GALOIS THEORY (2012, M24) NOTES

TERUYOSHI YOSHIDA

CONTENTS

Date: January 12, 2013.

Note: §3.4 and the Appendices are not examinable.

INTRO 1: CUBICS, QUARTICS

Lecture 1 (4 Oct, Th.)

Quadratics.

(1) $X^2 + b = 0 \Longrightarrow X = \pm\sqrt{-b}$.

(2) $X^2 - aX + b = (X - \alpha)(X - \beta) = 0$.

Note $a = \alpha + \beta,\ b = \alpha\beta$. We reduce to (1) i.e. the case $a = 0$. Set:

$$\alpha' := \alpha - \frac{a}{2}, \quad \beta' := \beta - \frac{a}{2}.$$

Then:
$$\alpha' + \beta' = 0, \qquad \alpha'\beta' = \alpha\beta - \frac{a}{2}(\alpha + \beta) + \frac{a^2}{4}$$
$$= b - \frac{a^2}{2} + \frac{a^2}{4} = b - \frac{a^2}{4},$$

hence α', β' are roots of $X^2 + \left(b - \dfrac{a^2}{4}\right) = 0$, i.e. $\pm\sqrt{\dfrac{a^2}{4} - b}$ by (1). Thus $\alpha, \beta = \dfrac{a}{2} \pm \sqrt{\dfrac{a^2}{4} - b}$.

Cubics.

(3) $X^3 - c = 0 \Longrightarrow X = \sqrt[3]{c}, \sqrt[3]{c}\zeta, \sqrt[3]{c}\zeta^2$,

where $1, \zeta, \zeta^2$ are the roots of $X^3 - 1 = 0$. As $X^3 - 1 = (X - 1)(X^2 + X + 1)$, we have $\zeta, \zeta^2 = -\dfrac{1}{2} \pm \sqrt{-\dfrac{3}{4}}$ by (2). [If one is ζ then the other is ζ^2. Note $\zeta^2 + \zeta + 1 = 0$.]

(4) $X^3 + bX - c = (X - \alpha)(X - \beta)(X - \gamma) = 0$. By expanding:

$$0 = \alpha + \beta + \gamma, \quad b = \alpha\beta + \beta\gamma + \gamma\alpha, \quad c = \alpha\beta\gamma.$$

The *Lagrange resolvents* of this cubic are defined as:

$$x := \alpha + \beta\zeta + \gamma\zeta^2, \quad x\zeta = \alpha\zeta + \beta\zeta^2 + \gamma, \quad x\zeta^2 = \alpha\zeta^2 + \beta + \gamma\zeta$$
$$y := \alpha + \beta\zeta^2 + \gamma\zeta, \quad y\zeta = \alpha\zeta + \beta + \gamma\zeta^2, \quad y\zeta^2 = \alpha\zeta^2 + \beta\zeta + \gamma.$$

By (3), the first row gives the roots of $X^3 - x^3 = 0$, second $X^3 - y^3 = 0$. Using $\zeta^2 + \zeta + 1 = 0$ and adding these expressions (remember $\alpha + \beta + \gamma = 0$), we get

$$x + y = 3\alpha, \quad x\zeta^2 + y\zeta = 3\beta, \quad x\zeta + y\zeta^2 = 3\gamma,$$

hence

$$(\alpha,\beta,\gamma)=\Big(\frac{x+y}{3},\frac{x\zeta^2+y\zeta}{3},\frac{x\zeta+y\zeta^2}{3}\Big).$$

Now by (note $\zeta\cdot\zeta^2=1$ and $\zeta^2+\zeta+1=0$)

$$\begin{aligned}xy&=\alpha^2+\beta^2+\gamma^2-\alpha\beta-\beta\gamma-\gamma\alpha\\&=(\alpha+\beta+\gamma)^2-3b=-3b,\end{aligned}$$

x,y determine each other. Also,

$$\begin{aligned}x^3+y^3&=(x+y)(x+y\zeta)(x+y\zeta^2)\\&=(x+y)(x\zeta+y\zeta^2)(x\zeta^2+y\zeta)=3\alpha\cdot3\beta\cdot3\gamma=27c\\x^3y^3&=-27b^3\end{aligned}$$

shows that x^3,y^3 are the two roots of $X^2-27cX-27b^3=0$, solved in (2).

(5) $X^3-aX^2+bX-c=(X-\alpha)(X-\beta)(X-\gamma)=0$.

Reduced to (4), i.e. the case $a=0$ as before, by setting

$$\alpha':=\alpha-\frac{a}{3},\quad \beta':=\beta-\frac{a}{3},\quad \gamma':=\gamma-\frac{a}{3}.$$

A computation (exercise) shows that α',β',γ' are the three roots of

$$X^3+\Big(b-\frac{a^2}{3}\Big)X-\Big(\frac{2}{27}a^3-\frac{ab}{3}+c\Big)=0,$$

solved in (4). We get α,β,γ by adding $\dfrac{a}{3}$ to them.

Quartics.

(6) $X^4-aX^3+bX^2-cX+d=(X-\alpha)(X-\beta)(X-\gamma)(X-\delta)=0$.

Similarly we subtract $\dfrac{a}{4}$ from $\alpha,\beta,\gamma,\delta$ and assume $a=\alpha+\beta+\gamma+\delta=0$.

Now we will reduce to (5). Let:

$$x:=\alpha+\beta=-(\gamma+\delta),\quad y:=\alpha+\gamma=-(\beta+\delta),\quad z:=\alpha+\delta=-(\beta+\gamma).$$

Then we have

$$(\alpha,\beta,\gamma,\delta)=\Big(\frac{x+y+z}{2},\frac{x-y-z}{2},\frac{-x+y-z}{2},\frac{-x-y+z}{2}\Big).$$

hence it suffices to find x,y,z. First note:

$$\begin{aligned}xyz&=(\alpha+\beta)(\alpha+\gamma)(\alpha+\delta)\\&=\alpha^3+(\beta+\gamma+\delta)\alpha^2+(\beta\gamma+\gamma\delta+\delta\beta)\alpha+\beta\gamma\delta\\&=(\alpha+\beta+\gamma+\delta)\alpha^2+(\beta\gamma\alpha+\gamma\delta\alpha+\delta\beta\alpha+\beta\gamma\delta)=c.\end{aligned}$$

As

$$x^2=-(\alpha+\beta)(\gamma+\delta),\quad y^2=-(\alpha+\gamma)(\beta+\delta),\quad z^2=-(\alpha+\delta)(\beta+\gamma),$$

we have

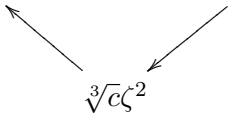
$$x^2+y^2+z^2 = -2(\alpha\beta+\alpha\gamma+\alpha\delta+\beta\gamma+\gamma\delta+\gamma\delta) = -2b,$$
$$x^2y^2+y^2z^2+z^2x^2 = b^2-4d \quad \text{(exercise)},$$
$$x^2y^2z^2 = c^2 \quad \text{(above)}.$$

Hence x^2, y^2, z^2 are roots of the *resolvent cubic*:

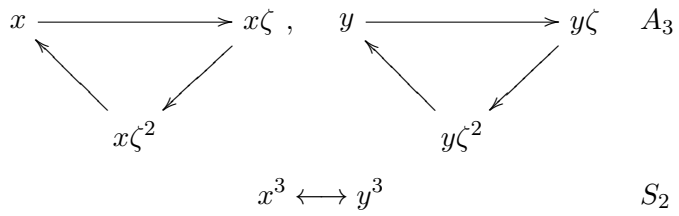
$$X^3+2bX^2+(b^2-4d)X-c^2=0,$$

which is solved in (5). Now we get x, y, z by (1). If we choose signs for x, y, then z is determined by $xyz = c$, hence there are 4 choices.

Summary of the symmetries.
(1): $\sqrt{-b} \longleftrightarrow -\sqrt{-b}, \quad S_2 = C_2.$
(1)⇒(2): rational $(+,-,\times,\div)$.
(3): $\sqrt[3]{c} \longrightarrow \sqrt[3]{c}\zeta$, $\quad A_3 = C_3.$



(4): Note $S_3 \rhd A_3$ (normal subgroup) and $S_3/A_3 \cong S_2$:



(4)⇒(5): rational $(+,-,\times,\div)$.
(6): $S_4 \curvearrowright \{\alpha,\beta,\gamma,\delta\}$ (group acting by permutation); this induces $S_4 \twoheadrightarrow S_3 \curvearrowright \{x^2,y^2,z^2\}$. The kernel of this surjective homomorphism $S_4 \twoheadrightarrow S_3$ is:

$$\begin{aligned} S_4 &\rhd \{\text{permutations of } \alpha,\beta,\gamma,\delta \text{ fixing each of } x^2,y^2,z^2\} \\ &= \{\mathrm{id}, (\alpha\ \beta)(\gamma\ \delta), (\alpha\ \gamma)(\beta\ \delta), (\alpha\ \delta)(\beta\ \gamma)\} \\ &= V_4 \cong C_2 \times C_2, \end{aligned}$$

i.e. $S_4 \rhd V_4$ and $S_4/V_4 \cong S_3$. Note that

$$\begin{aligned} V_4 &= \{x \leftrightarrow -x,\ y \leftrightarrow -y,\ z \leftrightarrow -z \mid \text{change signs of } x,y,z \text{ but not of } xyz\} \\ &\curvearrowright \{\pm x, \pm y, \pm z\}. \end{aligned}$$

Recall: *Field* = a set closed under $+,-,\times,\div$.

(i) Rational operations $(+, -, \times, \div)$ occur within the same field ((1)⇒(2), (4)⇒(5)).

(ii) But whenever the field has changed (been extended), an *additional symmetry* (will be called *Galois groups*) was introduced ((1),(3),(4),(6)).

- Galois' insight— ignore (i), and keep track of (ii).

- We exploited the *subgroups* $\longleftrightarrow$ "partially" symmetric polynomials of the roots.
- S_5 (or S_n for $n \geq 5$) has no proper normal subgroups other than A_5 (or A_n) which is simple, so similar reduction seems impossible.

INTRO 2: CIRCLES

Lecture 2 (6 Oct, Sa.)

(a) *Abstract = Intuitive.* By a *circle*, we mean:

(Euclid, BC 300) P: centre, r: radius, $C := \{Q \in \text{plane} \mid |PQ| = r\}$.

(Descartes, 17c) $C := \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = r^2\}$. $\cdots (*)$

(Galois/Lie, 19c) A set on which the following group acts:

$$\mathbb{R}/2\pi\mathbb{Z} \cong \left\{ \begin{array}{c} T_\theta : \textit{rotation of angle } \theta, s.t. \\ \text{(i) } T_0 = \mathrm{id}, \ \text{(ii) } T_{\theta'} \circ T_\theta = T_{\theta'+\theta}, \\ \text{(iii) } T_\theta = T_{\theta'} \iff \theta - \theta' \in 2\pi\mathbb{Z} \end{array} \right\} \qquad \cdots (\star)$$

— captures the essence of "circular" shapes of cylinders, cones, wine glasses...

(b) *Dictionaries.* Intuitions $\longleftrightarrow$ Manipulating symbols

Geometry		Algebra		Groups
$\lvert PQ\rvert = r$	$\overset{\text{Pythagoras}}{\longleftrightarrow}$	$r = \sqrt{x^2 + y^2}$	$\overset{\text{trigs}}{\longleftrightarrow}$	$T_\theta \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$

- $(x, y) \in C \Longrightarrow T_\theta(x, y) \in C$ gives $\cos^2\theta + \sin^2\theta = 1$,
- $T_{\theta'} \circ T_\theta = T_{\theta'+\theta}$ gives the addition formula.

The *symmetry group* $(\star)$ was hidden beneath the *equation* $(*)$... not so obvious!

Similarly, beneath the equation $X^2 - 3X - 5 = 0$ lies $X \longleftrightarrow 3 - X$, because

$$(3 - X)^2 - 3(3 - X) - 5 = X^2 - 3X - 5. \quad \text{(check!)}$$

Beneath the equation $X^4 + 52X^3 - 26X^2 - 12X + 1 = 0$ lies the group C_4:

$$\begin{array}{ccc} X & \longrightarrow & -\dfrac{4X}{(1-X)^2} \\ \uparrow & & \downarrow \\ \dfrac{(1-X)(1+3X)}{-4X^2} & \longleftarrow & \dfrac{1-X}{1+3X} \end{array}$$

(...check! [from Gauss' diary 1797])

1. Classical Galois Theory (as Galois did it)

1.1. **Basic notions.** The symbols K, L, F will always denote *fields*.

Definition 1. Let L be a field. If a subring K of L is a field, it is called a *subfield* of L. We say L is an *extension* of K. We refer to the pair as an *extension* L/K. (Read "L over K", not a quotient in any sense.)

Note that if K, L are both subfields of F and $K \subset L$, then K is a subfield of L, hence we have extensions $F/K, F/L$ and L/K; sometimes L/K is called a *subextension* of F/K.

In this section (§1) we are mainly interested in *subfields of* $\mathbb{C}$, although until §1.4 all will be valid for general fields.

Example. $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$. Recall the notation $\mathbb{Q}(\sqrt{2}) := \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$, similarly for $\mathbb{Q}(\sqrt{-1})$ etc. Then $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$ and $\mathbb{Q}(\sqrt{-1}) \not\subset \mathbb{R}$.

Recall that $\mathbb{C}$ was an $\mathbb{R}$-v.s. (vector space). In general, if L/K is an extension. The multiplication in L makes L into a K-v.s. (L is an additive group; $1 \cdot x = x,\ (ab)x = a(bx),\ (a+b)x = ax + bx,\ a(x+y) = ax + ay$ by the axiom for rings.) We always consider L as a K-v.s. in this way. If $K \subset L \subset F$, then L is a sub-K-v.s. of F.

Definition 2. We say an extension L/K is *finite* if L is a finite dimensional K-v.s., otherwise *infinite*. Its dimension is called the *degree* of L/K, denoted by $[L : K]$. (We also say "L is finite over K", "L is a finite extension of K".)

Example. $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$: finite, with basis $\{1, \sqrt{2}\}$.
$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2,\ \ [\mathbb{C} : \mathbb{R}] = 2,\ \ \mathbb{R}/\mathbb{Q}$: infinite.

Recall $K[X] :=$ the ring of polynomials in X with coefficients in K. [*Polynomials* are formal K-linear combinations of the monomials $1, X, X^2, \ldots$; they form a ring and a K-v.s., but usually not considered as functions.]

Definition 3. Let L/K be an extension, and $\alpha \in L$. Let

$$I_\alpha := \{P(X) \in K[X] \mid P(\alpha) = 0\} \subset K[X],$$

the set of all polynomial which has α as a root. We say α is *algebraic* over K if $I_\alpha \neq \{0\}$, and *transcendental* over K if $I_\alpha = \{0\}$. We say L/K is *algebraic* if every $\alpha \in L$ is algebraic $/K$ (reads "over K"); otherwise *transcendental*.

Example. $\sqrt{2}, \sqrt[3]{2}$: algebraic $/\mathbb{Q}$. π, e: transcendental $/\mathbb{Q}$.

Proposition 4. *Every finite extension is algebraic.*

Proof. If $[L : K] = n$ and $\alpha \in L$, then the elements $1, \alpha, \alpha^2, \ldots, \alpha^n \in L$ are linearly depedent over K, hence $P(\alpha) = 0$ for some nonzero $P \in K[X]$, i.e. $I_\alpha \neq 0$. □

Now note that I_α in Def. 3 is the *kernel* of the ring homomorphism

$$f_\alpha : K[X] \ni P(X) \longmapsto P(\alpha) \in L$$

("*plug in* α"; it is also a K-linear map), hence an *ideal* of $K[X]$. (Also directly checked from $P(\alpha) = Q(\alpha) = 0 \Longrightarrow (P+Q)(\alpha) = 0,\ R(\alpha)P(\alpha) = 0\ \forall R \in K[X]$.)

Lecture 3 (9 Oct, Tu.)

Definition 5. Let L/K be an extension, and $\alpha \in L$ be algebraic $/K$. As $K[X]$ is a PID, we have $I_\alpha = (P_\alpha) = \{\text{multiples of } P_\alpha\}$ for a unique monic $P_\alpha \in K[X]$. This P_α is called the *minimal polynomial* of α over K.

Note that $\deg P_\alpha$ is minimal among $\deg P$ for $P \neq 0$ in I_α.

Example. (i) Min. poly. of $\alpha = \sqrt{2}$ over $\mathbb{Q}$: $P_\alpha = X^2 - 2 \in \mathbb{Q}[X]$.
(ii) Min. poly. of $\alpha = \sqrt{2}$ over $\mathbb{R}$: $P_\alpha = X - \sqrt{2} \in \mathbb{R}[X]$.
(iii) Min. poly. of $\alpha = \sqrt[3]{2}$ over $\mathbb{Q}$: $P_\alpha = X^3 - 2 \in \mathbb{Q}[X]$. Consider $f_\alpha : \mathbb{Q}[X] \to \mathbb{C}$, and:

$$\mathbb{Q}(\alpha) := \operatorname{Im} f_\alpha = \{a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{Q}\} \subset \mathbb{C} \quad (\text{in fact } \subset \mathbb{R}).$$

This is a *field*: it is a ring, and every nonzero element is invertible. How do you find $(1+\alpha)^{-1}$? Use $(1+\alpha)(1-\alpha+\alpha^2) = 1 + \alpha^3 = 3$, hence $(1+\alpha)^{-1} = \dfrac{1}{3}(1 - \alpha + \alpha^2) \in \mathbb{Q}(\alpha)$.

1.2. **Simple extensions.**
Note: the intersection of subfields is a subfield; the unions are not in general.

Definition 6. Let L/K be an extension and $\alpha \in L$. We denote by $K(\alpha)$ the intersection of all subfields of L containing K and α, i.e. the minimal such subfield. Then $K(\alpha)/K$ is called the extension *generated by* α. We say L/K is *simple* if $L = K(\alpha)$ for some $\alpha \in L$.

Proposition 7. *Let L/K be an extension and $\alpha \in L$ be algebraic $/K$.*

(i) *Its minimimal polynomial P_α over K is irreducible in $K[X]$.*
(ii) $\operatorname{Im} f_\alpha = K(\alpha)$ *and* $[K(\alpha) : K] = \deg P_\alpha$. *In particular $K(\alpha)/K$ is finite.*

Proof. (i): If $P_\alpha(X) = P(X)Q(X)$, then $P(\alpha)Q(\alpha) = P_\alpha(\alpha) = 0$, hence $P(\alpha) = 0$ or $Q(\alpha) = 0$. Say $P(\alpha) = 0$; then $P \in I_\alpha = (P_\alpha)$, i.e. $P_\alpha \mid P$ (reads: P_α divides P), hence Q is a unit in $K[X]$.

