\end{tikzcd}$$

- Find the value of ?

$$\begin{tikzcd}
\mathbb{Q}(\sqrt[4]{2}) \arrow[d, dash, "?"'] \arrow[dd, dash, bend right=60, "4"'] \\
\mathbb{Q}(\sqrt{2}) \arrow[d, dash, "2"'] \\
\mathbb{Q}
\end{tikzcd}$$

- Bound d in terms of m and n.

$$\begin{tikzcd}
 & F(\alpha, \beta) \arrow[dl, dash] \arrow[dr, dash] \arrow[dd, dash, "d"] & \\
F(\alpha) \arrow[dr, dash, "m"'] & & F(\beta) \arrow[dl, dash, "n"] \\
 & F &
\end{tikzcd}$$

Note that $\operatorname{lcm}(m, n) \leq d \leq mn$.

Lecture 6

Recall the tower law from last time. We have the following, more-or-less straightforward, corollaries.

Corollary : 1

If we had extensions $K_n/K_{n-1}/\ldots/K_1/K_0$, then

$$[K_n : K_0] = \prod_{i=1}^{n} [K_i : K_{i-1}].$$

Proof. Induction. □

Corollary : 2

If we have a field extension K/F with $[K : F] < \infty$ and $\alpha \in K$ with minimal polynomial m_α over F, then $\partial m_\alpha \mid [K : F]$.

Proof. This follows from the tower law combined with the following diagram.

$$\begin{tikzcd}
K \\
F(\alpha) \arrow[u, dash] \\
F \arrow[u, dash, "\partial m_\alpha"'] \arrow[uu, dash, bend left=60, "{[K:F]}"]
\end{tikzcd}$$

□

Definition 12. We define the **degree** of α over F to be ∂m_α.

Corollary : 3

Let $f \in \mathbb{R}[x]$ be an irreducible polynomial. Then $\partial f = 1$ or $\partial f = 2$.

Proof. We know that f splits into linear factors in $\mathbb{C}[x]$. Since $[\mathbb{C} : \mathbb{R}] = 2$ we must have that $\partial f \leq 2$. □

Attaching all roots of $f \in F[x]$

- If $\partial f = 2$ is irreducible with roots α_1, α_2 (both of degree 2 over F)

$$[F(\alpha_1, \alpha_2) : F] = 2$$

  Proof. We know that $[F(\alpha_1) : F] = 2$. Since $f = (x - \alpha_1)(x - \alpha_2) = x^2 - (\alpha_1 + \alpha_2)x + \alpha_1\alpha_2$. We know that $\alpha_1 + \alpha_2 \in F$ and $\alpha_1 \in F(\alpha_1)$ so we must have $\alpha_2 \in F(\alpha_1)$. □

- If $\partial f = 3$ and f is irreducible with roots $\alpha_1, \alpha_2, \alpha_3$. We have

$$3 \leq [F(\alpha_1, \alpha_2, \alpha_3) : F] \leq 6$$

  Proof. The proof is not bad. Note that

$$\begin{tikzcd}
F(\alpha_1, \alpha_2) & = F(\alpha_1, \alpha_2, \alpha_3) \\
F(\alpha_1) \arrow[u, dash, "\leq 2"'] \\
F \arrow[u, dash, "3"']
\end{tikzcd}$$

□

We can generalize what we did as follows

Theorem 6

If f is an irreducible polynomial over F of degree n with roots $\alpha_1, \alpha_2, \ldots, \alpha_n$, then

$$[F(\alpha_1, \alpha_2, \ldots, \alpha_n) : F] \leq n!$$

Definition 13. In the setting of the theorem above where $F \subset \mathbb{C}$ we call $F(\alpha_1, \ldots, \alpha_n)/F$ the **splitting field** of f over F. We say that an extension K/F is **finite** if $[K : F] < \infty$.

Remark

- Note that $F(\alpha)/F$ is finite if and only if α is algebraic over F.
- However, K/F is algebraic does not necessarily imply that the extension is finite.
- K/F is **finitely generated** (meaning there exist $\gamma_1, \ldots, \gamma_m$ such that $K = F(\gamma_1, \ldots, \gamma_m)$) and algebraic if and only if K/F is finite.

Proposition

Let K/F be a field extension and let $S = \{\alpha \in K : \alpha \text{ algebraic over } F\}$, then S is a subfield of K.

Proof. Suppose $\alpha, \beta \in S$ are nonzero. We have $[F(\alpha, \beta) : F] \leq [F(\alpha) : F][F(\beta) : F] < \infty$. Hence we have $\alpha^{-1}, \alpha\beta, -\alpha$,etc are all in $F(\alpha, \beta) \subseteq S$. □

Theorem 7

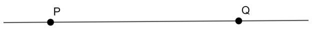
If L/K and K/F are algebraic extensions, then L/F is algebraic.

Proof. Eazy with a z. □

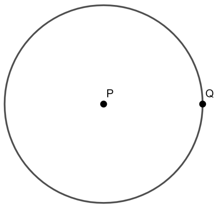
Constructions with Ruler and Compass

Starting set S of points in the plane. We're allowed 2 operations:

(1) Line $L(p, q)$

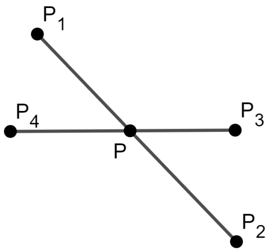


(2) Circle $C(p,q)$ (meaning circle with center at p passing through q)



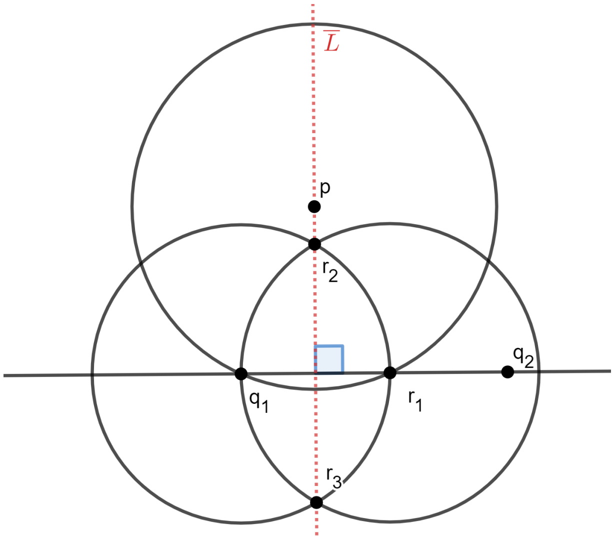
New points are going to be intersections of these.

Definition 14. A point p is **constructible** from S if you can reach it by finite series of allowed operations.



Construction 1:

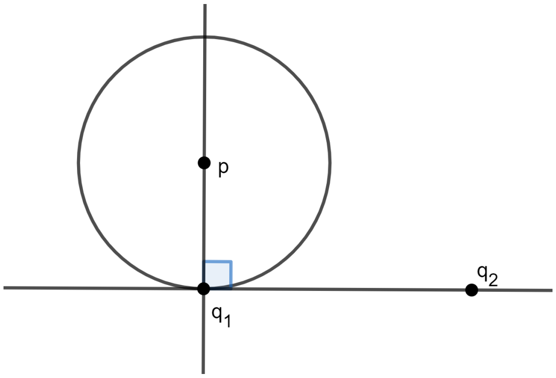
Given p and $L = L(q_1, q_2)$. Construct the line $\overline{L}$ perpendicular to L through p.
Without loss of generality, say $p \neq q_1$.



1. $C(p, q_1)$. Case 1: $L \subset C(p, q_1) = \{q_1, r_1\}$ $r_1 \neq q_1$.

2. $C(q_1, r_1), C(r_1, q_1)$ intersect at r_2 and r_3.

3. $\overline{L} = L(r_2, r_3)$.