(ii): (1) $\operatorname{Im} f_\alpha$ is a subfield of L.
$\because$) It is a ring (being the image of a ring hom. f_α). Every $x \in \operatorname{Im} f_\alpha$ is of the form $P(\alpha)$ for some $P \in K[X]$. If $x \neq 0$, then $P \notin (P_\alpha)$, i.e. P is not divisible by P_α. Hence $\exists Q \in K[X]$ with $PQ \equiv 1 \mod P_\alpha$, therefore $P(\alpha)^{-1} = Q(\alpha) \in \operatorname{Im} f_\alpha$.

(2) $\mathrm{Im}\, f_\alpha = K(\alpha)$.

$\because$) As $\mathrm{Im}\, f_\alpha$ is a subfield of L containing K and α, and any such subfield must contain $\mathrm{Im}\, f_\alpha$, we have $\mathrm{Im}\, f_\alpha = K(\alpha)$.

(3) If $\deg P_\alpha = n$, then $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ gives a basis of $K(\alpha)$.

$\because$) For every $x = P(\alpha) \in \mathrm{Im}\, f_\alpha$, there exists $Q, R \in K[X]$, with $P = P_\alpha \cdot Q + R$ and $\deg R < n$, hence $x = P(\alpha) = R(\alpha)$ is a K-linear combination of $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$. If $R(\alpha) = 0$ for some $R \in K[X]$ with $\deg R < n$, then $P_\alpha \mid R$, hence $R = 0$. [(1)] □

Remark. (i) Different elements can generate the same field, i.e. we can have $K(\alpha) = K(\alpha')$ with $\alpha \neq \alpha'$ (even $P_\alpha \neq P_{\alpha'}$), e.g. $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(1 + \sqrt{2})$.

(ii) By Prop. 4 and 7(ii), for an extension L/K and $\alpha \in L$:

$$\alpha : \text{algebraic } /K \iff K(\alpha)/K : \text{finite}.$$

(iii) If $K \subset L \subset F$ and $\alpha \in F$, then $K[X] \subset L[X]$ implies:

(1) α : algebraic $/K \Longrightarrow \alpha$: algebraic $/L$.

(2) its min. poly. Q_α over L divides its min. poly. P_α over K.

We will see in §1.3 that the converse of (i) holds if L/K is *finite*.

(iv) Related question. $\sqrt{2}$: alg./$\mathbb{Q}$ (root of $X^2 - 2$), $\sqrt[3]{2}$: alg./$\mathbb{Q}$ (root of $X^3 - 2$). Is $\sqrt{2} + \sqrt[3]{2}$ alg./$\mathbb{Q}$? (Root of what?) Note $\sqrt{2} + \sqrt[3]{2} \in \mathbb{Q}(\sqrt{2})(\sqrt[3]{2})$, a *tower* of simple extensions.

1.3. **Finite extensions.** *Note:* If $[L : K] = 1$, then $L = K$ (1-dim. K-v.s.).

Proposition 8. (Tower Law) *Let $K \subset L \subset F$. If F/K is finite, then so are L/K and F/L. Conversely, if L/K and F/L are finite, then so is F/K, and $[F : K] = [F : L][L : K]$.*

Proof. We have $\dim_K L \leq \dim_K F$ since L is a sub-K-v.s. of F, and $\dim_L F \leq \dim_K F$ since a spanning set of F as a K-v.s. is also spanning as a L-v.s. If $\{a_1, \ldots, a_n\} \subset L$ is a basis of L/K (i.e. a basis of L as a K-v.s.), and $\{b_1, \ldots, b_m\} \subset F$ is a basis of F/L, then every $x \in F$ is written as $x = x_1 b_1 + \cdots + x_m b_m$ with $x_j \in L$, and each $x_j \in L$ is written as $x_j = x_{1j} a_1 + \cdots + x_{nj} a_n$ with $x_{ij} \in K$. Hence $x = \sum_j \big(\sum_i x_{ij} a_i\big) b_j = \sum_{i,j} x_{ij} a_i b_j$. If $x = \sum_{i,j} x_{ij} a_i b_j = 0$, then $\sum_i x_{ij} a_i = 0\ \forall j$ by the L-linear independence of $\{b_j\}$, therefore $x_{ij} = 0\ \forall i, j$ by the K-linear independence of $\{a_i\}$. Thus $\{a_i b_j \mid 1 \leq i \leq n, 1 \leq j \leq m\}$ is a basis of F/K. [(2)] □

[(1)](optional) A slicker proof of Prop. 7. By hom. thm. $K[X]/(P_\alpha) \cong \mathrm{Im}\, f_\alpha$ as rings and K-v.s.; as RHS is a subring of a field L, hence an integral domain, (P_α) is prime; being non-zero it is maximal ($K[X]$: PID), hence LHS is a field; so is RHS. As a K-v.s. the LHS has basis $\{1, \overline{X}, \overline{X}^2, \ldots, \overline{X}^{n-1}\}$, where $\overline{X} = X \bmod P_\alpha$, we get $\dim = n$. This LHS is an ext'n of K in the abstract sense (a field $\supset K$, but not $\subset \mathbb{C}$). Its element $\overline{X}$ is an abstract root of P_α.

[(2)]More generally, any fin. dim. L-v.s. V can be considered as a K-v.s. by restricting the scalar multiplication, and the same proof shows $\dim_K V = [L : K] \cdot \dim_L V$.

Lecture 4 (11 Oct, Th.)

Definition 9. Let L/K be an extension and $\alpha_1, \ldots, \alpha_n \in L$. We denote by $K(\alpha_1, \ldots, \alpha_n)$ the intersection of all subfields of L containing K and $\alpha_1, \ldots, \alpha_n$, i.e. the minimal such subfield. Then $K(\alpha_1, \ldots, \alpha_n)/K$ is called the extension *generated by* $\alpha_1, \ldots, \alpha_n$.

The order of $\alpha_1, \ldots, \alpha_n$ is irrelevant, and $K(\alpha_1, \ldots, \alpha_n) = K(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n)$ (both inclusions are immediate from the definitions).

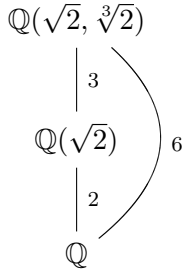
Proposition 10. (i) *If L/K is an extension and $\alpha_1, \ldots, \alpha_n \in L$ are algebraic over K, then $K(\alpha_1, \ldots, \alpha_n)/K$ is finite.*

(ii) *Conversely, every finite extension L/K is generated by finitely many elements, i.e. there exist $\alpha_1, \ldots, \alpha_n \in L$ with $L = K(\alpha_1, \ldots, \alpha_n)$.*

Proof. (i): As α_n is alg. $/K$, it is *a fortiori* alg. $/K(\alpha_1, \ldots, \alpha_{n-1})$, hence $K(\alpha_1, \ldots, \alpha_n) = K(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n)$ is finite over $K(\alpha_1, \ldots, \alpha_{n-1})$ by Prop. 7(ii). Repeat for each $K(\alpha_1, \ldots, \alpha_i)$ with $1 \leq i \leq n$ and use Tower Law (Prop. 8).

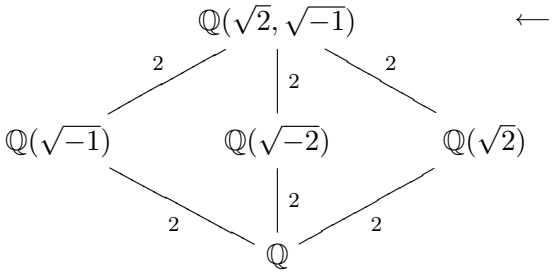
(ii): Take a basis $\{e_1, \ldots, e_n\}$ of L/K. Then $K(e_1, \ldots, e_n) = L$ because every $x \in L$ is a K-linear combination of $e_1, \ldots, e_n$. □

Example. The min. poly. of $\sqrt[3]{2}$ over $\mathbb{Q}(\sqrt{2})$ is $X^3 - 2$, as it is irreducible in $\mathbb{Q}(\sqrt{2})[X]$ (else its root $\in \mathbb{Q}(\sqrt{2})$ generates a field of deg. 3 $/\mathbb{Q}$), hence $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}(\sqrt{2})] = 3$ by Prop. 7(ii).



Thus $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}] = 6$ (Prop. 8). What is the min. poly. of $\sqrt{2} + \sqrt[3]{2}$ over $\mathbb{Q}$? (It has to have degree ≤ 6 because $[\mathbb{Q}(\sqrt{2} + \sqrt[3]{2}) : \mathbb{Q}] \leq 6$. In fact it is 1,2,3 or 6 by Tower Law.)

Example. The fields of the form $K(\sqrt{a})$ and $K(\sqrt{a}, \sqrt{b})$ for non-square elements $a, b \in K$ are called *quadratic* and *biquadratic* fields over K.



$\longleftarrow$ fin. ext. of degree 4 $/\mathbb{Q}$, with a basis $\{1, \sqrt{2}, \sqrt{-1}, \sqrt{-2}\}$

Remark. Finite extensions are algebraic (Prop. 4), but ∃*infinite* algebraic extensions. [(3)]

1.4. K-homomorphisms.

Lemma 11. *Let L be a field and L' be a ring with $L' \neq \{0\}$. Then any ring homomorphism $\tau : L \to L'$ is injective.*

Proof. As $\operatorname{Ker}\tau$ is an ideal of L not containing $1 \in L$ ($\because \tau(1) = 1$), hence $\{0\}$. □

Definition 12. Let $L/K, L'/K$ be two extensions of K. A *K-homomorphism* from L to L' is a ring hom. $\tau : L \to L'$ such that $\tau|_K = \mathrm{id}$. The set of all K-hom's from L to L' is denoted by $\operatorname{Hom}_K(L, L')$.

Note: All K-hom's are injective (also called *embeddings*), and they are K-linear. Here we're mainly interested in the set $\operatorname{Hom}_K(L, \mathbb{C})$ (when $K \subset L \subset \mathbb{C}$) and its cardinality.

Example. (i) $\mathbb{C}/\mathbb{R}$. $\mathbb{R}$-hom. $\tau : \mathbb{C} \to \mathbb{C}$... 2 of them (note $\mathbb{C} = \mathbb{R}(\sqrt{-1})$):

$$\operatorname{Hom}_{\mathbb{R}}(\mathbb{C}, \mathbb{C}) = \{\mathrm{id}, \text{cpx conj}\}, \quad \begin{cases} \mathrm{id} : & \sqrt{-1} \mapsto \sqrt{-1} \\ \text{cpx conj} : & \sqrt{-1} \mapsto -\sqrt{-1} \end{cases}$$

(ii) $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. $\mathbb{Q}$-hom. $\tau : \mathbb{Q}(\sqrt{2}) \to \mathbb{C}$... 2 of them:

$$\tau_1 = \mathrm{id} : \sqrt{2} \mapsto \sqrt{2}, \quad \tau_2 : \sqrt{2} \mapsto -\sqrt{2}.$$

Note: being a *ring hom.*, it must send a root of P to a root of P if $P \in K[X]$.

(iii) $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. Let $\zeta^3 = 1,\ \zeta \neq 1$.

3 $\mathbb{Q}$-hom's $\tau : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{C}$: $\begin{cases} \tau_1 = \mathrm{id} : & \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ \tau_2 : & \sqrt[3]{2} \mapsto \sqrt[3]{2}\zeta \\ \tau_3 : & \sqrt[3]{2} \mapsto \sqrt[3]{2}\zeta^2 \end{cases}$ ... 3 roots of $X^3 - 2$ in $\mathbb{C}$.

Note: in contrast to (i),(ii), here their images $\operatorname{Im}\tau_i$ are all different subfields of $\mathbb{C}$.

We see that K-hom's from $K(\alpha)$ are closely related to the roots of the minimal polynomial P_α of α over K.

Definition 13. (i) For a nonzero $P \in K[X]$ and an extension L/K, we denote by $\operatorname{Root}_P(L)$ the set of all roots of P in L.

(ii) Let $\alpha \in L$ be algebraic $/K$. A root of its minimal poly. P_α in L, i.e. an element of $\operatorname{Root}_{P_\alpha}(L)$ is called a *conjugate* of α in L over K.

[(3)] Take all $\alpha \in \mathbb{C}$ which are algebraic $/\mathbb{Q}$ (countable!), and order them as $\alpha_1, \alpha_2, \alpha_3, \ldots$. We get a sequence $\mathbb{Q}(\alpha_1) \subset \mathbb{Q}(\alpha_1, \alpha_2) \subset \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) \subset \cdots$, so form their union $\overline{\mathbb{Q}} := \bigcup_n \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$. It is a subfield of $\mathbb{C}$, and contains all $\alpha \in \mathbb{C}$ alg. $/\mathbb{Q}$. Conversely every $\alpha \in \overline{\mathbb{Q}}$ belongs to some finite ext'n of $\mathbb{Q}$, hence is alg. $/\mathbb{Q}$, i.e. $\overline{\mathbb{Q}}/\mathbb{Q}$ is algebraic. It is not finite, as $\exists$ irreducible poly. $/\mathbb{Q}$ of degree n for all $n \in \mathbb{N}$.

We denote the cardinality of the set X by $|X|$.

Proposition 14. (Roots and Hom's I) *Let $F/K, E/K$ be two extensions of K and $\alpha \in F$ be algebraic $/K$. Then we have a bijection:*

$$\mathrm{Hom}_K\big(K(\alpha), E\big) \ni \tau \overset{\cong}{\longmapsto} \tau(\alpha) \in \mathrm{Root}_{P_\alpha}(E).$$

In particular we have $|\mathrm{Hom}_K\big(K(\alpha), E\big)| \leq [K(\alpha) : K]$.

Remark. The case we have in mind in this §1 is when $K \subset \mathbb{C}$ and $F = E = \mathbb{C}$.

Proof. (1) We have a map.
$\because$) As $P_\alpha(\alpha) = 0$ and τ is ring hom. with $\tau|_K = \mathrm{id}$, we have $P_\alpha(\tau(\alpha)) = \tau(P_\alpha(\alpha)) = 0$, i.e. $\tau(\alpha) \in \mathrm{Root}_{P_\alpha}(E)$. (i.e. every K-hom. sends α to its conjugate over K.)

(2) It is injective.
$\because$) Recall $K(\alpha) = \mathrm{Im}\, f_\alpha$, where $f_\alpha : K[X] \ni P \mapsto P(\alpha) \in E$ (Prop. 7(ii)), i.e. all el'ts in $K(\alpha)$ are poly. in α with coeff. in K, the K-hom. τ is determined by $\tau(\alpha) \in E$.

(3) It is surjective.
$\because$) Let $\beta \in \mathrm{Root}_{P_\alpha}(E)$. We will define $\tau : K(\alpha) \to E$ satisfying $\tau(\alpha) = \beta$. Every $x \in K(\alpha)$ is written as $x = P(\alpha)$ with $P \in K[X]$, and P is unique up to adding multiples of P_α (any other choice of P is of the form $P + P_\alpha \cdot Q$) and $P_\alpha(\beta) = 0$, hence $P(\beta) \in E$ is well-defined. So let $\tau(x) := P(\beta)$, i.e. $\tau : K(\alpha) \ni P(\alpha) \mapsto P(\beta) \in E$. This is clearly a ring hom. with $\tau|_K = \mathrm{id}$.

(4) $|\mathrm{Hom}_K\big(K(\alpha), E\big)| = |\,\mathrm{Root}_{P_\alpha}(E)| \leq \deg P_\alpha \overset{\text{Prop.7(ii)}}{=} [K(\alpha) : K]$ (Lem. 53(ii)). □

Lecture 5 (13 Oct, Sa.)

1.5. K-homomorphism into $\mathbb{C}$.

Note: subfields of $\mathbb{C}$ are always extensions of $\mathbb{Q}$. For $K \subset \mathbb{C}$ and $\alpha \in \mathbb{C}$, by *conjugates* of α over K we will always mean its conjugates in $\mathbb{C}$, e.g. conj. of $\sqrt[3]{2}$ over $\mathbb{Q}$ are $\sqrt[3]{2}$, $\sqrt[3]{2}\zeta$, and $\sqrt[3]{2}\zeta^2$.

Proposition 15. *Let K be a subfield of $\mathbb{C}$.*

(i) *Let $P \in K[X]$ an irreducible poly. in $K[X]$. Then $|\,\mathrm{Root}_P(\mathbb{C})| = \deg P$.*
(This property will be called the separability *of P.)*

(ii) *Let $\alpha \in \mathbb{C}$ be algebraic $/K$. Then $|\mathrm{Hom}_K\big(K(\alpha), \mathbb{C}\big)| = [K(\alpha) : K]$.*

Proof. (i): A multiple root $\alpha \in \mathbb{C}$ of P would also be a root of $P'(X) := \dfrac{d}{dX}P(X) \in K[X]$, but $\deg P' < \deg P$ and P is irreducible, hence P, P' are coprime in $K[X]$, i.e. $\exists Q, R \in K[X]$ with $PQ + P'R = 1$ in $K[X]$, hence also in $\mathbb{C}[X]$. Thus P, P' are coprime in $\mathbb{C}[X]$, hence all roots are distinct ($\deg P$ of them, by the "fundamental th'm of alg.").

(ii): $|\mathrm{Hom}_K\big(K(\alpha), \mathbb{C}\big)| \overset{\text{Prop.14}}{=} |\,\mathrm{Root}_{P_\alpha}(\mathbb{C})| \overset{\text{(i)}}{=} \deg P_\alpha \overset{\text{Prop.7(ii)}}{=} [K(\alpha) : K]$. □

Next goal: generalise Prop. 15(ii) to:

$$|\mathrm{Hom}_K(F,\mathbb{C})| = [F:K] \quad \forall \text{ finite } F/K \text{ (called the } \textit{separability} \text{ of } F/K).^{(4)}$$

Method: break down to simple ext'ns & stack up. If $K \subset L \subset F$ and $\rho \in \mathrm{Hom}_K(F,\mathbb{C})$, then $\rho|_L \in \mathrm{Hom}_K(L,\mathbb{C})$ (ring hom., id on K), i.e. we have a *restriction* map:

$$\mathrm{Hom}_K(F,\mathbb{C}) \ni \rho \longmapsto \rho|_L \in \mathrm{Hom}_K(L,\mathbb{C}).$$

To climb up, count the # of ρ's with a fixed $\rho|_L$, i.e. the *fibres* of this map. (In other words, the # of ways to *extend* a given $\tau \in \mathrm{Hom}_K(L,\mathbb{C})$ to F. The essential case will be where $F = L(\alpha)$, i.e. F is simple over L.)