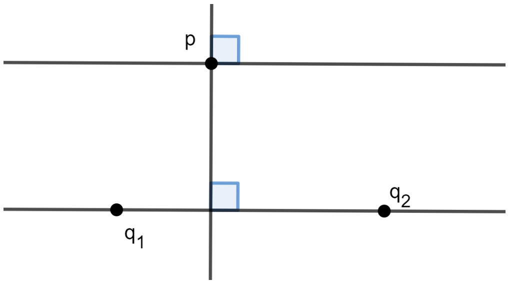


1. $C(p, q_1)$. Case 2: $L \subset C(p, q_1) = \{q_1\}$
2. $\overline{L} = L(p, q_1)$

Construction 2:

Given p and L. Draw $\overline{L}$ parallel to L through p.
Case 1: $p \in L$, then $\overline{L} = L$.
Case 2:

1. Draw L_1 perpendicular to L through p.
2. Draw $\overline{L}$ perpendicular to L, though p.



Construction 3:

Given $L(q_1, q_2), p_1, p_2$. Mark the distance between p_1 and p_2 on L, starting from q_1

Problem Set 3

Lecture 7

From now on, starting set $S = \{(0,0), (1,0)\}$. Hence constructible means from S.

Definition 15. $a \in \mathbb{R}$ is constructible if $|a|$ is a distance between constructible points.

Proposition

$p = (a, b)$ is constructible point if and only if a and b are constructible numbers.

Proof. You draw a rectangle. Done. □

Proposition

The set of constructible numbers is a subfield of $\mathbb{R}$.

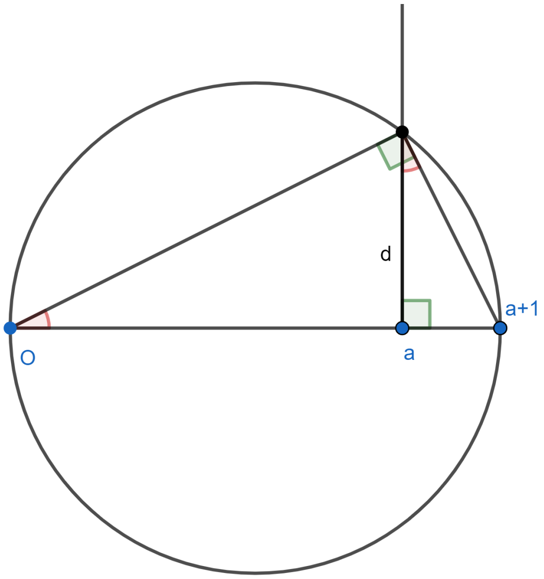
Proof. Easy to check. □

Which real numbers are constructible? It's easy to see that $\mathbb{Z}$ and $\mathbb{Q}$ are constructible. We can also construct $\sqrt{n}$ using the Pythagorean theorem repeatedly.

Proposition

If $a \in \mathbb{R}^+$ is constructible, so is $\sqrt{a}$.

Proof. Consider the following construction.



Note that by similarities of triangles we have $d^2 = a$. Hence we have that provided that a is constructible, so is $\sqrt{a}$. Using what we know from problem set 2, we have that if we can construct F, then we can construct any degree 2 extension of F (by adjoining a square root). □

Proposition

$a \in \mathbb{R}$ is constructible if and only if there exists a chain $F_0 = \mathbb{Q} \subset F_1 \subset F_2 \subset \cdots \subset F_n$ such that $a \in F_n$ and $\forall i$, $[F_i : F_{i-1}] = 2$.

Proof. "$\Leftarrow$" shown just now.
"$\Rightarrow$" Let $p_1 = (a_1, b_1)$, $p_2 = (a_2, b_2) \neq p_1$.
$L(p_1, p_2):\ (b_2 - b_1)(x - a_1) = (a_2 - a_1)(y - b_1)$.
$C(p_1, p_2):\ (x - a_1)^2 + (y - b_1)^2 = (a_2 - a_1)^2 + (b_2 - b_1)^2$ Something something. IDK. □

Consequence: $[F_n : F_0] = 2^n$

Ancient Questions

1. 'square a circle': Given a constructible circle, construct a square of the same area. This is not possible since π is transcendental over $\mathbb{Q}$ (we can't construct $\sqrt{\pi}$)

2. 'trisect an angle': Note that an angle α is constructible if $\cos\alpha$ and $\sin\alpha$ are constructible. Given a constructible angle α, construct the angle $\alpha/3$.
   This is not generally possible either, we can construct $\pi/3$ but not $\pi/9$. (we'll see this in the homework)

3. 'double a cube': Given a constructible cube (i.e., can get its side), construct a cube with twice the volume. This is impossible because $\deg_{\mathbb{Q}} \sqrt[3]{2} = 3$.

4. Which regular p-polygons are constructible (where p is prime)?

Galois & Roots of Polynomials

Examples:

1. $f = x^2 + 1$ has roots $r_1 = i$, $r_2 = -i$. We have $r_1^2 = -1$ so if $r_1 \rightsquigarrow s$, we must have $s^2 = -1$. Since $(r_1 + r_2) = 0$ if $r_1 \rightsquigarrow s_1$, $r_2 \rightsquigarrow s_2$ we need $s_1 + s_2 = 0$.

2. $f = x^4 - x^2 - 2 = (x^2 + 1)(x^2 - 2)$. We have $r_1 = i, r_2 = -i, r_3 = \sqrt{2}, r_4 = -\sqrt{2}$. Can we do $r_1 \rightsquigarrow r_3$? No, because $r^2 = -1 \neq r_3^2$. If $r_1 \rightsquigarrow s$, then $r_2 \rightsquigarrow -s$ because $r_1 + r_2 = 0$. What permutation of roots can we do? In S_4 notation: 1, (12), (34), (12)(34).

3. $f = x^4 + 2x^2 + 4$. $\alpha_1 = i + \sqrt{2}, \alpha_2 = -i + \sqrt{2}, \alpha_3 = i - \sqrt{2}, \alpha_4 = -i - \sqrt{2}$ Allowed permutations:1, (14)(23),(13)(24), (12)(34)

Lecture 8

Pre-Class Recap

Definition 16. Let K/F be an extension. We define the **Galois Group** of K/F as $\mathrm{Gal}(K/F) = \mathrm{Aut}_F(K) = \{\alpha \in \mathrm{Aut}(K) : \alpha|_F = id\}$. $\mathrm{Gal}(K/F)$ is a subgroup of $\mathrm{Aut}(K)$. Last time we saw that $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) \simeq Z_2$ and $\mathrm{Gal}(\mathbb{Q}(i,\sqrt{2})/\mathbb{Q}) \simeq Z_2 \times Z_2$. Examples:

1. Consider $\mathbb{Q}(i)/\mathbb{Q}$ and $\alpha \in \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$. We should have $\alpha(a) = a\ \forall a \in \mathbb{Q}$. We have $\alpha(i)^2 = -1$ so $\alpha(i) = \pm i$ and $\alpha(a_1 + a_2 i) = a_1 + a_2\alpha(i)$.

   – If $\alpha(i) = i$, then $\alpha_1 = id$.

   – Else $\alpha_2 : i \mapsto -i$.

   So $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) \simeq Z_2$.

2. $K = \mathbb{Q}(i,\sqrt{2})$ Consider $\alpha \in \mathrm{Gal}(K/\mathbb{Q})$. We have $\alpha(i) = \pm i$ and $\alpha(\sqrt{2})^2 = 2 \Rightarrow \alpha(\sqrt{2}) = \pm\sqrt{2}$. So $\alpha(a_1 + a_2 i + a_3\sqrt{2} + a_4 i\sqrt{2}) = a_1 + a_2\alpha(i) + a_3\alpha(\sqrt{2}) + a_4\alpha(i)\alpha(\sqrt{2})$. Based on these examples, we have the following application of the extension theorem.