Example. (i) $i := \sqrt{-1},\ L = \mathbb{Q}(\sqrt{2})$. $\mathrm{Hom}_K(L,\mathbb{C}) = \{\tau_1 = \mathrm{id},\ \tau_2 : \sqrt{2} \mapsto -\sqrt{2}\}$.

$$\begin{array}{c} F = \mathbb{Q}(\sqrt{2},i) \\ \Big| \, 2 \\ L = \mathbb{Q}(\sqrt{2}) \\ \Big| \, 2 \\ K = \mathbb{Q} \end{array} \qquad \text{Let } \rho \in \mathrm{Hom}_K(F,\mathbb{C}).$$

$$\begin{cases} \rho|_L = \tau_1, \text{ i.e. } \rho(\sqrt{2}) = \sqrt{2} & \begin{cases} \rho(i) = i & \Longrightarrow \rho_1 = \mathrm{id} \\ \rho(i) = -i & \Longrightarrow \rho_2 : (\sqrt{2},i) \mapsto (\sqrt{2},-i) \end{cases} \\ \rho|_L = \tau_2, \text{ i.e. } \rho(\sqrt{2}) = -\sqrt{2} & \begin{cases} \rho(i) = i & \Longrightarrow \rho_3 : (\sqrt{2},i) \mapsto (-\sqrt{2},i) \\ \rho(i) = -i & \Longrightarrow \rho_4 : (\sqrt{2},i) \mapsto (-\sqrt{2},-i) \end{cases} \end{cases}$$

(ii) The min. poly. of $\alpha := \sqrt{2}$ over $\mathbb{Q}$ is $X^4 - 2$.

$$\begin{array}{c} F = \mathbb{Q}(\sqrt[4]{2}) \\ \Big| \, 2 \\ L = \mathbb{Q}(\sqrt{2}) \\ \Big| \, 2 \\ K = \mathbb{Q} \end{array} \qquad \Longrightarrow \text{we know } \mathrm{Hom}_K(F,\mathbb{C}):$$

$$\begin{cases} \rho_1 = \mathrm{id} & : \sqrt[4]{2} \longmapsto \sqrt[4]{2} \\ \rho_2 & : \sqrt[4]{2} \longmapsto -\sqrt[4]{2} \\ \rho_3 & : \sqrt[4]{2} \longmapsto \sqrt[4]{2}i \\ \rho_4 & : \sqrt[4]{2} \longmapsto -\sqrt[4]{2}i \end{cases}$$

conjugates of α /K:
$\{\sqrt[4]{2}, -\sqrt[4]{2}, \sqrt[4]{2}i, -\sqrt[4]{2}i\}$.
First two: roots of $X^2 - \sqrt{2} =: P_\alpha$
(the min. poly. of α over L),
Last two: roots of $X^2 + \sqrt{2} = \tau_2 P_\alpha$.

Restrict them to L. Note $\rho(\sqrt{2}) = \rho(\alpha^2) = \rho(\alpha)^2$. Thus:

$$\begin{cases} \rho_1, \rho_2 : \sqrt{2} \longmapsto \sqrt{2}, & \text{i.e. } \rho_1|_L = \rho_2|_L = \tau_1 = \mathrm{id}, \\ \rho_3, \rho_4 : \sqrt{2} \longmapsto -\sqrt{2}, & \text{i.e. } \rho_3|_L = \rho_4|_L = \tau_2 \end{cases}$$

Start with $\rho|_L \in \mathrm{Hom}_K(L,\mathbb{C})$ and try to extend:

$$\begin{cases} \rho|_L = \tau_1 \implies & \rho \text{ must map } \alpha \text{ to a root of } P_\alpha, \\ \rho|_L = \tau_2 \implies & \rho \text{ must map } \alpha \text{ to a root of } \tau_2 P_\alpha, \text{ as } \rho \text{ maps } P_\alpha \text{ to } \tau_2 P_\alpha = X^2 + \sqrt{2}. \end{cases}$$

i.e. to extend $\tau : L \to \mathbb{C}$ to $F = L(\alpha)$, map α to a root of $\tau P_\alpha \in \mathbb{C}[X]$ (defined below).

---

(4) In fact we will see that every F/K inside $\mathbb{C}$ is simple (Th.20), but for that we need this first.

Definition 16. Let L be a field and $\tau : L \to L'$ be a ring hom. For $P \in L[X]$, we denote by $\tau P \in L'[X]$ the poly. obtained by applying τ to the coefficients of P.

In the following proposition, generalising Prop. 14 (where $L = K$ and $\tau = \mathrm{id}$), we allow arbitrary fields. But again we have the case $K \subset \mathbb{C}$ and $F = E = \mathbb{C}$ in mind.

Proposition 17. (Roots and Hom's II) *Let $F/K, E/K$ be two extensions of K. Let $K \subset L \subset F$ and $\alpha \in F$ be algebraic $/L$ with min. poly. P_α over L.*

Then for every $\tau \in \mathrm{Hom}_K(L, E)$ we have a bijection:

$$\big\{\rho \in \mathrm{Hom}_K\big(L(\alpha), E\big) \;\big|\; \rho|_L = \tau\big\} \ni \rho \overset{\cong}{\longmapsto} \rho(\alpha) \in \mathrm{Root}_{\tau P_\alpha}(E).$$

Proof. (1) $\exists$ map. $\because$) $P_\alpha(\alpha) = 0$, ρ is ring hom. with $\rho|_L = \tau$, we have $\tau P_\alpha(\rho(\alpha)) = \rho(P_\alpha(\alpha)) = 0$, i.e. $\rho(\alpha) \in \mathrm{Root}_{\tau P_\alpha}(E)$.

(2) Inj. $\because$) As all elements in $L(\alpha)$ are poly. in α with coeff. in L, the map ρ is determined by $\rho|_L = \tau$ and $\rho(\alpha) \in E$.

(3) Surj. $\because$) Let $\beta \in \mathrm{Root}_{\tau P_\alpha}(E)$, and we'll define ρ with $\rho(\alpha) = \beta$. Every $x \in L(\alpha)$ is written as $x = P(\alpha)$ with $P \in L[X]$, and P is unique up to adding multiples of P_α. As $\tau P_\alpha(\beta) = 0$, the element $\tau P(\beta) \in E$ is well-defined. So let $\rho(x) := \tau P(\beta)$, i.e. $\rho : L(\alpha) \ni P(\alpha) \mapsto \tau P(\beta) \in E$. This is clearly a ring hom. with $\rho|_K = \tau$. [5] □

Lecture 6 (16 Oct, Tu.)

Now we can prove our first big results.

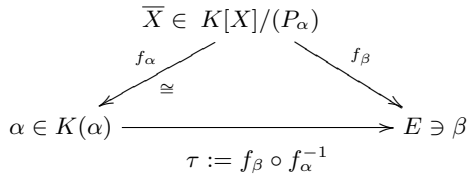
Theorem 18. (Separability) *Let F/K be a finite ext'n inside $\mathbb{C}$. Then:*

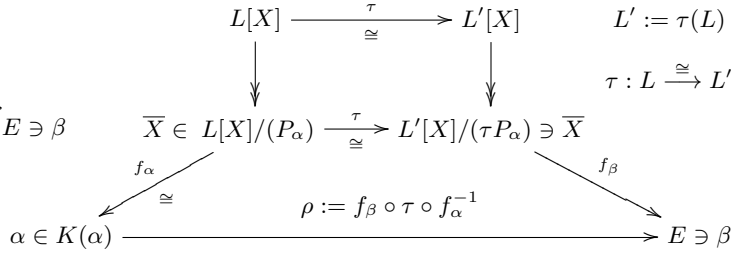
$$|\mathrm{Hom}_K(F, \mathbb{C})| = [F : K].$$

Proof. Let $F = K(\alpha_1, \ldots, \alpha_n)$ (Prop. 10(ii)). If $n = 1$ this is Prop. 15(ii). Use induction on n. Let $L := K(\alpha_1, \ldots, \alpha_{n-1}),\ F = L(\alpha)$ with $\alpha := \alpha_n$. Consider the restriction map:

$$\mathrm{Hom}_K(F, \mathbb{C}) \ni \rho \longmapsto \rho|_L \in \mathrm{Hom}_K(L, \mathbb{C}).$$

[5](optional) Proofs of Prop. 14, Prop. 17 in fancier diagrams:





By Prop. 17, the inverse image of each $\tau \in \mathrm{Hom}_K(L,\mathbb{C})$ has cardinality $|\,\mathrm{Root}_{\tau P_\alpha}(\mathbb{C})|$. Now τP_α is irred. in $\tau(L)[X]$, being the image of $P_\alpha \in L[X]$ (irred. by Prop. 7(ii)) under the ring isom. $L[X] \cong \tau(L)[X]$ extending $\tau : L \cong \tau(L)$. Hence

$$|\,\mathrm{Root}_{\tau P_\alpha}(\mathbb{C})| \overset{\text{Prop.15(i)}}{=} \deg \tau P_\alpha = \deg P_\alpha \overset{\text{Prop.7(ii)}}{=} [L(\alpha):L],$$

$$\begin{aligned} \text{thus} \quad |\mathrm{Hom}_K(F,\mathbb{C})| &= [L(\alpha):L]\cdot|\mathrm{Hom}_K(L,\mathbb{C})| \\ &= [F:L]\cdot[L:K] \quad \text{(ind. hyp.)} \\ &= [F:K]. \qquad \text{(Tower Law Prop. 8)} \end{aligned}$$ □

We have also proved:

Lemma 19. *Let F/K be a finite ext'n inside $\mathbb{C}$ and $K \subset L \subset F$. Then the map*

$$\mathrm{Hom}_K(F,\mathbb{C}) \ni \rho \longmapsto \rho|_L \in \mathrm{Hom}_K(L,\mathbb{C}).$$

is surjective, i.e. one can extend every K-hom. $\tau : L \to \mathbb{C}$ to F.

Theorem 20. (Primitive Element Theorem) *Let F/K be a finite ext'n. Then we have $|\mathrm{Hom}_K(F,E)| \le [F:K]$ for any ext'n E/K. Moreover if it is an equality for some E/K, then F/K is simple. In particular, every finite ext'n inside $\mathbb{C}$ is simple by Th. 18.*

Proof. When $|K| < \infty$ (finite fields), the simplicity will be proved directly (Th. 68) and the first claim follows by Prop. 14. So let $|K| = \infty$ (e.g. any $K \subset \mathbb{C}$, in which case $\mathbb{Q} \subset K$).

Let $F = K(\alpha_1,\dots,\alpha_n)$ (Prop. 10), and $\tau_1,\dots,\tau_d \in \mathrm{Hom}_K(F,E)$ be distinct. If we find $\alpha \in F$ such that $\tau_1(\alpha),\dots,\tau_d(\alpha)$ are all distinct, then $\tau_j|_{K(\alpha)} \in \mathrm{Hom}_K\big(K(\alpha),E\big)$ $(1 \le j \le d)$ are all distinct, hence

$$d \le |\mathrm{Hom}_K\big(K(\alpha),E\big)| \overset{\text{Prop.14}}{\le} [K(\alpha):K] \le [F:K],$$

and $d = [F:K]$ forces $K(\alpha) = F$, so we win.

Let $P = \sum_{i=1}^{n} \alpha_i X^n \in F[X]$, and we try $\alpha \in F$ of the form $\alpha = P(x)$ with $x \in K$. Since $\alpha_1,\dots,\alpha_n$ generate F/K, if $j \ne j'$ then we cannot have $\tau_j(\alpha_i) = \tau_{j'}(\alpha_i)$ for all $1 \le i \le n$. Thus $\tau_j P \in E[X]$ are all distinct poly's, so

$$\prod_{j \ne j'} \big(\tau_j P(X) - \tau_{j'} P(X)\big) \in E[X]$$

is a non-zero poly., hence $\exists x \in K$ which is not its root, since $|K| = \infty$. Then $\tau_j P(x) \ne \tau_{j'} P(x)$ for any $j \ne j'$, in other words for $\alpha := P(x)$ the el'ts $\tau_j(\alpha)$ are all distinct. □

Example. (i) $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$. (ii) $\mathbb{Q}(\sqrt{2},\sqrt[3]{2}) = \mathbb{Q}(\sqrt{2}+\sqrt[3]{2})$. [(6)]

[(6)] All but finitely many unlucky poly's in the generators would work, so PET is a "loose" th'm.

1.6. **Galois extensions.**

Definition 21. Let $L/K, L'/K$ be extensions. If a K-hom. $\tau : L \to L'$ is a bijection, then $\tau^{-1} : L' \to L$ is also a K-hom. (ring hom., id on K), & we say τ is a *K-isomorphism*. An K-isom. $L \to L$ is called a *K-automorphism* of L, and the set of all K-aut. of L is denoted by $\mathrm{Aut}_K(L)$, a subset of $\mathrm{Hom}_K(L, L)$. It is a group under composition ($\because \mathrm{id}_L \in \mathrm{Aut}_K(L)$; $\sigma, \tau \in \mathrm{Aut}_K(L) \Longrightarrow \sigma\tau, \sigma^{-1} \in \mathrm{Aut}_K(L)$).

Lemma 22. (i) *If there is a K-hom. $\tau : L \to L'$, then $[L : K] \le [L' : K]$.*
(ii) *If $[L : K] = [L' : K] < \infty$, then every $\tau \in \mathrm{Hom}_K(L, L')$ is a K-isom.*
(iii) *If L/K is a finite ext'n, then $\mathrm{Hom}_K(L, L) = \mathrm{Aut}_K(L)$ and $|\mathrm{Aut}_K(L)| \le [L : K]$.*

Proof. (i),(ii): Linear Algebra. Recall K-hom's are injective (Lemma 11). Let V, V' be K-v.s. If $\exists K$-lin. inj. $V \to V'$, then $\dim_K V \le \dim_K V'$. An injective K-lin. map $V \to V'$ is bij. if $\dim_K V = \dim_K V' < \infty$ by Rank-Nullity. (iii) follows from (ii) and Th. 20. □

Remark. If $L \subset \mathbb{C}$, then the last part of (iii) follows from $\mathrm{Hom}_K(L, L) \subset \mathrm{Hom}_K(L, \mathbb{C})$ and $|\mathrm{Hom}_K(L, \mathbb{C})| = [L : K]$ (Th.18).

Definition 23. A finite ext'n L/K is called a *Galois extension* if $|\mathrm{Aut}_K(L)| = [L : K]$. In this case $\mathrm{Aut}_K(L)$ is called the *Galois group* of L/K, and denoted by $\mathrm{Gal}(L/K)$.

Remark. Every Galois ext'n is simple by Th. 20. If $L = K(\alpha)$, then L/K is Galois iff $|\mathrm{Root}_{P_\alpha}(L)| = \deg P_\alpha$, where P_α is the min. poly. of α over K, by Prop. 14 and 7(ii).

Proposition 24. *Let L/K be a finite ext'n inside $\mathbb{C}$. TFAE:*
(i) *L/K : Galois.*
(ii) *Every K-hom. $\tau : L \to \mathbb{C}$ maps L into itself.*
(iii) *$\forall \alpha \in L$, every conjugate of α over K is in L.*
(iv) *$L = K(\alpha_1, \ldots, \alpha_n)$ and every conjugate of α_i over K is in L $(1 \le \forall i \le n)$.*

Proof. (i)⇔(ii): By the remark after Lem. 22, L/K is Galois iff $\mathrm{Hom}_K(L, L) = \mathrm{Hom}_K(L, \mathbb{C})$.

(ii)⇒(iii): Let β be a conjugate of α, i.e. $\beta \in \mathrm{Root}_{P_\alpha}(\mathbb{C})$. Then by Prop. 14 we have $\tau \in \mathrm{Hom}_K\big(K(\alpha), \mathbb{C}\big)$ with $\tau(\alpha) = \beta$, and it extends to $\rho \in \mathrm{Hom}_K(L, \mathbb{C})$ by Lem. 19. Then (ii) says $\beta = \rho(\alpha) \in L$. (iii)⇒(iv) is clear.

(iv)⇒(ii): Let $\tau \in \mathrm{Hom}_K(L, \mathbb{C})$. As every $\alpha \in L$ is a poly. in $\alpha_1, \ldots, \alpha_n$ with coeff. in K, $\tau(\alpha)$ is a poly. in $\tau(\alpha_1), \ldots, \tau(\alpha_n)$ with coeff. in K. But $\tau(\alpha_i)$ is a conj. of α_i over K (Prop. 14), hence in L by (iv), therefore $\tau(\alpha) \in L$. □

Example. (i) $\mathbb{C}/\mathbb{R}$: Galois. (ii) $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$: Galois. (iii) $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$: NOT Galois.[7]

[7]For $K \subset L \subset F$, even if $F/L, L/K$ are Galois F/K may not be Galois, e.g. $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$.

Lecture 7 (18 Oct, Th.)

Definition 25. Let $P \in K[X]$ with $K \subset \mathbb{C}$, and $\mathrm{Root}_P(\mathbb{C}) = \{\alpha_1, \ldots, \alpha_n\}$. Then $K(\alpha_1, \ldots, \alpha_n) \subset \mathbb{C}$ is called the *splitting field* of P over K.

Corollary 26. *Let $P \in K[X]$ with $K \subset \mathbb{C}$. Its splitting field over K is Galois over K.*

Proof. It is a finite ext'n of K by Prop. 10(i), and as all conjugates of α_i over K belong to $\mathrm{Root}_P(\mathbb{C})$ ($\because$ min. poly. of α_i divides P), it is a Galois ext'n of K by Prop. 24(iv). □

Example. (i) $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is the splitting field of $X^2 - 2$ over $\mathbb{Q}$.
(ii) The splitting field of $X^3 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\zeta, \sqrt[3]{2}\zeta^2) = \mathbb{Q}(\sqrt[3]{2}, \zeta)$, where $\zeta^3 = 1$.
(iii) If $K(\alpha)/K$ is Galois, then it is the splitting field of P_α. ($\because$ If $\mathrm{Root}_{P_\alpha}(\mathbb{C}) = \{\alpha_1, \ldots, \alpha_n\}$, they are all in $K(\alpha)$ by Prop. 24(iii), hence $K(\alpha) = K(\alpha_1, \ldots, \alpha_n)$.)

Big example 1: Cyclotomic ext'ns.