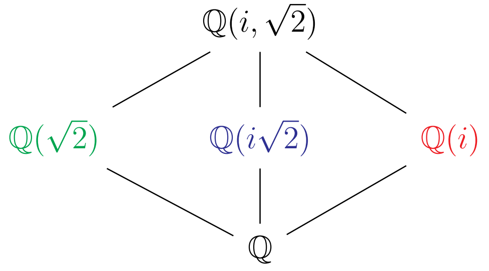
$$\begin{tikzcd}
\mathbb{Q}(i,\sqrt{2}) \arrow[rr, dotted, "\sqrt{2}\overset{\beta}{\mapsto}\pm\sqrt{2}"] \arrow[d, dash, "m=x^2-2"'] & & \mathbb{Q}(i,\sqrt{2}) \arrow[d, dash, "\alpha(m)=x^2-2"] \\
\mathbb{Q}(i) \arrow[rr, "i\overset{\alpha}{\mapsto}\pm i"] \arrow[dr, dash] & & \mathbb{Q}(i) \arrow[dl, dash] \\
& \mathbb{Q} &
\end{tikzcd}$$

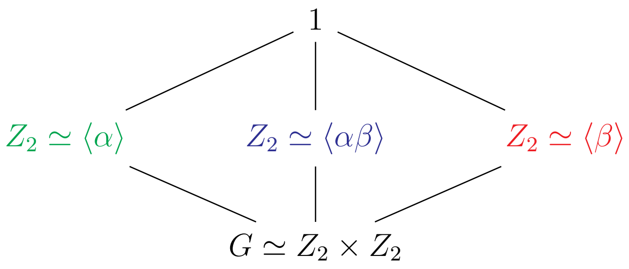
   All four maps are valid automorphisms in $\mathrm{Gal}(K/\mathbb{Q})$. Indeed $\mathrm{Gal}(K/\mathbb{Q}) \simeq Z_2 \times Z_2$.

Is it possible to establish a correspondence between intermediate fields in an extension and subgroups of $\mathrm{Gal}(K/F)$?

Definition 17. Let K/F be an extension, $G = G(K/F), H \leq G$. We define the **fixed field** of H to be $K^H := \{x \in K : h(x) = x \quad \forall h \in H\}$. It is easy to see that K^H is indeed a field. Also $K^H \supset F$ because $H \leq G$ fixes all of F. This gives us the means to establish the correspondence conjectured above. Example:

- $\mathrm{Gal}(\mathbb{Q}(i,\sqrt{2})/\mathbb{Q}) \simeq Z_2 \times Z_2$ with $\alpha(i) = -i, \alpha(\sqrt{2}) = \sqrt{2}$ and $\beta(i) = i, \beta(\sqrt{2}) = -\sqrt{2}$. We have the following lattices:




1
$Z_2 \simeq \langle\alpha\rangle$
$Z_2 \simeq \langle\alpha\beta\rangle$
$Z_2 \simeq \langle\beta\rangle$
$G \simeq Z_2 \times Z_2$

Proposition

Let K/F be a field extension and $G = \mathrm{Gal}(K/F)$. Given an intermediate field M take $H = \mathrm{Gal}(K/M) \leq G$. And then $K^H = K^{\mathrm{Gal}(K/M)}$. Claim: $M \subset K^{\mathrm{Gal}(K/M)}$.

Proposition

$H \leq G$.

Definition 18. A finite extension K/F is called **Galois** if $|\mathrm{Gal}(K/F)| = [K : F]$.

Theorem 8: Main Theorem of Galois Theory

Let K/F be a Galois extension and $G = \mathrm{Gal}(K/F)$.

(a) There is a bijection between field towers $F \subseteq E \subseteq K$ and subgroups $H \subseteq G$

$$\begin{tikzcd}
K & & 1 \\
E \arrow[u, dash] & \Longleftrightarrow & H \arrow[u, dash] \\
F \arrow[u, dash] & & G \arrow[u, dash]
\end{tikzcd}$$

The bijection sends H to its fixed field K^H, and hence is inclusion reversing.

(b) Under this bijection, we have $[K : E] = |H|$ and $[E : F] = [G : H]$.

(c) K/E is always Galois, and its Galois group is $\mathrm{Gal}(K/E) = H$.

(d) E/F is Galois if and only if H is normal in G. If so, $\mathrm{Gal}(E/F) = G/H$.

Example: $F \subset \mathbb{C}, f \in F[x]$, roots $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$. The **splitting field** of f over F is $F(\alpha_1, \ldots, \alpha_n)/F$.

Proposition

$f \in F[x]$, $F \subset \mathbb{C}$. The splitting field of f over F is a Galois extension.

Lecture 9

Missed class. Here's more or less what was done.
If $[K:F]$ is finite with Galois group G. Then $K^G = F$.

Definition 19. Let K/F be a field extension and $f \in F[x]$. We say that f **splits** over K if there exists $c, \alpha_1, \dots, \alpha_n \in K$ such that $f = c(x-\alpha_1)\dots(x-\alpha_n) \in K[x]$.

Definition 20. Let F be a field and $f \in F[x]$. The **spliting field** of f is an extension K/F such that

1. f splits over K, with roots α_i.
2. $K = F(\alpha_1, \dots, \alpha_n)$.

Theorem 9

Let $f \in F[x]$, there exists a splitting field K/F for f and is unique up to isomorphism.

Lemma

$f \in F[x]$, K/F is a splitting field

Problem Set 4

Lecture 10

Definition 21. A field extension K/F is called **normal** if every irreducible polynomial $f \in F[x]$ with a root in K splits over K. Example:

- $$\begin{tikzcd}\mathbb{Q}(\sqrt[3]{2}) \arrow[d, dash, "x^3-2"] \\ \mathbb{Q}\end{tikzcd}$$

  This is not normal as you will miss the non-real cubic roots of 2.

- $$\begin{tikzcd}\mathbb{Q}(\sqrt{2}) \arrow[d, dash] \\ \mathbb{Q}\end{tikzcd}$$

We claim that this is a normal extension. If $f \in \mathbb{Q}[x]$ is irreducible and has a root in $\mathbb{Q}(\sqrt{2})$ then $\partial f = 1$ or $\partial f = 2$. If $\partial f = 1$ then f splits over $\mathbb{Q}$. If $\partial f = 2$, then we have that f splits over $\mathbb{Q}(\sqrt{2})$.
Similarly, we can show that every degree 2 extension is normal.

Theorem 10

K/F is a finite and normal field extension if and only if it is the splitting field of some polynomial $f \in F[x]$.

Proof.
"$\Rightarrow$"
Let $K = F(\alpha_1, \dots, \alpha_k)$.

- Take m_i to be the minimal polynomial of α_i over F.
- $f := m_1 \dots m_k$
- m_i is irreducible with a root in K, K/F is normal so m_i splits over K. Hence f splits in K.
- Easy to check that K is the splitting field of f.