Definition 27. Let $N \geq 1$, and $\zeta = \zeta_N := \exp\Big(\dfrac{2\pi i}{N}\Big) \in \mathbb{C}$. Then:

$$\boldsymbol{\mu}_N := \mathrm{Root}_{X^N-1}(\mathbb{C}) = \{1, \zeta, \zeta^2, \ldots, \zeta^{N-1}\} \quad \text{(the set of } N\text{-}\textit{th roots of unity}\text{)}$$

is a multiplicative group, cyclic of order N. Its element ζ^i is a generator of this group iff $(i, N) = 1$; they are called the *primitive* roots.

For $K \subset \mathbb{C}$, the splitting field of $X^N - 1$ over K is denoted by $K(\boldsymbol{\mu}_N)$ and called a *cyclotomic extension* of K.

Note $K(\boldsymbol{\mu}_N) = K(1, \zeta, \zeta^2, \ldots, \zeta^{N-1}) = K(\zeta) = K(\zeta^i)$ $(\forall i \in \mathbb{N}$ with $(i, N) = 1)$.

Proposition 28. *Let $K \subset \mathbb{C}$ and $N \geq 1$. We have an injective group hom.:*

$$\begin{aligned} \mathrm{Gal}\big(K(\boldsymbol{\mu}_N)/K\big) &\longrightarrow \big(\mathbb{Z}/(N)\big)^\times \\ (\tau : \zeta \mapsto \zeta^i) &\longmapsto i \bmod N, \end{aligned}$$

where $\big(\mathbb{Z}/(N)\big)^\times := \{i \bmod N \mid (i, N) = 1\}$ is the multiplicative group of units in the ring $\mathbb{Z}/(N) = \{i \bmod N \mid i \in \mathbb{Z}\}$.

Proof. Let $\tau \in \mathrm{Gal}\big(K(\boldsymbol{\mu}_N)/K\big)$. As $\zeta \in \boldsymbol{\mu}_N$ and ζ has order N in $\boldsymbol{\mu}_N$, $\tau(\zeta) \in \boldsymbol{\mu}_N$ and has order N, i.e. $\tau(\zeta) = \zeta^i$ with $(i, N) = 1$, and i is well-def'd $\bmod N$ so we have a map.

As $\tau(\zeta)$ determines τ ($\because$ $K(\boldsymbol{\mu}_N) = K(\zeta)$), this map is injective. If $\tau(\zeta) = \zeta^i$ and $\sigma(\zeta) = \zeta^j$, then $\sigma\tau(\zeta) = \sigma(\zeta^i) = (\zeta^j)^i = \zeta^{ij}$, hence it is a group hom. □

Corollary 29. $K(\boldsymbol{\mu}_N)/K$ *is* abelian, *i.e. a Galois ext'n with an abelian Galois group.*

Remark. We will see that this injection is actually bijective when $K = \mathbb{Q}$ (*Irreducibility of Cyclotomic Polynomials, Th. 71*).

Big example 2: Kummer ext'ns.

Definition 30. Let $N \geq 1$ and $\boldsymbol{\mu}_N \subset K \subset \mathbb{C}$. Let $a \in K$, and if $\sqrt[N]{a} \in \mathbb{C}$ is a root of $X^N - a$, then

$$\mathrm{Root}_{X^N-a}(\mathbb{C}) = \{ \sqrt[N]{a},\ \sqrt[N]{a}\zeta,\ \sqrt[N]{a}\zeta^2, \ldots,\ \sqrt[N]{a}\zeta^{N-1}\},$$

where $\zeta = \zeta_N$. The splitting field of $X^N - a$ over K is called a *Kummer extension* of K, and is equal to $K(\sqrt[N]{a})$ for any choice of $\sqrt[N]{a}$.

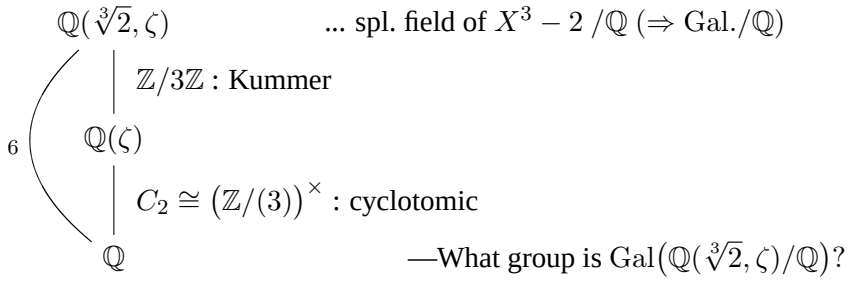
Proposition 31. *If $K(\sqrt[N]{a})/K$ is as above, we have an injective group hom.:*

$$\mathrm{Gal}\big(K(\sqrt[N]{a})/K\big) \longrightarrow \mathbb{Z}/N\mathbb{Z}$$
$$(\tau :\ \sqrt[N]{a} \mapsto\ \sqrt[N]{a}\zeta^i) \longmapsto i \bmod N,$$

where $\mathbb{Z}/N\mathbb{Z}$ is the additive group of $\mathbb{Z}/(N)$. In particular $K(\sqrt[N]{a})/K$ is abelian.

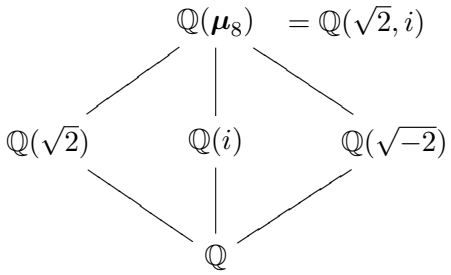
Proof. Let $\tau \in \mathrm{Gal}\big(K(\sqrt[N]{a})/K\big)$. Then $\tau(\sqrt[N]{a}) = \sqrt[N]{a}\zeta^i$ for some i, well-def'd $\bmod N$ and independent of the choice of $\sqrt[N]{a}$ ($\because \tau(\sqrt[N]{a}\zeta^j) = (\sqrt[N]{a}\zeta^i)\zeta^j = (\sqrt[N]{a}\zeta^j)\zeta^i$). As $\tau(\sqrt[N]{a})$ determines τ, this map is injective. If $\tau(\sqrt[N]{a}) = \sqrt[N]{a}\zeta^i$ and $\sigma(\sqrt[N]{a}) = \sqrt[N]{a}\zeta^j$, then $\sigma\tau(\sqrt[N]{a}) = \sigma(\sqrt[N]{a}\zeta^i) = (\sqrt[N]{a}\zeta^j)\zeta^i = \sqrt[N]{a}\zeta^{i+j}$, i.e. it is a group hom. □

Example. Let $\zeta^3 = 1$ with $\zeta \neq 1$.



1.7. **Galois correspondence.**

Example. $\zeta = \zeta_8 = \sqrt{2}(1+i)/2$: root of $X^4 + 1$.



$$\mathrm{Gal}\big(\mathbb{Q}(\boldsymbol{\mu}_8)/\mathbb{Q}\big) = \begin{cases} \rho_1 = \mathrm{id}, \\ \rho_2 : (\sqrt{2}, i) \mapsto (\sqrt{2}, -i), \\ \rho_3 : (\sqrt{2}, i) \mapsto (-\sqrt{2}, i), \\ \rho_4 : (\sqrt{2}, i) \mapsto (-\sqrt{2}, -i). \end{cases}$$

$$\overset{\text{Prop.28}}{\cong} \big(\mathbb{Z}/(8)\big)^\times = \{1, 3, 5, 7 \bmod 8\} \cong C_2 \times C_2.$$

ρ_1 fixes all elements in $\mathbb{Q}(\boldsymbol{\mu}_8)$.

$$\left.\begin{array}{l} \rho_2 \text{ fixes } \mathbb{Q}(\sqrt{2}), \\ \rho_3 \text{ fixes } \mathbb{Q}(i), \\ \rho_4 \text{ fixes } \mathbb{Q}(\sqrt{-2}). \end{array}\right\} \text{order 2} \left(\begin{array}{l} \rho_2 : \zeta \mapsto \zeta^7 \\ \rho_3 : \zeta \mapsto \zeta^5 = -\zeta \\ \rho_4 : \zeta \mapsto \zeta^3 \end{array}\right)$$

Note: $\sqrt{2} = \zeta + \zeta^7$, $\ i = \zeta^2 = -\zeta \cdot \zeta^5$, $\ \sqrt{-2} = \zeta + \zeta^3$.

Lecture 8 (20 Oct, Sa.)

Lemma 32. *Let F/K be an ext'n and $G := \mathrm{Aut}_K(F)$.*

(i) *Let $K \subset L \subset F$. Then $\mathrm{Aut}_L(F)$ is a subgroup of G, i.e.*

$$\mathrm{Aut}_L(F) = \{\sigma \in G \mid \sigma|_L = \mathrm{id}\} = \{\sigma \in G \mid \sigma(\alpha) = \alpha \ \forall \alpha \in L\} \subset G$$

(ii) *Let H be a subgroup of G. The subset $F^H := \{\alpha \in F \mid \sigma(\alpha) = \alpha \ \forall \sigma \in H\} \subset F$ of all elements in F fixed by all autom's in H is a subfield of F, called the* fixed field *of H. We have $K \subset F^G \subset F^H \subset F$ and $H \subset \mathrm{Aut}_{F^H}(F)$.*

Proof. (i): An L-autom. $F \to F$ is nothing other than a K-autom. satisfying $\sigma|_L = \mathrm{id}$.

(ii): As every $\sigma \in G$ is a ring hom., if $\sigma(\alpha) = \alpha$ and $\sigma(\beta) = \beta$, then $\sigma(\alpha + \beta) = \alpha + \beta$, $\sigma(\alpha\beta) = \alpha\beta$ and $\sigma(\alpha^{-1}) = \alpha^{-1}$ when $\alpha \neq 0$. Hence F^H is a field. As $\sigma|_K = \mathrm{id}\ \forall \sigma \in G$ we have $K \subset F^G$. As $\sigma|_{F^H} = \mathrm{id}\ \forall \sigma \in H$ we have $H \subset \mathrm{Aut}_{F^H}(F)$. □

Proposition 33. *Let F/K be a simple finite ext'n (e.g. any finite ext'n inside $\mathbb{C}$, cf. Th. 20).*

(i) *If F/K is Galois and $G := \mathrm{Gal}(F/K)$, then $F^G = K$.*

(ii) *If $F^G = K$ for a subgroup G of $\mathrm{Aut}_K(F)$, then F/K is Galois and $G = \mathrm{Aut}_K(F)$.*

Proof. (i): Note $K \subset F^G \subset F$. As $G \subset \mathrm{Aut}_{F^G}(F)$, we have:

$$|G| \leq |\mathrm{Aut}_{F^G}(F)| \overset{\text{Lem.22(iii)}}{\leq} [F : F^G] \leq [F : K].$$

But since F/K is Galois $|G| = [F : K]$, hence all are equalities & $F^G = K$.

(ii): Let $F = K(\alpha)$, and P_α be the min. poly. of α. Set:

$$Q_\alpha := \prod_{\sigma \in G} \big(X - \sigma(\alpha)\big) \in F[X].$$

It has α as a root, and its coeff. are the elementary symmetric poly. (Def. 81) of $\{\sigma(\alpha) \mid \sigma \in G\}$, hence in $F^G = K$ (since el'ts of G just permute $\{\sigma(\alpha) \mid \sigma \in G\}$). Hence $P_\alpha \mid Q_\alpha$. Thus

$$[F : K] \overset{\text{Prop.7(ii)}}{=} \deg P_\alpha \leq \deg Q_\alpha = |G| \leq |\mathrm{Aut}_K(F)| \overset{\text{Lem.22(iii)}}{\leq} [F : K],$$

hence all are equalities, F/K is Galois & $G = \mathrm{Aut}_K(F)$. [8] □

Remark. By Prop. 33, a finite F/K inside $\mathbb{C}$ is Galois iff $F^{\mathrm{Aut}_K(F)} = K$.

Theorem 34. (Fundamental Theorem of Galois Theory) *Let F/K be a Galois ext'n. Then the following maps* (Galois correspondence)*, defined by Lem. 32:*

$$\left\{\begin{array}{c} \textit{subfields } L \textit{ w/} \\ K \subset L \subset F \end{array}\right\} \begin{array}{c} \ni \\ \ni \end{array} \begin{array}{c} L \longmapsto \mathrm{Aut}_L(F) \\ F^H \longleftarrow\!\shortmid H \end{array} \begin{array}{c} \in \\ \in \end{array} \left\{\begin{array}{c} \textit{subgroups } H \textit{ of} \\ G := \mathrm{Gal}(F/K) \end{array}\right\}$$

are bijections, inverse to each other. If $L \leftrightarrow H$, then $[F : L] = |H|$ and $[L : K] = |G|/|H|$.

[8] Prop. 33(ii) holds without assuming F/K simple/finite, as long as G is finite (*Artin's Lemma*, Prop. 88).

Proof. Let $F = K(\alpha)$ by PET (Th. 20). The remark after Def. 23 says $|\operatorname{Root}_{P_\alpha}(F)| = \deg P_\alpha$, where P_α is the min. poly. of α /K (it splits into distinct linear factors in $F[X]$).

Take L. The min. poly. Q_α of α over L divides P_α, hence $|\operatorname{Root}_{Q_\alpha}(F)| = \deg Q_\alpha$. As $F = L(\alpha)$, the same remark says F/L is Galois. Now Prop. 33(i) shows $F^{\operatorname{Aut}_L(F)} = L$.

Take H. By above F/F^H is Galois, hence simple (Th. 20). Since $H \subset \operatorname{Aut}_{F^H}(F)$ by Lem. 32(ii), the Prop. 33(ii) shows $H = \operatorname{Aut}_{F^H}(F)$.

If $H = \operatorname{Aut}_L(F)$, then $[F : L] = |H|$ as F/L is Galois, and hence $[L : K] = |G|/|H|$ by Tower Law (Prop. 8). □

Corollary 35. *Let F/K be a Galois ext'n inside $\mathbb{C}$ with $G := \operatorname{Gal}(F/K)$, and $K \subset L \subset F$.*

(i) *F/L is Galois and $H := \operatorname{Gal}(F/L)$ is a subgroup of G.*

(ii) *L/K : Galois $\iff$ $H \lhd G$ (normal). If this holds, we have an isom. of groups:*

$$G/H \ni \sigma H \overset{\cong}{\longmapsto} \sigma|_L \in \operatorname{Gal}(L/K).$$

Proof. (i): Shown in the proof of Th. 34.

(ii): If $\sigma \in G$, then $K \subset \sigma(L) \subset F$, and the subgp. corresponding to $\sigma(L)$ is $\sigma H \sigma^{-1}$, because for $\rho \in G$ we have $\rho|_L = \mathrm{id} \iff \sigma\rho\sigma^{-1}|_{\sigma(L)} = \mathrm{id}$. Hence:

$$\begin{aligned} H \lhd G &\iff \sigma H \sigma^{-1} = H \ \ \forall \sigma \in G \\ &\iff \sigma(L) = L \ \ \forall \sigma \in G \ \ \cdots (\star) \ \text{(by Galois corresp. Th.34)}. \end{aligned}$$

By the surjection (Lem. 19):

$$G = \operatorname{Hom}_K(F, \mathbb{C}) \ni \sigma \longmapsto \sigma|_L \in \operatorname{Hom}_K(L, \mathbb{C}),$$

$(\star)$ is equivalent to say that every $\tau \in \operatorname{Hom}_K(L, \mathbb{C})$ maps L into L, i.e. L/K is Galois (Prop. 24(ii)). In this case, the surjection above is a gp. hom. $G \twoheadrightarrow \operatorname{Gal}(L/K)$ with kernel $= \{\sigma \in G \mid \sigma|_L = \mathrm{id}\} = H$. □

Lecture 9 (23 Oct, Tu.)

Example. (*5th roots of unity*) $\zeta = \zeta_5 := \exp\Big(\dfrac{2\pi i}{5}\Big)$: a root of

$$X^5 - 1 = (X - 1)(X^4 + X^3 + X^2 + X + 1).$$

We know (will prove later) $X^4 + X^3 + X^2 + X + 1$ is irred. in $\mathbb{Q}[X]$, hence is the min. poly. of ζ over $\mathbb{Q}$. Recall $\mathbb{Q}(\boldsymbol{\mu}_5) = \mathbb{Q}(\zeta)$ and $\operatorname{Gal}\big(\mathbb{Q}(\zeta)/\mathbb{Q}\big) = \{\mathrm{id}, \sigma, \sigma^2, \sigma^3\}$, where:

$$\mathrm{id} : \zeta \mapsto \zeta, \ \sigma : \zeta \mapsto \zeta^2, \ \sigma^2 : \zeta \mapsto \zeta^4, \ \sigma^3 : \zeta \mapsto \zeta^3,$$

and $G \cong \big(\mathbb{Z}/(5)\big)^\times \cong C_4$ (Prop. 28): $\begin{array}{ccc} \zeta & \overset{\sigma}{\longmapsto} & \zeta^2 \\ {\scriptstyle\sigma}\uparrow & & \downarrow{\scriptstyle\sigma} \\ \zeta^3 & \underset{\sigma}{\longmapsto} & \zeta^4 \end{array}$ $(\zeta^5 = 1)$.

It has a subgp $H := \{\mathrm{id}, \sigma^2\} \cong C_2$, and σ^2 interchanges $\zeta \leftrightarrow \zeta^4$.

$$\begin{array}{ccc} \{\mathrm{id}\} & \longleftrightarrow & F=\mathbb{Q}(\zeta) \\ \cap & & \cup \\ H & \longleftrightarrow & L=? \\ \cap & & \cup \\ G & \longleftrightarrow & K=\mathbb{Q} \end{array}$$

$\Longrightarrow H$ fixes $\zeta+\zeta^4$, and $\sigma(\zeta+\zeta^4)=\zeta^2+\zeta^3$.

As $L:=F^H$ must be quadratic,

$\zeta+\zeta^4,\ \zeta^2+\zeta^3$ must be roots of a quad. eq'n $/\mathbb{Q}$.

$$\begin{cases} (\zeta+\zeta^4)+(\zeta^2+\zeta^3)=\zeta^4+\zeta^3+\zeta^2+\zeta=-1, \\ (\zeta+\zeta^4)(\zeta^2+\zeta^3)=\zeta^3+\zeta^4+\zeta+\zeta^2=-1. \end{cases}$$

$\Longrightarrow$ they are roots of X^2+X-1, i.e. $\dfrac{-1\pm\sqrt{5}}{2}$. $\therefore L=\mathbb{Q}\Big(\dfrac{-1\pm\sqrt{5}}{2}\Big)=\mathbb{Q}(\sqrt{5})$.

Now ζ,ζ^4 are roots of $X^2-\Big(\dfrac{-1+\sqrt{5}}{2}\Big)X+1=0\quad[\because \mathrm{Re}\,(\zeta+\zeta^4)=\zeta+\zeta^4>0.]$

$$\Longrightarrow \zeta,\zeta^4=\frac{(-1+\sqrt{5})/2\pm\sqrt{(-1+\sqrt{5})^2/4-4}}{2}$$

$$=\frac{(-1+\sqrt{5})\pm\sqrt{-10-2\sqrt{5}}}{4}\quad\therefore \zeta=\frac{(-1+\sqrt{5})+\sqrt{-10-2\sqrt{5}}}{4}\ (\because \mathrm{Im}\,\zeta>0).$$

1.8. **Insolvability of quintics I: radical extensions.**

Example. $\zeta^3=1,\ \zeta\neq 1$. $F/\mathbb{Q}$: spl. field of $P:=X^3-2$. By Prop. 28 and 31:

$$\begin{array}{rl} F=\mathbb{Q}(\sqrt[3]{2},\zeta) & \begin{cases} \mathrm{Gal}(F/L)=\{\mathrm{id},\sigma,\sigma^2\},\ \ \sigma(\sqrt[3]{2})=\sqrt[3]{2}\zeta,\ \sigma|_L=\mathrm{id}, \\ \mathrm{Gal}(L/K)=\{\mathrm{id},\tau\},\ \ \tau(\zeta)=\zeta^2. \end{cases} \\ \text{Kummer, } \mathbb{Z}/3\mathbb{Z}\ \Big| & \\ L=\mathbb{Q}(\zeta) & \text{extend } \tau \text{ to } \rho\in\mathrm{Gal}(F/K), \text{ say:} \\ \text{cyclo., } C_2\ \Big| & \rho(\zeta)=\zeta^2,\ \ \rho(\sqrt[3]{2})=\sqrt[3]{2}. \\ K=\mathbb{Q} & (\exists \text{ 3 choices for roots of } \tau P=X^3-2.) \end{array}$$

$$\Longrightarrow\ \rho^2=\mathrm{id},\ \ \rho\sigma\rho^{-1}:\ \begin{array}{l} \sqrt[3]{2}\overset{\rho^{-1}}{\longmapsto}\sqrt[3]{2}\overset{\sigma}{\longmapsto}\sqrt[3]{2}\zeta\overset{\rho}{\longmapsto}\sqrt[3]{2}\zeta^2 \\ \zeta\overset{\rho^{-1}}{\longmapsto}\zeta^2\overset{\sigma}{\longmapsto}\zeta^2\overset{\rho}{\longmapsto}\zeta \end{array}$$

$\Longrightarrow\ \rho\sigma\rho^{-1}=\sigma^2$. $\therefore \mathrm{Gal}(F/K)\cong D_6\cong S_3$ (non-abelian).[9]

Idea: Solving radicals (cyclo/Kummer ext'ns) can only produce a tower of *abelian* ext'ns $\longrightarrow$ a limited class of Galois ext'ns.

Definition 36. Let F/K be a finite ext'n inside $\mathbb{C}$. It has a finite set of generators (Prop. 10(ii)), and the ext'n E/K generated by *all* conjugates (over K) of all of these generators is Galois (Prop. 10(i), 24(iv)). As every Galois ext'n of K inside $\mathbb{C}$ containing F must contain E by Prop. 24(iii),

[9]Exercise: write out the 3 order 2 subgps & the corresponding cubic subfields (see Example in §2.2).

it is the minimal Galois ext'n of K containing F. In particular it is independent of the choice of generators. We call E/K the *Galois closure* of F/K.

Example. (i) $\mathbb{Q}(\sqrt[3]{2},\zeta)=\mathbb{Q}(\sqrt[3]{2},\sqrt[3]{2}\zeta,\sqrt[3]{2}\zeta^2)$ is the Galois closure of $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$.
(ii) If $F=K(\alpha)$ (PET, Th. 20), then its Galois closure is $E=K(\alpha_1,\dots,\alpha_n)$, where $\alpha=\alpha_1,\dots,\alpha_n$ are conj. of α over K (i.e. the spl. field of P_α).

Remark. By Galois theory (Th. 34), if $G:=\mathrm{Gal}(E/K)$ then $G':=\mathrm{Gal}(E/F)$ is its subgroup; F/K corresponds to the pair (G,G').

$$\begin{array}{ccc} E & \longleftrightarrow & \{\mathrm{id}\} \\ \cup & & \cap \\ F & \longleftrightarrow & G' \\ \cup & & \cap \\ K & \longleftrightarrow & G \end{array}$$

Definition 37. We say a pair (G,G') of a finite group G and its subgroup G' is *soluble* if there is a sequence (G_i) of subgroups $G=G_0\supset G_1\supset\cdots\supset G_{n-1}\supset G_n=G'$ with $G_{i-1}\rhd G_i$ (normal) and G_{i-1}/G_i cyclic for $1\le i\le n$. We say G is *soluble* if $(G,\{\mathrm{id}\})$ is.

A Galois ext'n is called *soluble* if its Galois group is soluble.

Example. The symmetric groups S_3,S_4 are soluble:

$$S_3 \overset{2}{\rhd} A_3 \overset{3}{\rhd} \{\mathrm{id}\},\quad S_4 \overset{2}{\rhd} A_4 \overset{3}{\rhd} V_4 \overset{2}{\rhd} C_2 \overset{2}{\rhd} \{\mathrm{id}\}.$$

Lemma 38. (i) *Let G be a finite group. If $G\rhd H\supset G'$, then:*

$$(G,G')\text{ : soluble }\iff G/H,\ (H,G')\text{ : both soluble}.$$

(ii) *Finite abelian groups are soluble.*

Proof. (i): Let $p:G\twoheadrightarrow G/H$ be the canonical surjection $\sigma\mapsto\sigma H$.
($\Rightarrow$): If (G_i) is a sequence for (G,G'), then $\big(p(G_i)\big),\ (H\cap G_i)$ give sequences for $G/H,\ (H,G')$:

$$\begin{array}{ccccc} (H\cap G_{i-1})/(H\cap G_i) & \hookrightarrow & G_{i-1}/G_i & \twoheadrightarrow & p(G_{i-1})/p(G_i) \\ \text{cyclic} & \Longleftarrow & \text{cyclic} & \Longrightarrow & \text{cyclic} \end{array}$$

($\Leftarrow$): If $(G_i),(H_i)$ are sequences for $G/H,\ (H,G')$, then combine $\big(p^{-1}(G_i)\big)$ and (H_i):

$$\begin{array}{ccccccccc} G/H=G_0 & \rhd & G_1 & \rhd & \cdots & \rhd & G_m=\{\mathrm{id}\} & & \\ \uparrow{\scriptstyle p} & & \uparrow{\scriptstyle p} & & & & \uparrow{\scriptstyle p} & \text{cyclic} & \text{cyclic} \\ G=p^{-1}(G_0) & \rhd & p^{-1}(G_1) & \rhd & \cdots & \rhd & p^{-1}(G_m)=H=H_0 & p^{-1}(G_{i-1})/p^{-1}(G_i) \xrightarrow[p]{\cong} & G_{i-1}/G_i \end{array}$$

$$\rhd\ H_1\ \rhd\cdots\rhd\ H_n=G'$$

(ii): Induction on $|G|$. If $G\ni\sigma\ne\mathrm{id}$ and $H=\langle\sigma\rangle$, then H is cyclic and $|G/H|<|G|$, so use (i)($\Leftarrow$). [or: Str. Th'm.] □

Example. S_n is *not* soluble for $n\ge5$. ($\because$ $S_n\rhd A_n$ and A_n $(n\ge5)$ is simple non-abelian hence not soluble; use Lem. 38(i)($\Rightarrow$).)

Lecture 10 (25 Oct, Th., 201st birthday of Évariste Galois)

Definition 39. We say a Galois ext'n L/K inside $\mathbb{C}$ is *radical* if there is a finite ext'n F of L such that F/K is a succession of cyclotomic and Kummer ext'ns, i.e. $K = K_0 \subset K_1 \subset \cdots \subset K_n = F$, with K_i/K_{i-1} : cyclo. or Kummer.

Theorem 40. *Radical extensions are soluble.* [10]

Proof. Let L/K be radical and take F/L as in Def. Let E/K be the Galois closure of F/K, and $G := \mathrm{Gal}(E/K)$, $H := \mathrm{Gal}(E/L)$ and $G' := \mathrm{Gal}(E/F)$. As cyclo./Kummer ext'ns are abelian, (G, G') is soluble by the Galois correp. (Th. 34, Cor. 35) and Lem. 38(ii),(i)($\Leftarrow$). Hence $G/H \cong \mathrm{Gal}(L/K)$ (Cor. 35) is soluble by Lem. 38(i)($\Rightarrow$). □

$$
\begin{array}{ccccccc}
 & & & & E & \longleftrightarrow & \{\mathrm{id}\} \\
 & & & & | & & \cap \\
 & & K_n & = & F & \longleftrightarrow & G' = G_n \\
\text{cyclo. (abelian) or} & & | & & | & & \cap \quad \triangle \\
\text{Kummer (cyclic)} & & \vdots & & L & \longleftrightarrow & H \quad \vdots \\
 & & | & & | & & \triangle \quad \triangle \\
 & & K_0 & = & K & \longleftrightarrow & G = G_0
\end{array}
\qquad \text{soluble}
$$

Remark. (oral) (i) Recall the Example in the beginning (S_3).
(ii) There are many equations whose spl. fields have Galois group S_n (examples later).
(iii) Next we prove that "general eqn's" (the roots $\alpha, \beta, \gamma, \ldots$ are transcendental numbers) of deg. n have Galois group S_n. Hence there cannot be a formula to solve quintics (or higher) by radicals ($\because$ S_n not soluble).

1.9. **Insolvability of quintics II: general equations.**

Definition 41. Let $K \subset \mathbb{C}$ and $P \in K[X]$. The *Galois group* $\mathrm{Gal}(P)$ of P is defined as the Galois group $\mathrm{Gal}(F/K)$ for the splitting field F of P over K.

Next: For "general" equation P of degree n, we have $\mathrm{Gal}(P) \cong S_n$.

Proposition 42. *Let $K \subset \mathbb{C}$ and $P \in K[X]$.*

(i) *Then $\mathrm{Gal}(P)$ is a subgroup of the autom. group $\mathrm{Aut}\big(\mathrm{Root}_P(\mathbb{C})\big)$ of the finite set $\mathrm{Root}_P(\mathbb{C})$. In particular, a choice an ordering of the roots $\mathrm{Root}_P(\mathbb{C}) = \{\alpha_1, \ldots, \alpha_n\}$ gives an injection $\mathrm{Gal}(P) \hookrightarrow S_n = \mathrm{Aut}\big(\{1, \ldots, n\}\big)$.*

(ii) *If P is irred. in $K[X]$ with $\deg P = n$, then $\mathrm{Gal}(P)$ is isomorphic to a* transitive *subgroup $G \subset S_n$ i.e. for every $i, j \in \{1, \ldots, n\}$, there exists $\sigma \in G$ with $\sigma(i) = j$.*

[10] We can extend the definition of radical ext'ns to any (non-Galois) finite ext'n, and prove that its Galois closure is soluble (see Appendix 1).

Remark. As a reordering in (i) amounts to a *conjugation* in S_n, we can consider $\mathrm{Gal}(P)$ as a subgroup of S_n, well-def'd up to conjugation.

Proof. (i): Let F be the spl. field of P over K. An el't $\sigma \in \mathrm{Gal}(P) = \mathrm{Gal}(F/K)$, being a K-hom., maps $\mathrm{Root}_P(\mathbb{C})$ into itself. As σ is injective (Lem. 11) and $\mathrm{Root}_P(\mathbb{C})$ is a finite set, $\sigma : \mathrm{Root}_P(\mathbb{C}) \to \mathrm{Root}_P(\mathbb{C})$ is a bijection (autom.). As F/K is generated by $\mathrm{Root}_P(\mathbb{C})$, the action of σ on $\mathrm{Root}_P(\mathbb{C})$ determines σ.

(ii): As P is irred. of deg. n, $|\mathrm{Root}_P(\mathbb{C})| = n$ by Prop. 15(i). If $\mathrm{Root}_P(\mathbb{C}) = \{\alpha_1, \dots, \alpha_n\}$, then P is the min. poly. of α_i for all i, hence for every i, j there exists $\tau \in \mathrm{Hom}_K\big(K(\alpha_i), \mathbb{C}\big)$ with $\tau(\alpha_i) = \alpha_j$ by Prop. 14. Extending this τ to $\sigma \in \mathrm{Hom}_K(F, \mathbb{C}) = \mathrm{Gal}(F/K)$ by Lem. 19, we get $\sigma(\alpha_i) = \alpha_j$. □

Example. (i) If a cyclic subgroup of S_n is transitive, then it has order n.
(ii) Transitive subgroups of S_3 are: $A_3 \cong C_3,\ S_3$.
(iii) Transitive subgroups of S_4 are, up to conj.: $C_4,\ V_4,\ D_8,\ A_4,$ and S_4.
(Here $V_4 := \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\} \cong C_2 \times C_2$, the *Klein 4-group*.)
(iv) Transitive subgroups of S_5 are, up to conj.: $C_5,\ D_{10},\ F_{20},\ A_5,$ and S_5.
(Here $F_{20} := \langle (12345), (1)(2453) \rangle$, the *Frobenius group of order 20*.)

Remark. (oral) All transitive subgroups of S_n appear as $\mathrm{Gal}(P)$ for some $P \in K[X]$ for some K, but $\mathrm{Gal}(P)$ is the whole S_n for "most" irred. eq'ns P of deg. n.

Definition 43. Let K be a field, $X_1, \dots, X_n$ be indeterminates, and $K[X_1, \dots, X_n]$ be the ring of poly. in $X_1, \dots, X_n$ with coefficients in K (an integral domain). Its field of fractions is denoted by $K(X_1, \dots, X_n)$, the *field of rational functions in n variables $/K$*.

Proposition 44. *Let $n \geq 1$.*

(i) *There exist $\alpha_1, \dots, \alpha_n \in \mathbb{C}$, transcendental over $\mathbb{Q}$, such that the field $F := \mathbb{Q}(\alpha_1, \dots, \alpha_n) \subset \mathbb{C}$ is isom. to $\mathbb{Q}(X_1, \dots, X_n)$ by $X_i \mapsto \alpha_i$ for $1 \leq i \leq n$.*
(ii) *The symmetric group $G := S_n$ acts on F by permuting $\alpha_1, \dots, \alpha_n$, and F/F^G is Galois with the Galois group G.*

Proof. (i): Use induction on n. As $L := \mathbb{Q}(\alpha_1, \dots, \alpha_{n-1})$ is isom. to $\mathbb{Q}(X_1, \dots, X_{n-1})$ (ind. hyp.), it is countable, hence only countably many el'ts in $\mathbb{C}$ are alg. $/L$. So choose $\alpha_n \in \mathbb{C}$ which is transcendental over L. Then there is no non-zero $P(X_1, \dots, X_n) \in \mathbb{Q}[X_1, \dots, X_n]$ with $P(\alpha_1, \dots, \alpha_n) = 0$, hence the ring hom. $f : \mathbb{Q}[X_1, \dots, X_n] \ni P \longmapsto P(\alpha_1, \dots, \alpha_n) \in \mathbb{C}$ is injective, and extends to a ring hom. $f : \mathbb{Q}(X_1, \dots, X_n) \ni \dfrac{P}{Q} \longmapsto \dfrac{P(\alpha_1, \dots, \alpha_n)}{Q(\alpha_1, \dots, \alpha_n)} \in \mathbb{C}$ because $\mathbb{C}$ is a field. Then $F := \mathrm{Im}\, f$ is isom. to $\mathbb{Q}(X_1, \dots, X_n)$, and it is the minimal field containing $\alpha_1, \dots, \alpha_n$, i.e. $\mathbb{Q}(\alpha_1, \dots, \alpha_n)$.

(ii): G acts on $\mathbb{Q}(X_1,\dots,X_n)$ by permuting X_i, hence also on F, i.e. $\sigma \in G$ acts as $f\sigma f^{-1}$, by permuting α_i. Let $K := F^G$. Then $F = \mathbb{Q}(\alpha_1,\dots,\alpha_n)$ implies $F = K(\alpha_1,\dots,\alpha_n)$, and $G \subset \mathrm{Aut}_K(F)$ by Lem. 32(ii). The coefficients of $P = \prod_{i=1}^{n}(X-\alpha_i) \in F[X]$ are the elementary symmetric poly.'s in α_i, hence in K. Hence α_i are the roots of $P \in K[X]$, i.e. alg. $/K$. Thus F/K is finite (Prop. 10(i)), and Prop. 33(ii) shows that F/K is Galois and $G = \mathrm{Gal}(F/K)$. □

Theorem 45. (Insolvability of Quintics) *For $n \geq 5$, there is no formula, involving only radicals and rational functions, which expresses $\alpha_1,\dots,\alpha_n$ in terms of their elementary symmetric polynomials.*

Proof. The Galois ext'n F/F^G in Prop. 44 is not soluble, hence not radical by Th. 40. □

Lecture 11 (27 Oct, Sa.)

1.10. **Solving by radicals.**

Next goal: Converse of Th. 40, i.e. all soluble ext'ns are radical.

Recall: soluble groups are built out of cyclic groups.

Definition 46. A Galois ext'n is called *cyclic* if its Galois group is cyclic.

Recall: for $N \geq 1$ and $\boldsymbol{\mu}_N \subset K \subset \mathbb{C}$, *Kummer ext'ns* of K are $K(\sqrt[N]{a})/K$ for $a \in K$. Their Galois groups inject to $\mathbb{Z}/N\mathbb{Z}$ (Prop. 31), hence they are cyclic.

Example. For $N = 2$, as $\boldsymbol{\mu}_2 = \{\pm 1\} \subset K$ for any $K \subset \mathbb{C}$, every quadratic ext'n is Kummer (i.e. every quad. eq'n is solved by $\sqrt{}$).

Theorem 47. (Kummer Theory) *Let $N \geq 1$ and $\boldsymbol{\mu}_N \subset K \subset \mathbb{C}$. Then every cyclic ext'n of K with degree N is a Kummer ext'n.*

Proof. Let L/K be cyclic of deg. N. Choose a generator σ of the Galois group: $\mathrm{Gal}(L/K) = \{\mathrm{id}, \sigma, \sigma^2, \dots, \sigma^{N-1}\}$. Let $\zeta = \zeta_N \in \boldsymbol{\mu}_N$.