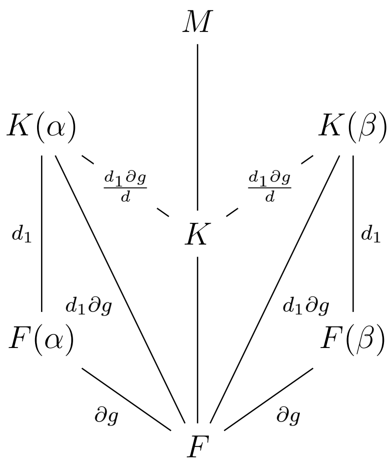
"$\Leftarrow$"
Let K/F be the splitting field of some $f \in F[x]$. We have that K/F is finite. Hence it remains to show that it is normal. To do so, take $g \in F[x]$ to be irreducible. Take M/K to be the splitting field of g over K and let α, β be roots of g in M. We have

- $K(\alpha)/F(\alpha)$ is the splitting field of $f \in F(\alpha)[x]$
- $K(\beta)/F(\beta)$ is the splitting field of $f \in F(\beta)[x]$

From the diagram

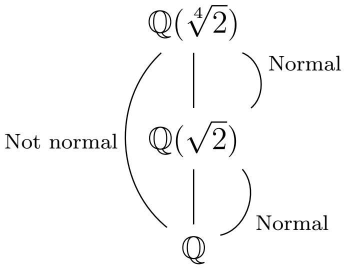
$$\begin{tikzcd}
K(\alpha) \arrow[r, dotted, "\sim", "j"'] \arrow[d, dash] & K(\beta) \arrow[d, dash] \\
F(\alpha) \arrow[r, "\sim"] & F(\beta)
\end{tikzcd}$$

we derive $[K(\alpha) : F(\alpha)] = [K(\beta) : F(\beta)] = d_1$. So we can fill in the following diagram:



So if $\alpha \in K$, then $[K(\alpha) : K] = 1$. Consequentially, $[K(\beta) : K] = 1$ so $\beta \in K$ too. Hence if g has a root in K, then it splits. □

If K/F and L/K are normal, is L/F normal? Nope. Consider the following:



This will inspire the concept of normal closure. For isntance, the normal closure of $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is $\mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2})$

Definition 22. The normal closure of a finite field extension K/F is a field extension N/K so that N/F is normal and minimal such.

Theorem 11

Let K/F be a finite field extension, then the normal closure exists and is unique, up to isomorphism.

Proof.
Existence:
Let $K = F(\alpha_1, \ldots, \alpha_k)$, take m_i to be the minimal polynomial of α_i over F, and let $f := \prod m_i$. Let N/K be the splitting field of $f \in K[x]$ (notice that we've changed the ground field here). This satisfies minimality, and is normal.
Uniqueness:
Let N'/K be another normal closure of K/F. We have $N' \supset K$ so each m_i has a root implies that it splits over N'. Hence f splits over N'. N/F is the splitting field of S so

$$\begin{tikzcd}
N \arrow[rr, hook, "j"] \arrow[dr, dash] & & N' \arrow[dl, dash] \\
& F &
\end{tikzcd}$$

So $j(N) \subseteq N'$. And as

$$\begin{tikzcd}
N' \arrow[d, dash] \\
j(N) \arrow[d, dash] \arrow[dd, dash, bend left=60, "\text{SF}\rightsquigarrow\text{normal}"] \\
K \arrow[d, dash] \\
F
\end{tikzcd}$$

We must have that $j(N) = N'$ by minimality. $\square$

Definition 23. We say that f is **separable** if it has no repeated roots in its splitting field.

Definition 24. We define the **formal derivative** as follows: It's a map $D : F[x] \to F[x]$ such that

1. $D(f+g) = D(f) + D(g)$
2. $D(fg) = fD(g) + D(f)g$
3. $D(a) = 0$ for all $a \in F$
4. $D(x) = 1$

It's easy to show that there exists only one map with these properties:

$$D(\sum a_i x^i) = na_n x^{n-1} + \cdots + a_1.$$

Lecture 11

Definition 25. Let R be a commutative ring with 1. We say that M is an **R-module** if $(M, +)$ is an abelian group and $R \times M \to M$ with

- $1_R m = m$
- $(r+s)m = rm + sm$
- $(rs)m = r(sm)$
- $r(m+n) = rm + rn$

for all $s, r \in R$ and $m, n \in M$.

Proposition

Let $f \in F[x]$ be irreducible. The following are equivalent:

(a) f is inseparable

(b) f, Df are not relatively prime

(c) $Df = 0$

(d) char $F = p$ and f is a polynomial in x^p.

Remark

(a)$\longleftrightarrow$(b) even if f is not irreducible.
Irreducible inseparable does not happen in $\mathbb{C}$ (char 0).

Lemma

Let f and g be nonzero polynomials in $F[x]$. The following are equivalent:

(a) There exists a field extension K/F with $\alpha \in K$ a root of both f and g ($(x-\alpha) \mid f, g$ in $K[x]$)

(b) f and g are not relatively prime in $F[x]$.

Proof.
"(a)$\Rightarrow$(b)"
Let m_α be the minimal polynomial of α over F. We have $m_\alpha \mid f, g$ in $F[x]$.
"(b)$\Rightarrow$(a)"
Say f and g have common factor h with $\partial h \geq 1$. Adjoin root α of h and let $K := F(\alpha)$. □

Lemma

Let $f \in F[x]$ be nonzero and its splitting field K/F.

(a) Assume $\alpha \in K$ is a root of f. Then $(x-\alpha)^2 \mid f$ in $K[x]$ if and only if $Df(\alpha) = 0$.

(b) f and Df are not relatively prime if and only if f has a double root in K.

Proof.

(a) in $K[x]$, $(x-\alpha) \mid f$. So $f = (x-\alpha)g$, $Df = g + (x-\alpha)Dg$.

$$Df(\alpha) = 0 \iff g(\alpha) = 0 \iff (x-\alpha) \mid g \iff (x-\alpha)^2 \mid f.$$

(b) f has a double root α if and only if α is a root of Df if and only if f, Df are not relatively prime in $F[x]$.

□

Definition 26. A field F of characteristic p is called **perfect** if it contains the p-th root of every element.
By convention, fields of char 0 are perfect.

Proposition

If F is perfect, then every irreducible polynomial is separable.

Proof. If char $F = 0$, we're done by the proposition.
If char $F = p > 0$ assume, by way of contradiction, that f is irreducible and inseparable. Let $f = a_n x^{np} + \cdots + a_1 x^p + a_0$ (by Prop) For all i take $b_i \in F$ such that $B_i^p = a_i$ (since F is perfect)
$f = b_n^p x^{pn} + \cdots + b_1^p x^p + b_0^p = (b_n x^n + \cdots + b_1 x + b_0)^p$. Therefore f is not irreducible. $\rightarrow\leftarrow$ □

Definition 27. Let K/F be a field extension.

(a) $\alpha \in K$ is **separable over F** if its minimal polynomial m_α over F is separable.

(b) K/F is **separable** if all $\alpha \in K$ are separable over F.

Lemma

Let $L/K/F$ be algebraic extensions. If L/F is separable, then L/K and K/F are also separable.

Proof. □

Definition 28. Let R be a commutative ring with 1. A **derivation** of R is a map $D : R \to R$ with

(1) $D(a+b) = D(a) + D(b)$

(2) $D(ab) = D(a)b + aD(b)$

Example:

- $R = \mathbb{Z}[x]$. $D =$ formal derivative. $D = \dfrac{d}{dx}$.
- Also $D = x\dfrac{d}{dx}$ works: $x\dfrac{d}{dx}(x^2+1) = x(2x+0) = 2x^2$.

Definition 29. Let **Der** R be the set of derivations of R.

Proposition

Der R is an R-module with $(D_1 + D_2)(a) = D_1(a) + D_2(a)$ and $(rD)(a) = r(D(a))$.

Corollary

$D = g\dfrac{d}{dx}$ is a derivative of $\mathbb{Z}[x]$ for all $g \in \mathbb{Z}[x]$

Remark

On $\mathbb{Z}[x]$, these are the ONLY derivations (HW 6).