Suppose we found $\alpha \in L^\times (= L \setminus \{0\})$ with $\sigma(\alpha) = \alpha\zeta$. Then the conjugates of α over K are $\sigma^i(\alpha) = \alpha\zeta^i$ for $1 \leq i \leq N$ (Prop. 14), and these are all distinct. Hence $[K(\alpha) : K] = N$ (Prop. 7(ii)), therefore $K(\alpha) = L$. Let $a := \alpha^N$. Then $\sigma(a) = \sigma(\alpha^N) = \sigma(\alpha)^N = (\alpha\zeta)^N = a$, so a is fixed by all σ^i, hence $a \in K$ (Prop. 33(i)). $\therefore\ L = K(\sqrt[N]{a})$.

So STP: considering σ as a K-linear transformation of L as a K-v.s., ζ is an eigenvalue of σ. Let $Q \in K[X]$ be the min. poly. of σ (as in Linear Algebra). Then $\Lambda := \mathrm{Root}_Q(K)$ is the set of all eigenvalues of σ. We want $\zeta \in \Lambda$.

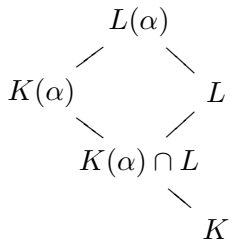
As $\sigma^N = \mathrm{id}$, we have $Q \mid X^N - 1$, hence $\Lambda \subset \boldsymbol{\mu}_N$. Now Λ is a multiplicative subgroup of $\boldsymbol{\mu}_N$, because if $\lambda, \mu \in \Lambda$ and $\sigma(\alpha) = \lambda\alpha,\ \sigma(\beta) = \mu\beta$ for $\alpha, \beta \in L^\times$, then as σ is a ring hom. $\sigma(\alpha\beta) = (\lambda\alpha)(\mu\beta) = (\lambda\mu)\cdot\alpha\beta$ and $\sigma(\alpha^{-1}) = (\lambda\alpha)^{-1} = \lambda^{-1}\alpha^{-1}$, i.e. $\lambda\mu, \lambda^{-1} \in \Lambda$.

Hence $\Lambda = \boldsymbol{\mu}_d$ for some $d|N$, i.e. $Q = X^d - 1$. But σ has order N, so $\sigma^d \neq \mathrm{id}$ unless $d = N$. $\therefore\ Q = X^N - 1,\ \Lambda = \boldsymbol{\mu}_N$ and $\zeta \in \Lambda$. □

Corollary: soluble ext'ns are radical as long as K contains $\boldsymbol{\mu}_N$ for large enough N.

Lemma 48. *Let $K \subset L \subset F$ and $\alpha \in F$. If $K(\alpha)/K$ is Galois, then $L(\alpha)/L$ is Galois, and $\mathrm{Gal}\big(L(\alpha)/L\big) \ni \sigma \longmapsto \sigma|_{K(\alpha)} \in \mathrm{Gal}\big(K(\alpha)/K\big)$ is an injective group hom.*

Proof. As the min. poly. of α over L divides that of α over K, by Prop. 24(iii) all conj. of α over L are in $K(\alpha) \subset L(\alpha)$, hence $L(\alpha)/L$ is Galois (Prop. 24(iv)). The map is clearly a group hom., and injective as σ is determined by $\sigma(\alpha)$, hence by $\sigma|_{K(\alpha)}$. □



Remark. The image corresponds to $K(\alpha) \cap L$ by Galois theory, i.e. $\mathrm{Gal}\big(L(\alpha)/L\big) \xrightarrow{\cong} \mathrm{Gal}\big(K(\alpha)/K(\alpha) \cap L\big)$.

Theorem 49. *Soluble ext'ns inside $\mathbb{C}$ are radical.*

Proof. Let L/K be Galois with $\mathrm{Gal}(L/K) = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{\mathrm{id}\}$ and G_{i-1}/G_i cyclic. Let $K_i := L^{G_i}$ be the corresponding subfields under Galois theory (Th. 34), so $K = K_0 \subset K_1 \subset \cdots \subset K_n = L$ with K_i/K_{i-1} cyclic, $\mathrm{Gal}(K_i/K_{i-1}) \cong G_i/G_{i-1}$ (Cor. 35). Let $N_i := |G_{i-1}/G_i|$ for $1 \leq i \leq n$, and $N := N_1 \cdots N_n$. Then we have a tower of fields $K \subset K(\boldsymbol{\mu}_N) \subset K_1(\boldsymbol{\mu}_N) \subset \cdots \subset K_n(\boldsymbol{\mu}_N) = L(\boldsymbol{\mu}_N)$, with $L \subset L(\boldsymbol{\mu}_N)$. Applying Lem. 48 to $K_i := K_{i-1}(\alpha)$ (PET, Th. 20), we see that $K_i(\boldsymbol{\mu}_N) = K_{i-1}(\boldsymbol{\mu}_N)(\alpha)$ is cyclic over $K_{i-1}(\boldsymbol{\mu}_N)$ of degree dividing N_i ($\because$ its Galois group is isom. to a subgroup of G_{i-1}/G_i), hence N. Thus $K_i(\boldsymbol{\mu}_N)/K_{i-1}(\boldsymbol{\mu}_N)$ is Kummer by Kummer Theory (Th. 47). □

1.11. **Discriminants, and revisiting Intro 1.**

Any formula for solving eq'ns by radicals? We need normal subgps of $\mathrm{Gal}(P)$ to climb up the splitting field of P, but the only non-trivial normal subgps of S_n are A_n and V_4.

Definition 50. Let $n \geq 1$, $K \subset \mathbb{C}$ and $P \in K[X]$ with $\deg P = |\mathrm{Root}_P(\mathbb{C})| = n$. Let $i : \mathrm{Gal}(P) \hookrightarrow S_n$ be the injection in Prop. 42, defined up to conjugation in S_n. If $H \lhd S_n$ (normal), then we have a well-defined normal subgroup $\mathrm{Gal}(P) \cap H := i^{-1}(H)$ of $\mathrm{Gal}(P)$.

First consider $H = A_n$.

Let P as in Def. 50, F/K its spl. field and $\mathrm{Root}_P(\mathbb{C}) = \{\alpha_1, \ldots, \alpha_n\} \curvearrowleft \mathrm{Gal}(P)$. Let:

$$\Delta_P := \prod_{i<j} (\alpha_i - \alpha_j)^2 = (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j} (\alpha_i - \alpha_j) \in F. \quad \text{(called the } \textit{discriminant} \text{ of } P)$$

As the RHS is clearly fixed by $\mathrm{Gal}(P)$, it is in K by Prop. 33(i). Note that $\Delta_P \neq 0$ because we assumed $|\mathrm{Root}_P(\mathbb{C})| = n$. For example:

$$\begin{cases} P = X^2 - aX + b & \Longrightarrow \Delta_P = (\alpha-\beta)^2 = a^2 - 4b, \\ P = X^3 + bX - c & \Longrightarrow \Delta_P = (\alpha-\beta)^2(\beta-\gamma)^2(\gamma-\alpha)^2 = -4b^3 - 27c^2, \end{cases}$$

where we used α, β, γ for $\alpha_1, \alpha_2, \alpha_3$.

Lecture 12 (30 Oct, Tu.)

Proposition 51. *For P as in Def. 50, we have*

$$\mathrm{Gal}(P) \subset A_n \iff \Delta_P \textit{ : square in } K \quad \cdots(*),$$

and the subgroup $\mathrm{Gal}(P) \cap A_n$ of $\mathrm{Gal}(P)$ corresponds to $K\big(\sqrt{\Delta_P}\big)$ by Galois theory.

Proof. Take one of the square roots of Δ_P (depending on the ordering of roots!)

$$\sqrt{\Delta_P} := \prod_{i<j} (\alpha_i - \alpha_j),$$

and consider the action of $\sigma \in \mathrm{Gal}(P) \hookrightarrow S_n$ on it. As a transposition (ij) changes signs of $\alpha_i - \alpha_j,\ \alpha_i - \alpha_m,\ \alpha_m - \alpha_j$ for $i < m < j$, it sends $\sqrt{\Delta_P}$ to $-\sqrt{\Delta_P}$. Hence we have

$$\sigma \in \mathrm{Gal}(P) \cap A_n \iff \sigma\big(\sqrt{\Delta_P}\big) = \sqrt{\Delta_P}. \quad \cdots(\star)$$

Now we prove $(*)$. ($\Leftarrow$): If $\sqrt{\Delta_P} \in K$, then every $\sigma \in \mathrm{Gal}(P)$ is in $\mathrm{Gal}(P) \cap A_n$ by $(\star)$. ($\Rightarrow$): As $(\star)$ says $\sqrt{\Delta_P}$ is fixed by all $\sigma \in \mathrm{Gal}(P)$, it is in K by Prop. 33(i).

The latter claim is clear if either side of $(*)$ is true. If not, then $\mathrm{Gal}(P) \cap A_n$ has index 2 in $\mathrm{Gal}(P)$, and its fixed field L satisfies $[L : K] = 2$ by Th. 34. Now $(*)$ says $[K\big(\sqrt{\Delta_P}\big) : K] = 2$ and $(\star)$ says $K\big(\sqrt{\Delta_P}\big) \subset L$, hence $K\big(\sqrt{\Delta_P}\big) = L$. □

Example. Let $P = X^3 + bX - c \in K[X]$ be irred. with $\mathrm{Root}_P(\mathbb{C}) = \{\alpha, \beta, \gamma\}$ (distinct). Then $\mathrm{Gal}(P)$ is A_3 or S_3 (Prop. 42(ii)), and Prop. 51 tells you which, e.g. when $K = \mathbb{Q}$:

$$\begin{cases} P = X^3 - 3X + 1 : & \Delta_P = 81 & \Longrightarrow \mathrm{Gal}(P) \cong A_3, \\ P = X^3 + 2X + 2 : & \Delta_P = -140 & \Longrightarrow \mathrm{Gal}(P) \cong S_3. \end{cases}$$

Now we revisit Lecture 1. To make the Kummer theory work for cyclic cubic extensions, we assume $\zeta = \zeta_3 \in K$. For a cubic with distinct roots

$$P = X^3 + bX - c = (X-\alpha)(X-\beta)(X-\gamma) \in K[X]$$

and its Langrange resolvents $x = \alpha + \beta\zeta + \gamma\zeta^2,\ y = \alpha + \beta\zeta^2 + \gamma\zeta$, the el'ts x^3, y^3 were the roots of $X^2 - 27cX - 27b^3$. Let $L := K(x^3) = K(y^3)$.

$$\begin{array}{ccc} K(\alpha,\beta,\gamma) = F = K(x) & \longleftrightarrow & \{\mathrm{id}\} \\ \big| \leq 3 & & \cap \\ L = K(x^3) & \longleftrightarrow & \mathrm{Gal}(P) \cap A_3 \\ \big| \leq 2 & & \cap \\ K & \longleftrightarrow & \mathrm{Gal}(P) \end{array}$$

Solving the quadratic shows $L = K\big(\sqrt{-27\Delta_P}\big)$, but $-27 = (3\sqrt{-3})^2 = (3(2\zeta+1))^2$ is a square in K, hence $L = K\big(\sqrt{\Delta_P}\big)$.

For a quartic with distinct roots

$$P = X^3 + bX^2 - cX + d = (X-\alpha)(X-\beta)(X-\gamma)(X-\delta) \in K[X],$$

recall we had

$$x := \alpha+\beta = -(\gamma+\delta), \quad y := \alpha+\gamma = -(\beta+\delta), \quad z := \alpha+\delta = -(\beta+\gamma),$$
$$xyz = c, \quad x^2, y^2, z^2 : \text{roots of } X^3 + 2bX^2 + (b^2-4d)X - c^2.$$

For $G := \mathrm{Gal}(P)$,

$$G \ \rhd \ G \cap A_4 \ \rhd \ G \cap V_4 \ \rhd \ \{\mathrm{id}\},$$

coming from the solubility of S_4:

$$S_4 \rhd A_4 \rhd V_4 \rhd C_2 \rhd \{\mathrm{id}\}, \text{ with}$$
$$S_4/V_4 \cong S_3, \quad V_4 \cong C_2 \times C_2,$$

and S_3 permutes x^2, y^2, z^2.

$$\begin{array}{ccc} K(\alpha,\beta,\gamma,\delta) = F = K(x,y,z) & \longleftrightarrow & \{\mathrm{id}\} \\ \text{biquad.} \big| \leq 4 & & \cap \\ L = K(x^2,y^2,z^2) & \longleftrightarrow & \mathrm{Gal}(P) \cap V_4 \\ \big| \leq 3 & & \cap \\ K\big(\sqrt{\Delta_P}\big) & \longleftrightarrow & \mathrm{Gal}(P) \cap A_4 \\ \big| \leq 2 & & \cap \\ K & \longleftrightarrow & \mathrm{Gal}(P) \end{array}$$

Exercise. (Appendix 1) Every cyclo. ext'n is contained in a tower of Kummer ext'ns (do induction on N for $K(\boldsymbol{\mu}_1, \boldsymbol{\mu}_2, \ldots, \boldsymbol{\mu}_N)$). So cyclo. ext'ns are not needed in the def. of radical ext'ns.

Solving eq'ns is related to *ruler-and-compass constructions*: in terms of Cartesian coord. $(x,y) \in \mathbb{R}^2$ or $x+yi \in \mathbb{C}$, it can only do $+, -, \times, \div$ and solve *quadratic* eq'ns (intersection with circles), so all coord. of the *obtained* points lie in a successive quadratic ext'ns of the field generated over $\mathbb{Q}$ by the coord. of *given* points.

Example. (i) Cannot *trisect a general given angle* — $\cos\alpha$ generates a cubic ext'n of $\mathbb{Q}(\cos 3\alpha)$; a successive quadratic ext'ns have degree 2^n, hence cannot contain a cubic ext'n by Tower Law (Prop. 8). Similarly, cannot *double a given cube* — solving $X^3 - 2$ is also cubic (the altar of Apollo at Delphi; oracle to the Delians).
(ii) Constructing *regular N-gons* — essential cases are when $N = p$ prime. Need to solve

$$(X^p - 1)/(X-1) = X^{p-1} + \cdots + X^2 + X + 1 \in \mathbb{Q}[X],$$

which is irreducible (set $X = Y + 1$ and use Eisenstein's criterion; we prove a more general theorem later). This is impossible unless $p-1$ is a power of 2; only known such primes are $2, 3, 5, 17, 257$ and 65537 (it has to be of the form $2^{2^m}+1$, called *Fermat primes*, as $2^b+1 \mid 2^{ab}+1$ if a is odd). We'll see that these cases are constructible (Gauss).

Lecture 13 (1 Nov, Th.)

2. General Fields and Applications

(oral) In this section, we generalise §1 to arbitrary fields (pre-war 20c; see Appendix 2), and discuss applications to Galois groups over $\mathbb{Q}$.

2.1. **General remarks.**

Definition 52. Let K be a field. The kernel of the unique ring hom. $f : \mathbb{Z} \ni n \mapsto 1 + \cdots (n \text{ times}) \cdots + 1 \in K$ from $\mathbb{Z}$ is a prime ideal in $\mathbb{Z}$. Hence $\mathrm{Ker}\, f = (p)$ for $p = 0$ or a prime number p, the *characteristic* of K, denoted by $\mathrm{char}\, K$.

If $\mathrm{char}\, K = 0$, then f is injective and extends to $\mathbb{Q} \hookrightarrow K$, hence its image is a subfield isom. to $\mathbb{Q}$ (unique isom.). If $\mathrm{char}\, K = p > 0$, then $\mathrm{Im}\, f \cong \mathbb{Z}/(p) =: \mathbb{F}_p$ is a subfield isom. to $\mathbb{F}_p$ (again unique isom.). In both cases $\mathrm{Im}\, f$ is the smallest subfield (*prime field*) of K.

Remark. When we have a *fixed* ring hom. $\tau : K \to L$ of fields (hence τ : inj. by Lem. 11), we may want to identify the isomorphic fields K and $\tau(K)$, and consider L as an extension of K. We do this only in the following two cases: [(11)]

(i) Every field can be considered as an ext'n of $\mathbb{Q}$ or $\mathbb{F}_p$ in a unique way, as its prime field is uniquely isom. to $\mathbb{Q}$ or $\mathbb{F}_p$.

(ii) If $P \in K[X]$ is an irred. poly., then (P) is a maximal ideal of $K[X]$ and $K_P := K[X]/(P)$ is a field. The *canonical* injection $K \hookrightarrow K[X]$ gives a ring hom. $K \hookrightarrow K[X] \twoheadrightarrow K[X]/(P)$, hence $K \hookrightarrow K_P$ (Lem. 11, or: non-zero constants are not in (P)). We consider $K \subset K_P$, and call K_P/K the ext'n obtained by *adjoining a root of* P (the root $\overline{X} := X \bmod P \in K_P$ is an "abstract" root of P, which generates K_P/K).

Example. $X^2 + 1 \in \mathbb{F}_3[X]$: irred. ($\because\ 0^2 = 0,\ 1^2 = 2^2 = 1 \neq -1$ in $\mathbb{F}_3$).
$\Longrightarrow \mathbb{F}_3[X]/(X^2+1) = \{0,\ 1,\ 2,\ X,\ X+1,\ X+2,\ 2X,\ 2X+1,\ 2X+2 \bmod X^2+1\}$
$\cdots$ quadratic ext'n of $\mathbb{F}_3$ (a field with 9 el'ts, isom. to $\mathbb{Z}[i]/(3)$).

(iii) (non-example) $K = \mathbb{Q}(\sqrt[3]{2})$ has three $\mathbb{Q}$-hom's $\tau_1, \tau_2, \tau_3 : K \hookrightarrow \mathbb{C}$. Apart from $\tau_1 = \mathrm{id}$, we'd rather *not* identify K with $\tau_2(K)$ or $\tau_3(K)$ — because K is given as a subfield of $\mathbb{C}$, and $\tau_2(K), \tau_3(K)$ are different subsets of $\mathbb{C}$, though *isomorphic* as fields.

Remark. (oral) Once we start considering ext'ns of K which are not subsets of a fixed set ($\mathbb{C}$ in §1) but sticking out into nowhere, the notion of K-isom's gets more important. K-isomorphic ext'ns share many properties (they "look the same" from the K-point of view): algebraicity; finiteness; degree; structure of subfields; Hom sets with other ext'ns; Root sets of poly.'s. But we don't *identify* K-isomorphic ext'ns (e.g. (iii) above), and we also care about *how many* K-isom's there are (e.g. Galois groups).

[(11)] In (i) τ is *unique*, and in (ii) τ is *canonical*, i.e. uniquely fixed by the context.

2.2. **Splitting fields and algebraic closures.** The only tool (from GR&M):

Lemma 53. *For any field K, the ring $K[X]$ is a Euclidean domain. Hence:*

(i) $\alpha \in \mathrm{Root}_P(K) \iff X - \alpha \mid P$ *in* $K[X]$ *(use* $P = (X-\alpha)Q + \beta$*).*

(ii) $K[X]$ *is a PID, hence a UFD. In particular,* $|\mathrm{Root}_P(K)| \leq \deg P$.

Definition 54. For $P \in K[X] \setminus K$ (i.e. non-const.) and an ext'n E/K, we say P *splits in* E if P is a product of linear factors in $E[X]$. If moreover E is generated by $\mathrm{Root}_P(E)$, then we say E is a *splitting field* of P over K.

As $|\mathrm{Root}_P(E)|$ is finite (Lem. 53), a spl. field is finite over K (Prop. 10(i)). If P splits in E, then it contains a unique spl. field of P, i.e. its subfield gen'd by $\mathrm{Root}_P(E)$ over K.

Lemma 55. *Let E/K be a splitting field of P over K. Then for an ext'n E'/K:*

$$P \text{ splits in } E' \iff \mathrm{Hom}_K(E, E') \neq \emptyset.$$

The number $|\mathrm{Root}_P(E')|$ *is constant for any E' in which P splits.*

Proof. ($\Rightarrow$): For a root α_1 of P, its min. poly. P_1 over K divides P, hence splits in E'. Choose $\beta_1 \in \mathrm{Root}_{P_1}(E')$, and let $\tau \in \mathrm{Hom}_K\big(K(\alpha_1), E'\big)$ be the K-hom. with $\tau(\alpha_1) = \beta_1$ (Prop. 14). Now factor $P = (X-\alpha_1)Q$ in $K(\alpha_1)[X]$ and choose a root α_2 of Q. Its min. poly. P_2 over $K(\alpha_1)$ divides Q, hence P. As $P_2 \mid P$ we have $\tau P_2 \mid \tau P = P$, hence τP_2 splits in E'. So choosing $\beta_2 \in \mathrm{Root}_{P_2}(E')$, we get $\rho \in \mathrm{Hom}_K\big(K(\alpha_1, \alpha_2), E'\big)$ with $\rho(\alpha_i) = \beta_i$ $(i = 1, 2)$ by Prop. 17. Repeating, we arrive at an el't in $\mathrm{Hom}_K(E, E')$ because $E = K(\alpha_1, \ldots, \alpha_n)$ if $\mathrm{Root}_P(E) = \{\alpha_1, \ldots, \alpha_n\}$.

($\Leftarrow$): If $\tau \in \mathrm{Hom}_K(E, E')$ and $P(X) = \prod_{i=1}^{n} (X - \alpha_i)^{m_i}$ in $E[X]$, then $P(X) = \tau P(X) = \prod_{i=1}^{n} \big(X - \tau(\alpha_i)\big)^{m_i}$ in $E'[X]$, as $\tau|_K = \mathrm{id}$. This also shows $|\mathrm{Root}_P(E')| = n = |\mathrm{Root}_P(E)|$ by the unique factorisation in $E'[X]$. □

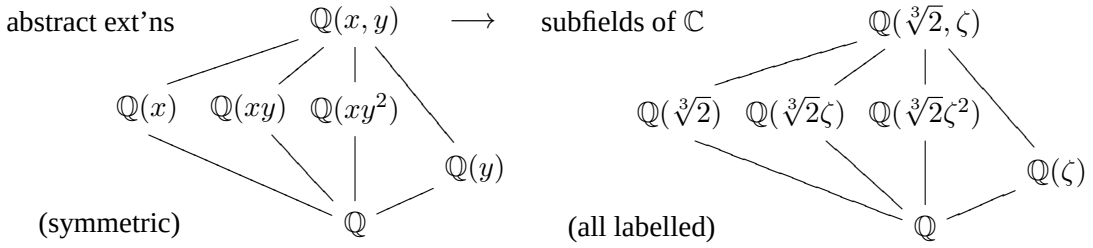
Proposition 56. *For every $P \in K[X] \setminus K$, its splitting field over K exists, and is unique up to K-isom. (i.e. there exists a (possibly many) K-isom. between any two of them).*

Proof. (Existence) Let L/K be the ext'n obtained by adjoining a root of an irreducible factor of P, as in Remark (ii) after Def. 52. Then $L = K(\alpha_1)$ with $\alpha_1 \in \mathrm{Root}_P(L)$, and $P = (X - \alpha_1) \cdot Q$ in $L[X]$. Then adjoin a root of an irred. factor of Q, and repeat. Each step is a simple ext'n gen'd by a root of P, hence after $\deg P$ steps we get a finite ext'n E/K, gen'd by all roots of P, and P splits in E.

(Uniqueness) If E, E' are both splitting fields of P over K, then by Lem. 55 we have $\mathrm{Hom}_K(E, E') \neq \emptyset$ and $\mathrm{Hom}_K(E', E) \neq \emptyset$, hence $[E : K] = [E' : K]$ by Lem. 22(i), and any el't in $\mathrm{Hom}_K(E, E')$ is a K-isom. by Lem. 22(ii). □

Lecture 14 (3 Nov, Sa.)

Example. $\mathbb{Q}(x,y) := \mathbb{Q}[X,Y]/(X^3-2,\ Y^2+Y+1),\ x=\overline{X},\ y=\overline{Y}.\ \zeta=\zeta_3.$



$\exists\ 6\ \mathbb{Q}$-hom's $\mathbb{Q}(x,y)\to\mathbb{C} : x\mapsto$ any of $\sqrt[3]{2},\ \sqrt[3]{2}\zeta,\ \sqrt[3]{2}\zeta^2,\ \ y\mapsto$ any of ζ,ζ^2.

Definition 57. A field F is called *algebraically closed* if every $P\in F[X]\setminus F$ splits in F itself. An alg. ext'n F/K is called an *algebraic closure* of K if F is algebraically closed.

Theorem 58. *For every field K, its alg. closure $\overline{K}$ exists and is unique up to K-isom. Any alg. ext'n of K is K-isomorphic to a subext'n of $\overline{K}/K$.*

Almost a proof. (Existence) Suppose $\{P_1,P_2,\ldots\}$ is the set of all irred. monics$^{(*A)}$ in $K[X]$. Let K_1 be a spl. field of P_1 over K, then K_2 be a spl. field of P_2 over K_1, and so on, to obtain a sequence $K=K_0\subset K_1\subset K_2\subset\cdots$, and let $\overline{K}:=\bigcup_{i=0}^{\infty}K_i$. Then it is an alg. ext'n of K (each step is a finite ext'n), in which all irred's in $K[X]$ split. Then $\overline{K}$ is alg. closed: for every $P\in\overline{K}[X]$, its coefficients belong to some K_i, hence all the roots of P are alg. over K_i, hence over K, hence already in $\overline{K}$.

(Uniqueness) Let F be another alg. closure of K. As P_1 splits in F, we have $\tau_1\in\mathrm{Hom}_K(K_1,F)$ by Lem. 55. As $P_2=\tau_1P_2$ splits in F, we have $\tau_2\in\mathrm{Hom}_K(K_2,F)$ extending τ_1. Repeating, after making infinitely many choices$^{(*B)}$, we obtain $\tau\in\mathrm{Hom}_K(\overline{K},F)$. (Same procedure gives a K-hom. from any alg. ext'n of K into F.) As every el't in F is alg. over K, hence a root of some P_i, it is in $\tau(\overline{K})$. Thus $\tau:\overline{K}\to F$ is a K-isom.

Remark. (oral) The real proof is obtained by making (*A),(*B) valid using *Zorn's Lemma*, an equivalent form of the *Well-Ordering Th'm* and the *Axiom of Choice* (Appendix 3).[12] We will not use algebraic closures in the sequel, but sometimes refer to $\overline{K}$ when it helps the understanding.

2.3. **Example I: Finite fields.**

Lemma 59. *Let K be a field with q el'ts ($q\in\mathbb{N}$; suppose such K exists). Then:*

(i) *$q=p^d$ for some $d\geq 1$, where $p=\mathrm{char}\,K$.*

(ii) *Every el't in K is a root of $X^q-X\in\mathbb{F}_p[X]$, which splits in K. In particular, K is a splitting field of X^q-X over $\mathbb{F}_p$.*

[12] For (*A), even when K countable one needs to order the irred. factors of P_{n+1} over K_n.

Proof. (i): As $\mathbb{Q} \subsetneq K$, we have $\operatorname{char} K = p > 0$ and $\mathbb{F}_p \hookrightarrow K$. If $[K : \mathbb{F}_p] = \infty$, then $|K| = \infty$, hence $[K : \mathbb{F}_p] =: d < \infty$. Then $K \cong \mathbb{F}_p^d$ as $\mathbb{F}_p$-v.s., hence $|K| = p^d$.

(ii): $K^\times = K \setminus \{0\}$ (multiplicative group) is a finite group of order $q-1$, hence every $x \in K^\times$ satisfies $x^{q-1} = 1$ by Lagrange. Thus $X^q - X = X(X^{q-1} - 1)$ has q distinct roots in K (all el'ts of K), hence splits in K. The roots clearly generate K over $\mathbb{F}_p$. □

Remark. Recall $x^p = x \ \forall x \in \mathbb{F}_p$ by Fermat.

Conversely, we'll show the existence of K by proving that $X^q - X$ has q distinct roots in its splitting field.

Definition 60. Let K be a field. Recall that $K[X]$ has $\{1, X, X^2, \ldots\}$ as its basis as K-v.s. Let the *derivation* $D : K[X] \to K[X]$ be the K-linear map defined by $D(1) = 0$ and $D(X^n) = nX^{n-1}$ $(\forall n \geq 1)$.

Proposition 61. *Let K be a field.*

(i) $D(PQ) = D(P)Q + D(Q)P \ \ (\forall P, Q \in K[X])$.

(ii) $\alpha \in K$ *: multiple root of* $P \iff X - \alpha$ *divides both* $P, D(P)$ *in* $K[X]$.

Proof. (i): Both sides are K-bilinear in P, Q, and $D(X^m \cdot X^n) = D(X^m) \cdot X^n + D(X^n) \cdot X^m$ $(\forall m, n \geq 0)$. (ii): If $P = (X - \alpha) \cdot Q$, then $D(P) = Q + (X - \alpha)D(Q)$ by (i). Hence $X - \alpha \mid D(P) \iff X - \alpha \mid Q \iff \alpha$: multiple root. □

Corollary 62. *If* $(\operatorname{char} K, N) = 1$ *(by which we mean:* $\operatorname{char} K = 0$ *or* $\operatorname{char} K$ *does not divide* N*), then* $X^N - 1$ *has no multiple root in* K.

Proof. Since $N \neq 0$ in K, the only root of $D(X^N - 1) = NX^{N-1}$ is 0, which is not a root of $X^N - 1$. □

Remark. If $\operatorname{char} K = p > 0$, then $D(X^p - 1) = pX^{p-1} = 0$ and $X^p - 1 = (X - 1)^p$ (multiple root); see below.

Lemma 63. *If* $\operatorname{char} K = p > 0$*, then the map* $K \to K$ *defined by* $x \mapsto x^p$ *is a ring hom. (hence an* $\mathbb{F}_p$*-hom.).*

Proof. $0^p = 0, \ 1^p = 1, \ (ab)^p = a^p b^p$.

$$\begin{aligned}(a+b)^p &= a^p + \sum_{i=1}^{p-1} \binom{p}{i} a^{p-i} b^i + b^p \\ &= a^p + b^p \quad (\because \binom{p}{i} = \frac{p!}{i!(p-i)!} = 0 \ \text{[divisible by } p\text{]}\ ).\end{aligned}$$ □

Definition 64. The $\mathbb{F}_p$-hom. in Lem. 63 is called the *Frobenius map* of K, which we denote by Fr_p. For $q = p^d$, its d-th iterate $\mathrm{Fr}_q := (\mathrm{Fr}_p)^d : K \to K$ is the *q-th power Frobenius map*.

Lecture 15 (6 Nov, Tu.)

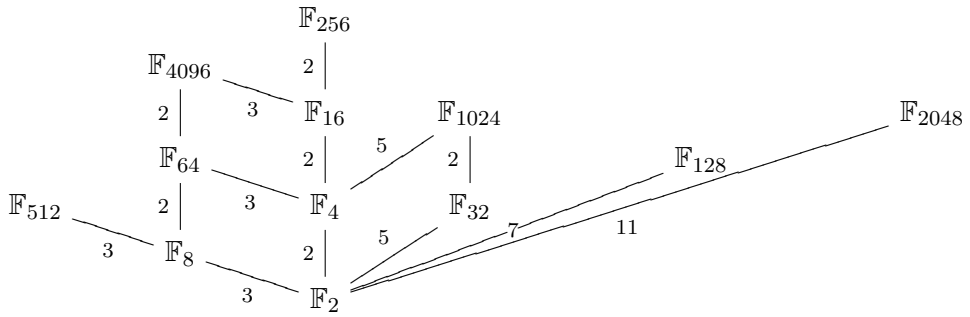
Theorem 65. (i) *For each prime power $q = p^d$, there exists a field with q el'ts, unique up to $\mathbb{F}_p$-isom. (i.e. field isom.). This field is denoted by $\mathbb{F}_q$.* [13]

(ii) *Let $d, d' \geq 1$ and $q = p^d,\ q' = p^{d'}$. Then $\mathbb{F}_{q'}$ contains $\mathbb{F}_q$ if and only if d' is a power of d, i.e. $d \mid d'$. If $q' = q^n$, then $[\mathbb{F}_{q'} : \mathbb{F}_q] = n$.*

Proof. (i): Let K be a splitting field of $X^q - X$ over $\mathbb{F}_p$ (Prop. 56). By Cor. 62, $X^q - X$ has q distinct roots in K (as p does not divide $q-1$). Then the set of all roots $\{x \in K \mid x^q = x\}$ is a subfield of K by Lem. 63 ($\because\ a^q = a,\ b^q = b \Longrightarrow (a+b)^q = a+b,\ (ab)^q = ab,\ (a^{-1})^q = (a^q)^{-1} = a^{-1}$). As K is a splitting field, i.e. gen'd by these roots, it is equal to this subfield and $|K| = q$. By Lem. 59 every field with q el'ts is $\mathbb{F}_p$-isom. to this one, by the uniquness of splitting fields (Prop. 56).

(ii): If $q' = q^n$, then every root of $X^q - X$ is a root of $X^{q'} - X$, since $x^q = x$ implies $x^{q'} = (\cdots (x^q)^q \cdots)^q = x$, hence $\mathbb{F}_{q'}$ contains $\mathbb{F}_q$. Conversely, if $\mathbb{F}_q \subset \mathbb{F}_{q'}$, then $\mathbb{F}_{q'}$ is an $\mathbb{F}_q$-v.s., and if $[\mathbb{F}_{q'} : \mathbb{F}_q] = n$, then $q' = |\mathbb{F}_{q'}| = |\mathbb{F}_q|^n = q^n$. □

Example. We have the same diagram for every p, but $p = 2$ below.
The union of all these fields is $\overline{\mathbb{F}}_p$, and $\mathbb{F}_q = \{x \in \overline{\mathbb{F}}_p \mid x^q = x\}$ for $q = p^d$.



Lemma 66. *Consider a finite ext'n $\mathbb{F}_{q^n}/\mathbb{F}_q$. Then $\mathrm{Fr}_q : x \mapsto x^q$ is an $\mathbb{F}_q$-autom. of $\mathbb{F}_{q^n}$ with order n, i.e. $\{\mathrm{id}, \mathrm{Fr}_q, \mathrm{Fr}_q^2, \ldots, \mathrm{Fr}_q^{n-1}\} \subset \mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^n})$.*

Proof. The map Fr_q fixes all el'ts in $\mathbb{F}_q$ (the roots of $X^q - X$), hence an $\mathbb{F}_q$-hom. Being an injective map (Lem. 11) of a finite set $\mathbb{F}_{q^n}$ into itself, it is bijective, hence an $\mathbb{F}_q$-autom. Since $x^{q^n} = x\ (\forall x \in \mathbb{F}_{q^n})$ we have $\mathrm{Fr}_q^n = \mathrm{id}$ on $\mathbb{F}_{q^n}$, i.e. the order of Fr_q in $\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^n})$ divides n. But, for each $m \mid n$, the el'ts fixed by Fr_q^m are exactly the el'ts of $\mathbb{F}_{q^m}$, so the order is n. □

Remark. For non-finite K with $\mathrm{char}\, K = p$, the Frobenius map is injective but not an automorphism (e.g. $\mathrm{Fr}_p : \mathbb{F}_p(X) \to \mathbb{F}_p(X)$ has image $\mathbb{F}_p(X^p)$).

[13] In contrast to $\mathbb{F}_p$, the field $\mathbb{F}_q$ is only well-defined up to non-canonical isomorphisms. But since any field contains at most one copy of $\mathbb{F}_q$ by Lem. 59, this notation causes no ambuiguity in most contexts.

Lemma 67. *Let K be a field, and $K^\times = K \setminus \{0\}$ be its multiplicative group. Then every finite subgroup G of $K^\times$ is cyclic.*

Proof. Let $x \in G$ be an el't with the maximal order; call its order n. We show that for any $y \in G$, its order m has to divide n. Suppose not. Then $\exists p$ prime such that $m = p^j m',\ n = p^k n'$ where m', n' are not divisible by p and $j > k$. Let $z := x^{p^k} y^{m'}$. Then:

$$z^i = 1 \Longrightarrow x^{p^k i} = y^{-im'}$$

$$\Longrightarrow \begin{cases} x^{p^j p^k i} = y^{-im} = 1 \Longrightarrow n \mid p^{j+k} i \Longrightarrow n' \mid i \\ 1 = x^{ni} = y^{-im'n'} \Longrightarrow m \mid im'n' \Longrightarrow p^j \mid i \end{cases} \Longrightarrow p^j n' \mid i,$$

i.e. the order of z is $p^j n' > n$, contradiction.