Definition 30. Let $F \subset K$ be commutative rings with 1. Define $\mathbf{Der}_F K$ to be $\{D \in \mathrm{Der} K : D(a) = 0 \;\forall\; a \in F\}$.
Example:

- $\mathrm{Der}_{\mathbb{Z}}\mathbb{Z}[x] = \{g\dfrac{d}{dx} : \forall g \in \mathbb{Z}[x]\} = \mathrm{Der}\mathbb{Z}[x]$.
- $\mathrm{Der}_{\mathbb{Z}[x]}\mathbb{Z}[x] = \{0\}$

Problem Set 5

Lecture 12

Proposition

Let $K = F(\alpha)$ where α is algebraic over F. Then:

(1) α is separable over F if and only if $\mathrm{Der}_F K = \{0\}$

(2) If α is separable over F, then any derivation D_F of F extends uniquely to a derivation D of K. (i.e. $\exists!\; D \in \mathrm{Der}K \;:\; D|_F = D_F$.)

Proof. □

Proposition

Let K/F be a finite extension and $D \in \mathrm{Der}_F K$. If α is separable over F, then $D(\alpha) = 0$.

Proof. □

Theorem 12

Let K/F be a finite extension.

(1) K/F is separable $\iff$ $\mathrm{Der}_F K = \{0\}$

(2) $K/M/F$. If K/M and M/F are separable, then K/F is separable.

(3) If $K = F(\alpha_1, \ldots, \alpha_n)$ where each α_i is separable over F, then K/F is separable.

Proof. □

Lecture 13

Known Results:
R1: $n > m$. A system of m homogeneous linear equations of n unknowns over K has a nonzero solution.
R2: G is a group. $G = \{g_1, \ldots, g_n\}$. If $g \in G$, then $\{gg_1, \ldots, gg_n\}$.

Theorem 13: Dedekind Lemma

Let G be a group, $\mathbb{F}$ be a field and $\{\chi_i : G \to \mathbb{F}^\times\}_{i=1}^n$ be pairwise distinct group homomorphisms. The $\{\chi_i\}$ are linearly independent over $\mathbb{F}$.

Corollary

Let K, L be fields. Any finite set of pairwise distinct field homomorphisms $\overline{\chi_i} : K \to L$ is linearly independent over L.

Theorem 14

Let K be a filed and $G \leq \mathrm{Aut}K$ be a finite subgroup. Then $[K : K^G] = |G|$

Corollary

Let K/F be a finite extension, then $|\mathrm{Gal}(K/F)| \leq [K : F]$

Midterm

Lecture 14

Theorem 15

Let N/F be a finite normal extension $N/K/F$. Suppose $\tau : K \hookrightarrow N$ is an F-monomorphism. Then $\exists \sigma \in \mathrm{Aut}_F(N)$ such that $\sigma|_K = \tau$.

$$\begin{tikzcd}
N \arrow[r, dotted, "\sigma"] \arrow[d, dash] & N \arrow[d, dash] \\
K \arrow[r, hook, "\tau"] \arrow[d, dash] & \tau(K) \arrow[d, dash] \\
F \arrow[r, "\mathrm{id}"] & F
\end{tikzcd}$$

Proof. Let N/F be a finite and normal extension. Then it is a splitting field for some $f \in F[x]$. So

- N/K is the splitting field of $f \in K[x]$
- $N/\tau(K)$ is the splitting field of $\tau f \in \tau K[x]$

Result follows from lemma about splitting fields. □

Corollary

Let N/F be a finite normal extension, $f \in F[x]$ be irreducible with two of its roots $\alpha_1, \alpha_2 \in N$. Then there exists $\sigma \in \mathrm{Aut}_F N$ such that $\sigma(\alpha_1) = \alpha_2$.

Proof. We know that there exists τ such that

$$\begin{tikzcd}
F(\alpha_1) \arrow[rr, "\alpha_1 \mapsto \alpha_2"] \arrow[dr, dash] & & F(\alpha_2) \arrow[dl, dash] \\
& F &
\end{tikzcd}$$

So by theorem we have

$$\begin{tikzcd}
N \arrow[r, dotted, "\sigma"] \arrow[d, dash] & N \arrow[d, dash] \\
K = F(\alpha_1) \arrow[r, hook, "\tau"] \arrow[d, dash] & \tau(K) = F(\alpha_2) \arrow[d, dash] \\
F \arrow[r, "\mathrm{id}"] & F
\end{tikzcd}$$

So there exists σ such that $\sigma|_K = \tau$. □

Examples:

- $f \in \mathbb{Q}(x)$, $f = x^3 - 2$ is irreducible. Let $N/\mathbb{Q}$ be the splitting field. So $N = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$. We know that $G = \mathrm{Gal}(N/\mathbb{Q}) \simeq S_3$
  Elements sending:
  - $\alpha_1 \to \alpha_2$: $(12), (123)$
  - $\alpha_1 \to \alpha_1$: $1, (23)$
  - $\alpha_1 \to \alpha_3$: $(13), (132)$

  G is transitive on $\{\alpha_1, \alpha_2, \alpha_3\}$
  Two elements carry α_1 to α_i for any i.
- $f = (x^2 - 2)(x^2 + 1) \in \mathbb{Q}[x]$. Roots: $\sqrt{2}, -\sqrt{2}, i, -i$. Let $N/\mathbb{Q}$ be the splitting field over f. We know that $G = \mathrm{Gal}(N/\mathbb{Q}) \simeq Z_2 \times Z_2 = \langle \sigma, \tau \rangle$ where $\sigma = (12)$ and $\tau = (34)$. G is not transitive on roots of f.
- Same setting but write $\mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(\beta_1)$ where $\beta_1 = i + \sqrt{2}$. We've shown that $m_{\beta_1} = x^4 + 2x^2 + 9$. We have $\sigma(\beta_1) = i - \sqrt{2}$, $\tau(\beta_1) = -i + \sqrt{2}$, and $\sigma\tau(\beta_1) = -i - \sqrt{2}$. They must be roots of m_{β_1}. Note that G is transitive on roots of m_{β_1}. The Galois group is $\{(12)(34), (13)(24), (14)(23), 1\}$.

Let K/F be a finite extension. We know that $|\mathrm{Gal}(K/F)| \leq [K : F]$. When does equality occur?

Theorem 16

$M/N/K/F$. If K/F is finite, N/K its normal closure. Then any F-morphism $K \xrightarrow{\tau} M$ actually lands in N.

Proof. Let $\alpha \in K$ and m be its minimal polynomial over F. $\tau(\alpha)$ is a root of m. m splits over N, thus $\tau(\alpha) \in N$. □

Theorem 17

Let K/F be a separable extension. And $[K : F] = n < \infty$, $N/K/F$ with N/F normal. There are exactly n distinct F-monomorphisms from K to N.

We look at the following example before proving the theorem. Example:
$F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt[3]{2})$.

- How many F-monomorphisms $K \to K$? 1.

Let $N = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$

- How many F-monomorphisms $K \to N$? 3.
- How many F-monomorphisms $N \to N$? 6.

Proof. We'll do induction on $n = [K : F]$. Let $n = 1$. We have $K = F$ so one F-monomorphism $K \to N$.
Let $n > 1$. Take $\alpha \in K \setminus F$. Say α is degree d over F. The minimal polynomial of α over F has roots $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_d \in N$ all distinct because K/F is separable.

$$\begin{tikzcd}
N \arrow[d, dash] \\
K \arrow[d, dash, "n/d"'] \\
F(\alpha_1) \arrow[d, dash, "d"'] \\
F
\end{tikzcd}$$

By strong induction there are exactly n/d distinct $F(\alpha_1)$-monomorphisms $K \to N$. Call them $\rho_1, \ldots, \rho_{n/d}$.
We know that for all i there exists $\tau_i \in \mathrm{Aut}_F N$ such that $\tau_i(\alpha_1) = \alpha_i$. Take $\{\tau_i \rho_j | j \in \{1, \ldots, d\}, j \in \{1, \ldots, n/d\}\}$ these do the job. Just check they're distinct and we have them all. □

Lecture 15

Theorem 18

A finite extension K/F is Galois if and only if it is normal and separable.

Proof. "$\Leftarrow$" Apply theorem from last time with $N = K$ to get $|\mathrm{Aut}_F K| = [K : F]$.
"$\Rightarrow$" Assumption: K/F is Galois. This implies that $K^G = F$. We'll show that for all $\alpha \in K$, m_α has all roots in K and is separable. Let $G\alpha = \{\underset{\text{pairwise distinct}}{\alpha = \alpha_1, \alpha_2, \ldots, \alpha_l}\}$ (orbit of α under G). Let $f(x) = (x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_l) \in K[x]$. Since G permutes roots of f, we have $f \in K^G[x] = F[x]$.
Claim: f is the minimal polynomial of α over F.

- f is monic and has α as a root.

- If $g \in F[x]$ with α as a root. G fixes g so $\alpha_1, \ldots, \alpha_l$ are all roots of g. Thus $\partial g \geq \partial f$.

$f = m_\alpha$ is separable by construction and all its roots are in K. □

What if you make f in the extension K/F that is

1) Not normal? eg $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, $G = 1$. $G\alpha = \{\alpha\}$, $f = x - \alpha \in K[x] \notin F[x]$.
2) Not separable? $\mathbb{F}_2(t) = F$, α - root of $x^2 - t$. $x^2 + t \in K[x]$. $x^2 + 2 = (x + \alpha)^2$. $G = 1$.

Example:

- SF $K/\mathbb{Q}$ of $x^4 - 2$. Let $\alpha = \sqrt[4]{2}$, $\beta = \sqrt{2}$.
  What is $G\alpha$? $G\alpha = \{\sqrt[4]{2}, \zeta\sqrt[4]{2}, \zeta^3\sqrt[4]{2}, -\sqrt[4]{2}\}$. $x^4 - 2$ is irreducible so Gal is transitive on the roots.
  $G\beta = \{\sqrt{2}, -\sqrt{2}\}$.

Corollary

$K/M/F$. If K/F is finite and Galois, then K/M is finite and Galois. (M/F might not be.)

Corollary

If K/F is finite and separable, then $\exists N : N/K/F$ such that N/F is finite and Galois.

Let K/F be a finite Galois extension with Galois group G. $f \in F[x]$ with roots $\alpha_1, \ldots, \alpha_n \in K$.

(1) $\forall i$, $\sigma \in G$ we have $\sigma(\alpha_i) = \alpha_j$ for some j.

(2) If f is irreducible, then $\forall i, j\ \exists \sigma \in G :\ \sigma(\alpha_i) = \alpha_j$.

(3) If K/F is the splitting field of f ($K = F(\alpha_1, \ldots, \alpha_n)$) then the action is faithful (i.e. if $\sigma(\alpha_i) = \alpha_i \forall i \ \Rightarrow \sigma = id$).

Lecture 16

Recap: Finite K/F is Galois if and only if it is normal and separable. Let $M = K^H$ for some $K \leq H$. We know K/K^H is Galois with Galois group H. We also have that K^H/F is Galois if and only if H is normal in G. (GJEJE SIMBOLIN PER NORMAL). Moreover, in such a case $\text{Gal}(K^H/F) \simeq G/H$.

Proposition

Let K/F be a finite Galois extension with Galois group G and let $\tau \in G$. Let M be an intermediate field corresponding to $H \leq G$. Then τM corresponds to $\tau H \tau^{-1}$

Proof. Define H' to be the group corresponding to τM. We know from the fundamental theorem of Galois theory that $|H'| = [K : \tau M] = [K : M] = |H| < \infty$. We claim that $\tau H \tau^{-1} \subset H'$. Take $\tau\sigma\tau^{-1} \in \tau H \tau^{-1}$ (where $\sigma \in H$). We want to show that $\tau\sigma\tau^{-1} \subset H = \text{Gal}(K/\tau M)$ (i.e. $\tau\sigma\tau^{-1}$ fixes τM). Take $\tau x \in \tau M$ (where $x \in M$) and we have $\tau\sigma\tau^{-1}(\tau x) = \tau\sigma x = \tau x$ since σ fixes M. So we have that $\tau H \tau^{-1}$ fixes τM hence we're done. □

We now prove that K^H/F is Galois if and only if H is normal in G.

Proof.

"⇒" Suppose K^H/F is Galois. We have that K^H/F is the splitting field of some polynomial $f \in F[x]$. If $\sigma \in G$, it permutes the roots of f. Thus $\sigma K^H = K^H$. By the proposition above we have that $\sigma H \sigma^{-1} = H$ for all $\sigma \in G$ so H is normal in G.

"⇐" Assume H is normal in G, the for all $\tau \in G$, $\tau H \tau^{-1} = H$. So $\tau K^H = K^H$ for all $\tau \in G$ by the proposition above. So $\pi : G \to \text{Gal}(K^H/F)$ via $\tau \mapsto \tau|_{K^H}$ thus $\ker \pi = \{\tau \in G : \tau \text{ fixes } K^H\} = H$. So $G/H \hookrightarrow \text{Gal}(K^H/F)$ by isomorphism theorems. $|\text{Gal}(K^H/F)| \leq [K^H : F] = |G|/|H| = |G/H|$. Hence $G/H \xrightarrow{\sim} \text{Gal}(K^H/F)$.

□

Lecture 17

---

350 Reminder

G is **solvable** if there exists a chain of subgroups

$$G_r = G \triangleright G_{r-1} \triangleright \cdots \triangleright G_1 \triangleright G_0 = 1$$

with G_{i+1}/G_i abelian for all i.

Theorem 19

(a) If G is solvable, then all subgroups and quotient groups are solvable.

(b) If $N \triangleleft G$ and $G/N \& N$ are solvable, then G is solvable.

Theorem 20: Theorem of the Primitive Element

K/F is a finite extension within $\mathbb{C}$, then $\exists z \in K : \; F(z) = K$.

From now on, we will work in $\mathbb{C}$.

Solving Polynomials by Radicals

- deg 1: Nothing to be done.
- deg 2: $ax^2 + bx + c = 0 \rightsquigarrow x_{1/2} = \dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}$.
- deg 3: We have a formula. It's long.
- deg 4: We have a formula. It's even longer.

Theorem 21

$F \subset \mathbb{C}$ we have $f \in F[x]$ is solvable by radicals if and only if its Galois group is solvable.

- Solvable groups:

- S_1 is abelian - so solvable.
- S_2 is abelian - so solvable.
- $G = S_3$, we have $S_3 \underset{Z_2}{\triangleright} A_3 \underset{Z_3}{\triangleright} 1$.
- $S_4 \underset{Z_2}{\triangleright} A_4 \underset{Z_3}{\triangleright} G_2 \underset{Z_2}{\triangleright} G_1 \underset{Z_2}{\triangleright} 1$. Where $G_2 = \{(\cdot\cdot)(\cdot\cdot)\}$ and $G_1 = \langle(\cdot\cdot)(\cdot\cdot)\rangle$. So S_4 is solvable.
- We know from 350 that A_5 is simple and A_5 is not abelian. Thus A_5 is not solvable. Therefore S_4 is not solvable.

Now let's produce $f \in \mathbb{Q}[x]$ with Galois group S_5. Assuming the theorem above, this would mean that there exists a polynomial whose roots cannot be found by radicals. We claim that $f = x^5 + x^3 - 8x + 1$.

(1) f is irreducible (non-trivial but annoying).

(2) f has exactly 3 real roots.
Complex conjugation swaps roots 4 and 5 so G contains a transposition (45). Since $G \subset S_5$ is transitive on the roots and contains a transposition, we have that $G = S_5$.

Lecture 18

Definition 31. Let K be a field. Its **primesubfield** is said to be $K_0 := \bigcap_{F \text{ subfield}} F$.

Claim: $K_0 \simeq \mathbb{Q}$ or $\mathbb{Z}/p\mathbb{Z}$.
Claim: If K/F is a field extension, then $\mathrm{char} K = \mathrm{char} F$.

Lemma

Let G be a p-group, then there exists $H \leq G$ such that $[G : H] = p$. (In fact, H can be chosen to be normal).

Proof. We proceed by induction on n where $|G| = p^n$. □

Finite Fields

We will begin the study of finite fields and their extensions. Our main result for now will be the following:

Theorem 22: Finite Fields Theorem

Let p be a positive prime integer, $r \in \mathbb{N}$ and $q = p^r$.

(a) There exists a field $\mathbb{F}_q$ of order $|\mathbb{F}_q| = q$.

(b) Every field of order q is isomorphic to $\mathbb{F}_q$.

(c) $\mathbb{F}_q^\times \simeq Z_{q-1}$

(d) Elements of $\mathbb{F}_q$ are roots of $x^q - x$.

(e) In $\mathbb{F}_p[x]$, the monic irreducible factors of $x^q - x$ are precisely the irreducible monic polynomials whose degree divides r. (In particular, all degree r irreducible polynomials divide $x^q - x$.)

(f) $\mathbb{F}_q$ contains a copy of $\mathbb{F}_{p^k}$ if and only if k divides r.

We'll demonstrate this result in the following example: $p = 2$, $r = 2$, $q = p^r = 2^2$.

(a) $\mathbb{F}_{2^2} = \mathbb{F}_2(\alpha)$ where α is a root of $x^2 + x + 1$. So $\mathbb{F}_{2^2} = \{0, 1, \alpha, \alpha + 1\}$

(b) $|K| = 4 \Rightarrow K/\mathbb{F}_2$ so $[K : \mathbb{F}_2] = 2$. Take $\beta \in K \setminus \mathbb{F}_2$ then $K \simeq \mathbb{F}_2(\beta)$ and β is a root of $x^2 + x + 1$. We have

$$\begin{tikzcd}
\mathbb{F}_2(\beta) \arrow[rr, dash, "\simeq"] \arrow[dr, dash] & & \mathbb{F}_2(\alpha) \arrow[dl, dash] \\
& \mathbb{F}_2 &
\end{tikzcd}$$

(c) $\mathbb{F}_{2^2}^\times = \{1, \alpha, \alpha^2 = \alpha + 1\}$

(d) Say α is a root of $x^2 + x + 1$. We claim that $\alpha + 1$ is a root too. $(\alpha + 1)^2 + (\alpha + 1) + 1 = \alpha^2 + 1 + \alpha + 1 + 1 = 0$.

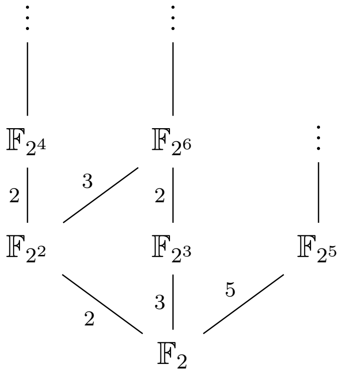
(e) $x^4 - x = x(x^3 - 1) = x(x-1)(x^2 + x + 1)$

(f) Need a bigger field to illustrate this.

More on $(d), (e), (f)$:

- $\mathbb{F}_2 :\ x^2 - x = x(x+1)$
- $\mathbb{F}_{2^2} :\ x^4 - x = x(x+1)(x^2+x+1)$
- $\mathbb{F}_{2^8} :\ x^8 - x = x(x^7 - 1) = x(x+1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1) = x(x+1)(x^3 + x^2 + 1)(x^3 + x + 1)$.
- $\mathbb{F}_{2^4} :\ x^{2^k} - x = x(x+1)(x^2+x+1)\ \underbrace{(\cdots)(\cdots)(\cdots)}_{\text{3 deg 4 irred polynomials}}$

In general we have a tree of field extensions as follows:



We may use (e) to compute the number of irreducible polynomials over $\mathbb{F}_2$.

- Degree 1: 2
- Degree 2: 1
- Degree 3: 2
- Degree 4: 3
- Degree 5: 6
- Degree 6: 9
- Degree 7: 18
- Degree 8: 30
- Degree 9: 56
- Degree 10: 99

Lecture 19

Warm-up: Prove that $(x+y)^{p^r} = x^{p^r} + y^{p^r}$ in characteristic p. (Just induct on r).
We will now prove the Finite Field Theorem from the previous lecture.

Proof.

(d) If K is a field with $|K| = q = p^r$. As $|K^\times| = q-1$ so if $\alpha \in K$ then $|\alpha| \mid q-1$ thus $\alpha^{q-1} = 1 \Rightarrow \alpha^q = \alpha$ $(\alpha \neq 0)$. If $\alpha = 0$, then $\alpha^q = \alpha$.

(c) If K is a field of order q we have $\alpha^{q-1} = 1$ for all $\alpha \in K^\times$. Since $K^\times$ is a finite abelian group, so $K^\times = Z_{d_1} \times Z_{d_2} \times \cdots \times Z_{d_s}$ where $d_s \mid d_{s-1} \mid \cdots \mid d_1$. Because of this decomposition we actually get that $\alpha^{d_1} = 1$ for all $\alpha \in K^\times$. However $x^{d_1} = 1$ has at most d_1 solutions in K (field), therefore $d_1 = q-1$.

(a) Take $L/\mathbb{F}_p$ to be the splitting field of $x^q - x$. Let $K \subset L$ be a subset $K = \{\alpha \in L : \alpha^q - \alpha = 0\}$. We want to show that K is a field. $|K| = q$ because $\gcd(x^q - x, (x^q - x)') = 1$. Suppose $\alpha, \beta \in K$ with $\alpha^q = \alpha$, $\beta^q = \beta$. We want $(-\alpha)^q = -\alpha$ and $(\alpha\beta)^q = \alpha\beta$. Like this we get K is a field. Let $\mathbb{F}_q := K$ (note that $\mathbb{F}_q/\mathbb{F}_p$ is the splitting field of $x^q - x$).

(b) Take $|K| = q$, we want to show that $K \simeq \mathbb{F}_q$. From (c) we have $K^\times = Z_{q-1}$ take a generator α of $K^\times$. Let m_α be the minimal polynomial over $\mathbb{F}_p$. So $K = \mathbb{F}_p(\alpha)$. From (d) α is a root of $x^q - x$ hence $m_\alpha \mid x^q - x$. Since $\mathbb{F}_q/\mathbb{F}_p$ is the SF of $x^q - x$ there exists $\beta \in \mathbb{F}_q$ that is a root of m_α. $K = \mathbb{F}_p(\alpha) = \mathbb{F}_p[x]/(m_\alpha) \simeq \mathbb{F}_p(\beta) \subset \mathbb{F}_q$. Since $|K| = |\mathbb{F}_q| \Rightarrow K \simeq \mathbb{F}_q$.

(e) Let $f \in \mathbb{F}_p[x]$ be a monic irreducible polynomial of degree d. Attach a root α:

$$\begin{tikzcd}
\mathbb{F}_p(\alpha) \arrow[rr, "\simeq"] \arrow[dr, dash] & & \mathbb{F}_{p^\alpha} \arrow[dl, dash] \\
& \mathbb{F}_p &
\end{tikzcd}$$

So α satisfies $x^{p^d} - x = 0$. Hence $f \mid x^{p^d} - x$.

Lemma

$x^{p^i} - x \mid x^{p^{ij}} - x$ for all $i, j \in \mathbb{N}$.

Proof. We know that $x^r - 1 \mid x^s - 1$ if $r \mid s$. We use this repeatedly:

$$p^i - 1 \mid p^{ij} - 1$$

$$x^{p^i - 1} - 1 \mid x^{p^{ij} - 1} - 1$$

Multiply by x and get

$$x^{p^i} - x \mid x^{p^{ij}} - x.$$

□

So if $f \in \mathbb{F}_p[x]$ be an irreducible degree $d \mid r \Rightarrow f \mid x^{p^d} - x \mid x^{p^r} - x$. We have $x^{p^r} - x$ is separable so for all $d \mid r$ every irreducible polynomial $f \in \mathbb{F}_p[x]$ of degree d appear exactly once in the irreducible factorization of $x^{p^r} - x \in \mathbb{F}_p[x]$.
If $g \in \mathbb{F}_p[x]$ is irreducible polynomial of degree e and $g \mid x^{p^r} - x$ WTS $e \mid r$. $x^{p^r} - x$ splits in $\mathbb{F}_q[x]$ thus $\exists \alpha \in \mathbb{F}_q$ root of g. From the tower law we have $e \mid r$.

□

Definition 32. Let R be a commutative ring of characteristic p. The map $\psi : R \to R$ via $x \mapsto x^p$ is called the **Frobenius map**.

Lemma

ψ is a ring homomorphism.

There's some nice properties of this map that we'll see soon enough.

Lecture 20

Warm-up: K/M and M/F are _______ if and only if K/F is _______

1. Finite ✓
2. Algebraic ✓
3. Normal ✗
4. Finite separable ✓
5. Finite Galois ✗

Warm-up 2: Verify the following equivalent definitions.

Definition 33. A field F is **algebraically closed** if the following equivalent statements are true.

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

(b) Every irreducible polynomial $f \in F[x]$ has a root in F

(c) All irreducible polynomials in $F[x]$ are linear.

(d) Every nontrivial extension K/F consists a purely transcendental extension.

(e) Every algebraic extension K/F is trivial.

Theorem 23

$\mathbb{C}$ is algebraically closed.

Claim 1: If $f \in \mathbb{R}[x]$ is monic and has odd degree then it has a real root.
Consequence: $\mathbb{R}$ has no nontrivial extensions of odd degree.
Claim 2: Every quadratic polynomial over $\mathbb{C}$ splits.
Consequence: $\mathbb{C}$ has no degree 2 extension.
We now prove the theorem.

Proof. Suppose $\mathbb{C}$ is not algebraically closed, then there exists $f \in \mathbb{C}[x]$ irreducible such that $\partial f > 1$. Attach a root of f say α to get $K = \mathbb{C}(\alpha)$. Take the normal closure N/K of $K/\mathbb{R}$. We have that $N/\mathbb{R}$ is finite, normal, separable, so it must be Galois. Let $G = \mathrm{Gal}(N/\mathbb{R})$

$$\begin{tikzcd}
N \arrow[d, dash] \\
K \arrow[d, dash] \\
\mathbb{C} \arrow[d, dash, "2"'] \\
\mathbb{R}
\end{tikzcd}$$

Since $2 \mid [N : \mathbb{R}]$, we have $2 \mid |G|$. So G has a Sylow 2-subgroup H.

$$\begin{tikzcd}
N \arrow[dd, dash, "|G|"'] \arrow[dr, dash, "|H|"] & \\
& N^H \arrow[dl, dash] \\
\mathbb{R} &
\end{tikzcd}$$

We have that $[N^H : \mathbb{R}]$ is odd. By claim 1, we have $[N^H : \mathbb{R}] = 1$ thus $H = G$. Therefore

$$\begin{tikzcd}
N \arrow[d, dash] \arrow[dd, dash, bend left, "2^n"] \\
K \arrow[d, dash] \\
\mathbb{C}
\end{tikzcd}$$

So $[N : \mathbb{C}] = 2^n$ for $n \in \mathbb{N}$.
$N/\mathbb{C}$ is Galois, group G'. G' has an index 2 subgroup H'.

$$\begin{tikzcd}
N \arrow[dd, dash, "2^n"'] \arrow[dr, dash, "2^{n-1}"] & \\
& N^{H'} \arrow[dl, dash, "2"'] \\
\mathbb{C} &
\end{tikzcd}$$

$[N^{H'} : \mathbb{C}] = 2$. Which is a contradiction. □

Definition 34. Let F be a field. The **algebraic closure** of F is a field extension $\overline{F}/F$ such that

(1) $\overline{F}$ is algebraically closed

(2) $\overline{F}/F$ is algebraic

Theorem 24

Every field F has algebraic closure, unique up to isomorphism.

Lemma

K is algebraically closed, if $F \subset K$ is a subfield then $\overline{F} = \{x \in K : x \text{ is algebraic over } F\}$ is the algebraic closure of F.

Claim: If $K/\mathbb{Q}$ is a Galois extension of degree 2^n, then any $\alpha \in K$ is constructible.
Let p be a prime, we know that if a p-gon is constructible, then $p = 2^n + 1$. If p is a prime of the form $2^n + 1$, we know $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = 2^n$ and $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is Galois. So everything in $\mathbb{Q}(\zeta_p)$ is constructible.
Fermat numbers are numbers of the form $F_k = 2^{2^k} + 1$. If you look at the first few you notice $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$ are all primes. Fermat conjectured that all Fermat numbers are primes, that's not true at all. For instance, $F_5 = 641 \cdot 6700417$.
Conjecture: F_i for all $i > 4$ are composite.

Theorem 25

The regular n-gon is constructible if and only if $n = 2^r F_{k_1} F_{k_2} \dots F_{k_r}$ where F_{k_i} are distinct Fermat primes.

Lecture 21

Definition 35. A **primitive n-th root** of 1 (in $\mathbb{C}$) is $\zeta_n \in \mathbb{C}$ with

(1) $\zeta_n^n = 1$

(2) $\zeta_n^d \neq 1$ for all d such that $0 < d < n$.

Definition 36. The ***n*-th cyclotomic field** is $\mathbb{Q}(\zeta_n) \subset \mathbb{C}$.
$\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is the splitting field of $x^n - 1$ so it is Galois. Let $G_n = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. We return to $G_n \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$. We crucially have to answer the question: do ζ_n and ζ_n^a share the same minimal polynomial?

- If $(a, n) \neq 1$, NO.
- If $(a, n) = 1$, yes.

When n is prime this stuff is pretty easy. The only non-trivial thing you have to remember here is the following:

Theorem 26

$$x^n - 1 = \prod_{d|n} \Phi_d$$

Symmetric Polynomials

Take a polynomial ring $R[x_1, x_2, \ldots, x_n]$. S_n acts on it via $\sigma : x_i \to x_{\sigma(i)}$. So, for example, $(12)x_1x_3^2 = x_2x_3^2$. We say that a polynomial is **symmetric** if $\sigma f = f$ for all $\sigma \in S_n$. We denote the set of symmetric polynomials as $R[x_1, x_2, \ldots, x_n]^{S_n}$.
We define **elementary symmetric polynomials** $s_k = \sum\limits_{i_1<\cdots<i_k} x_{i_1}x_{i_2}\ldots x_{i_k} \in R[x_1, \ldots, x_n]$.
For example, in the $n = 3$ case we have $s_1 = x_1 + x_2 + x_3$, $s_2 = x_1x_2 + x_2x_3 + x_3x_1$, and $s_3 = x_1x_2x_3$.

Theorem 27

$$R[x_1, \ldots, x_n]^{S_n} = R[s_1, \ldots, s_n]$$

Let $f = \prod\limits_{1\leq i\leq n} (x - \alpha_i) = x^n - s_1x^{n-1} + \cdots + (-1)^n s_n$. Recall that $\triangle$ is symmetric ($\triangle = \prod_{i<j}(\alpha_i - \alpha_j)^2$)

Lecture 22

Theorem 28: T

e extension $\mathbb{Q}(x_1, \ldots, x_n)/\mathbb{Q}(s_1, \ldots, s_n)$ has Galois group S_n.

As consequence of this we get that for any finite group G there exists a Galois extension K/F with Galois group G.