Now $(x^{n/m})^i$ $(1 \le i \le m)$ are m distinct roots of $X^m - 1$ in K, hence all its roots (Lem. 53(ii)). As y is a root, it is a power of x. [$\exists$ proof via Str. Th'm. of fin. abelian groups.] □

Theorem 68. *Every finite ext'n $\mathbb{F}_{q^n}/\mathbb{F}_q$ of finite fields is simple and Galois, with*

$$\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) = \{\mathrm{id}, \mathrm{Fr}_q, \mathrm{Fr}_q^2, \dots, \mathrm{Fr}_q^{n-1}\} \cong \mathbb{Z}/n\mathbb{Z}.$$

Proof. By Lem. 67, $\mathbb{F}_{q^n}^\times = \mathbb{F}_{q^n} \setminus \{0\}$ is cyclic, i.e. $\mathbb{F}_{q^n} = \{0, 1, \zeta, \zeta^2, \dots, \zeta^{q^n-2}\}$ for some $\zeta \in \mathbb{F}_{q^n}$, hence $\mathbb{F}_{q^n} = \mathbb{F}_q(\zeta)$ (simple). If P_ζ is the min. poly. of ζ over $\mathbb{F}_q$, then $|\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^n})| \le |\mathrm{Hom}_{\mathbb{F}_q}(\mathbb{F}_{q^n}, \mathbb{F}_{q^n})| = |\mathrm{Root}_{P_\zeta}(\mathbb{F}_{q^n})| \le n$ by Prop. 14. Now Lem. 66 implies the rest. □

Remark. Th. 68 + Prop. 14 $\Longrightarrow$ Conjugates of ζ are $\{\mathrm{Fr}_q^i(\zeta) = \zeta^{q^i} \mid 0 \le i \le n-1\}$, i.e.:

$$P_\zeta(X) = (X - \zeta)(X - \zeta^q)(X - \zeta^{q^2}) \cdots (X - \zeta^{q^{n-1}}) \quad (\deg P_\zeta = n = [\mathbb{F}_{q^n} : \mathbb{F}_q]).$$

Example. Not all generators ζ of the group $\mathbb{F}_{q^n}^\times$ are conj. over $\mathbb{F}_q$. In $\mathbb{F}_2[X]$:

$$X^{16} - X = X(X+1)(X^2+X+1)(X^4+X^3+X^2+X+1)(X^4+X+1)(X^4+X^3+1),$$

whose roots are all el'ts in $\mathbb{F}_{16}$. The first 2 factors have roots in $\mathbb{F}_2 = \{0, 1\}$, the first 3 in $\mathbb{F}_4$. The roots of any of the latter 3 factors generate the deg. 4 ext'n $\mathbb{F}_{16}/\mathbb{F}_2$. The roots of last 2 are generators of $\mathbb{F}_{16}^\times$ (Lem. 67 says $\mathbb{F}_{16}^\times \cong C_{15} \cong C_3 \times C_5$, which has 8 generators; they form 2 groups of conjugates over $\mathbb{F}_2$).

Lecture 16 (8 Nov, Th.)

2.4. **Application I: Cyclotomic fields.**

Definition 69. For a field K and $N \ge 1$, let $K(\boldsymbol{\mu}_N)$ be a splitting field of $X^N - 1$ over K (*cyclotomic ext'n* of K), and $\boldsymbol{\mu}_N := \mathrm{Root}_{X^N-1}\big(K(\boldsymbol{\mu}_N)\big) \subset K(\boldsymbol{\mu}_N)^\times$, which lies in a finite ext'n of $\mathbb{Q}$ or $\mathbb{F}_p$ inside $K(\boldsymbol{\mu}_N)$. Then $\boldsymbol{\mu}_N$ is a finite multiplicative group, hence cyclic by Lem. 67. If $(\mathrm{char}\, K, N) = 1$, then $|\boldsymbol{\mu}_N| = N$ by Cor. 62, hence there exist *primitive* N-th roots of unity, i.e. $\zeta \in \boldsymbol{\mu}_N$ with order N. There are $|\big(\mathbb{Z}/(N)\big)^\times|$ of them, but no canonical choice like $e^{2\pi i/N} \in \mathbb{C}$.[14]

[14]Situation with the notation $K(\boldsymbol{\mu}_N)$ is similar to $\mathbb{F}_q$.

Proposition 70. (i) *There exists an* N-th cyclotomic polynomial $\Phi_N \in \mathbb{Z}[X]$ *for each* $N \geq 1$, *satisfying:* (a) *the equality*

$$X^N - 1 = \prod_{d|N} \Phi_d(X),$$

where d *runs through all positive divisors of* N *in the product,* (b) *for any field* K *with* $(\mathrm{char}\, K, N) = 1$, *denoting the image of* Φ_N *in* $K[X]$ *also by* Φ_N, *we have*

$$\mathrm{Root}_{\Phi_N}\big(K(\boldsymbol{\mu}_N)\big) = \{ \textit{ all primitive } N\textit{-th roots of unity } \} \subset \boldsymbol{\mu}_N.$$

(ii) *If* $(\mathrm{char}\, K, N) = 1$, *then* $K(\boldsymbol{\mu}_N)/K$ *is Galois, with the injective group hom.:*

$$\begin{aligned} \mathrm{Gal}\big(K(\boldsymbol{\mu}_N)/K\big) &\longrightarrow \big(\mathbb{Z}/(N)\big)^\times \\ (\zeta \mapsto \zeta^i \ \forall \zeta \in \boldsymbol{\mu}_N) &\longmapsto i \bmod N. \end{aligned}$$

If $[K(\boldsymbol{\mu}_N) : K] = n$, *then all irred. factors of* Φ_N *in* $K[X]$ *have degree* n.

Proof. (i): Use induction on N. By the ind. hyp., $\displaystyle\prod_{d|N,\ d<N} \Phi_d(X)$ is in $\mathbb{Z}[X]$, and its roots in $K(\boldsymbol{\mu}_N)$ are all the *non*-primitive N-th roots of 1, all distinct (Cor. 62). So it divides $X^N - 1$ in $K(\boldsymbol{\mu}_N)[X]$, and the roots of the quotient $\Phi_N(X)$ are the *primitive* N-th roots of 1. In particular when $K = \mathbb{Q}$, our $\Phi_N \in \mathbb{Q}(\boldsymbol{\mu}_N)[X]$ is obtained by the division algorithm as the quotient of $X^N - 1$ by a monic in $\mathbb{Z}[X]$, hence $\Phi_N \in \mathbb{Z}[X]$.

(ii): Let $[K(\boldsymbol{\mu}_N) : K] = n$ and ζ be a primitive N-th root of 1. As $K(\boldsymbol{\mu}_N) = K(\zeta)$ and the min. poly. P_ζ has $\deg P_\zeta = n$ distinct roots in $\boldsymbol{\mu}_N$ (Cor. 62), $K(\boldsymbol{\mu}_N)/K$ is Galois by the remark after Def. 23. If $\sigma(\zeta) = \zeta^i$, then $\sigma(\zeta^j) = (\zeta^i)^j = (\zeta^j)^i$ for all j. The map is injective as $i \bmod N$ determines σ ($\because$ $K(\boldsymbol{\mu}_N) = K(\zeta)$), and is a group hom. as $(\zeta \mapsto \zeta^i) \circ (\zeta \mapsto \zeta^j) = (\zeta \mapsto \zeta^{ij})$. Finally, every irred. factor of Φ_N is the min. poly. P_ζ for some primitive N-th root ζ by (i), hence has degree $[K(\zeta) : K] = n$. □

Example. $\Phi_2(X) = X + 1,\ \Phi_3(X) = X^2 + X + 1,\ \Phi_4(X) = X^2 + 1.$
$\Phi_5(X) = X^4 + X^3 + X^2 + X + 1,\ \Phi_6(X) = X^2 - X + 1.$

Example. Recall: in $\mathbb{F}_2[X]$,

$$\begin{aligned} X^{15} - 1 &= (X+1)(X^2+X+1)(X^4+X^3+X^2+X+1)(X^4+X+1)(X^4+X^3+1) \\ &= (\Phi_1 \bmod 2)(\Phi_3 \bmod 2)(\Phi_5 \bmod 2)(\Phi_{15} \bmod 2), \end{aligned}$$

so $\Phi_{15} \bmod 2$ is a product of two irred. factors. Note that roots of $\Phi_5 \bmod 2$ are not generators of $\boldsymbol{\mu}_{15}$ but still generate $\mathbb{F}_{16}$ over $\mathbb{F}_2$.

Example. Let $K = \mathbb{F}_q$ and $n \geq 1$. Since $\mathbb{F}_{q^n}^\times = \boldsymbol{\mu}_{q^n-1}$ we have $\mathbb{F}_{q^n} = \mathbb{F}_q(\boldsymbol{\mu}_{q^n-1})$ (spl. field of $X^{q^n} - X$, also of $X^{q^n-1} - 1$). So every finite ext'n of finite fields is a cyclotomic ext'n. Note

$(\operatorname{char} K, q^n - 1) = 1$. More generally, for $N \geq 1$ prime to q, let n be the order of $q \bmod N$ in $\big(\mathbb{Z}/(N)\big)^\times$. Then by Th. 68 and Prop. 70(ii):

$$\begin{aligned} \operatorname{Gal}\big(\mathbb{F}_q(\boldsymbol{\mu}_N)/\mathbb{F}_q\big) &\xrightarrow{\cong} \{1, q, q^2, \ldots, q^{n-1} \bmod N\} \subset \big(\mathbb{Z}/(N)\big)^\times \\ (\mathrm{Fr}_q : x \mapsto x^q) &\longmapsto q, \end{aligned}$$

is an isom., i.e. $\mathbb{F}_q(\boldsymbol{\mu}_N) = \mathbb{F}_{q^n}$, and all irred. factors of Φ_N in $\mathbb{F}_q[X]$ have deg. n. The previous Ex. is $q = 2$ and $N = 5$ or 15, and $n = 4$.

So we know how $\Phi_N \bmod p$ factorises for p prime to N. What about in $\mathbb{Z}[X]$? Simplest case: if $\big(\mathbb{Z}/(N)\big)^\times$ is cyclic and has a generator $p \bmod N$ with p prime, then $\Phi_N \bmod p$ is irred. (previous Ex.), hence so is Φ_N (if $\Phi_N = PQ$ then $\overline{\Phi_N} = \overline{P} \cdot \overline{Q}$, writing $\overline{P} := P \bmod p$). But e.g. for $N = 8$, $\Phi_8 \bmod p$ is reducible $\forall p$, but $\Phi_8 = X^4 + 1$ is irred. in $\mathbb{Z}[X]$.

Theorem 71. (Gauss, Irreducibility of Cyclotomic Polynomials) *For all $N \geq 1$, the poly. Φ_N is irreducible in $\mathbb{Q}[X]$ (hence also in $\mathbb{Z}[X]$ by Gauss' Lemma). In other words, the group hom. $\operatorname{Gal}\big(\mathbb{Q}(\boldsymbol{\mu}_N)/\mathbb{Q}\big) \longrightarrow \big(\mathbb{Z}/(N)\big)^\times$ in Prop. 70(ii) is an isom.*

Proof. STP: Φ_N is the min. poly. $/\mathbb{Q}$ of every primitive N-th roots of 1, i.e. all el'ts of $\operatorname{Root}_{\Phi_N}\big(\mathbb{Q}(\boldsymbol{\mu}_N)\big) = \{\zeta^a \mid a \in \big(\mathbb{Z}/(N)\big)^\times\}$ are conjugates over $\mathbb{Q}$. As every $a \in \big(\mathbb{Z}/(N)\big)^\times$ is some product of $p \bmod N$ for primes p not dividing N, STP: ζ^p is a conj. of ζ over $\mathbb{Q}$ for every p prime to N and every primitive ζ.

Let P_ζ be the min. poly. of ζ over $\mathbb{Q}$, and $\Phi_N = P_\zeta \cdot Q$ in $\mathbb{Q}[X]$. As Φ_N, P_ζ are monics, so is Q, hence $P_\zeta, Q \in \mathbb{Z}[X]$ by Gauss' Lemma (since $\Phi_N \in \mathbb{Z}[X]$).[(15)] Suppose ζ^p is not a root of P_ζ; then it's a root of Q. Then ζ is a root of $Q(X^p)$, hence $P_\zeta(X) \mid Q(X^p)$ in $\mathbb{Q}[X]$, hence in $\mathbb{Z}[X]$ (division by a monic in $\mathbb{Z}[X]$). Reducing this $\bmod p$ (and writing $\overline{P} := P \bmod p$), we have $\overline{P_\zeta(X)} \mid \overline{Q(X^p)} = \overline{Q(X)}^p$ in $\mathbb{F}_p[X]$ (here $(\sum a_i X^i)^p = \sum (a_i X)^p = \sum a_i X^p$, since p-th power is a ring hom. and fixes $a_i \in \mathbb{F}_p$). Thus $\overline{P_\zeta}, \overline{Q}$ have common roots in $\mathbb{F}_p(\boldsymbol{\mu}_N)$, but this contradicts Cor. 62 since $\overline{\Phi_N} \mid X^N - 1$ in $\mathbb{F}_p[X]$. □

Lecture 17 (10 Nov, Sa.)

Remark. (i) Later we'll see another "$\bmod p$ proof", i.e. proving that $\operatorname{Gal}(P)$ for $P \in \mathbb{Q}[X]$ (in fact $\mathbb{Z}[X]$) is large by showing $\operatorname{Gal}(P \bmod p)$ is large for some prime p (Th. 84).
(ii) Consider $N = 8$ and $\zeta = \zeta_8$, so $\Phi_8(X) = (X - \zeta)(X - \zeta^3)(X - \zeta^5)(X - \zeta^7)$. By building the theory of *number fields* and reducing $\mathbb{Z}[\zeta]$ modulo p to get $\mathbb{F}_p(\boldsymbol{\mu}_N) \ni \overline{\zeta} =$ "$\zeta \bmod p$" [in fact it's a natural way to obtain all finite ext'ns of $\mathbb{F}_p$], one sees from the Remark after Th. 68, that the

[(15)] For the statement of Gauss' Lemma that we're using, see Appendix 4.

factorisation of $\overline{\Phi_8} = \Phi_8 \bmod p$ in $\mathbb{F}_p[X]$ is:

$$\begin{cases} p \equiv 1 \bmod 8 & \Longrightarrow \overline{\Phi_8} = (X-\overline{\zeta})(X-\overline{\zeta}^3)(X-\overline{\zeta}^5)(X-\overline{\zeta}^7) \\ p \equiv 3 \bmod 8 & \Longrightarrow \overline{\Phi_8} = \big[(X-\overline{\zeta})(X-\overline{\zeta}^3)\big]\big[(X-\overline{\zeta}^5)(X-\overline{\zeta}^7)\big] \\ (\text{e.g. } p=3 & \Longrightarrow \Phi_8 \bmod 3 = (X^2+X-1)(X^2-X-1)\ ) \\ p \equiv 5 \bmod 8 & \Longrightarrow \overline{\Phi_8} = \big[(X-\overline{\zeta})(X-\overline{\zeta}^5)\big]\big[(X-\overline{\zeta}^3)(X-\overline{\zeta}^7)\big] \\ (\text{e.g. } p=5 & \Longrightarrow \Phi_8 \bmod 5 = (X^2-2)(X^2+2)\ ) \\ p \equiv 7 \bmod 8 & \Longrightarrow \overline{\Phi_8} = \big[(X-\overline{\zeta})(X-\overline{\zeta}^7)\big]\big[(X-\overline{\zeta}^3)(X-\overline{\zeta}^5)\big] \\ (\text{e.g. } p=7 & \Longrightarrow \Phi_8 \bmod 7 = (X^2+3X+1)(X^2-3X+1)\ ), \end{cases}$$

which explains why Φ_8 is irred. in $\mathbb{Q}[X]$: if it were factorised in $\mathbb{Z}[X]$ (into $(X-\zeta)(X-\zeta^3)$ etc.), every $\bmod p$ reduction must respect this. [16]

(iii) Th. 71 says $\mathbb{Q}(\boldsymbol{\mu}_N)/\mathbb{Q}$ has Galois group $\big(\mathbb{Z}/(N)\big)^\times$, an abelian group of order $\varphi(N) := |\{i \bmod N \mid 1 \le i < N,\ (i,N)=1\}$ (*Euler's function*). If $N = \prod_i p_i^{m_i}$, then $\varphi(N) = \prod_i \varphi(p_i^{m_i})$ and $\varphi(p^m) = p^{m-1}(p-1)$ for p prime.

Revisit the ruler-and-compass construction (Ex. in §1.11). A *regular N-gon*, i.e. points in $\mathbb{Q}(\boldsymbol{\mu}_N)$, are constructible iff $[\mathbb{Q}(\boldsymbol{\mu}_N):\mathbb{Q}] = \varphi(N)$ is a power of 2, iff $N = 2^a p_1 \cdots p_r$, where p_i are *distinct* Fermat primes. E.g. when $p = 17$ (Gauss, Ex. Sheet 2.10):

$$\begin{array}{ccc} \mathbb{Q}(\boldsymbol{\mu}_{17}) & \longleftrightarrow & \{\mathrm{id}\} \\ {\scriptstyle 2}\,\big| & & \cap \\ \mathbb{Q}(\alpha) & \longleftrightarrow & \{1,16\} \\ {\scriptstyle 2}\,\big| & & \cap \\ \mathbb{Q}(\beta) & \longleftrightarrow & \{1,13,16,4\} \\ {\scriptstyle 2}\,\big| & & \cap \\ \mathbb{Q}(\gamma) & \longleftrightarrow & \{1,9,13,15,16,8,4,2\} \\ {\scriptstyle 2}\,\big| & & \cap \\ \mathbb{Q} & \longleftrightarrow & \big(\mathbb{Z}/(17)\big)^\times \cong C_{16} \end{array}$$

$\zeta = \zeta_{17}$. $\alpha = \zeta + \zeta^{16} = 2\cos\dfrac{2\pi}{17}$, $\alpha' = \zeta^{13} + \zeta^4$: roots of $X^2 - \beta_1 X + \beta_3$, where

$$\left.\begin{array}{r} \beta = \beta_1 = \zeta + \zeta^{13} + \zeta^{16} + \zeta^4 \\ \beta_2 = \zeta^9 + \zeta^{15} + \zeta^8 + \zeta^2 \end{array}\right\} : \text{roots of } X^2 - \gamma X - 1,$$

β_3, β_4 : roots of $X^2 - \gamma' X - 1$.

$\gamma = \zeta + \zeta^9 + \cdots + \zeta^2$ (8 terms),

$\gamma' = \zeta^3 + \zeta^{10} + \cdots +$ (the rest).

$$\left.\begin{array}{l} \gamma + \gamma' = -1 \\ \gamma\gamma' = -4 \end{array}\right\} \Longrightarrow \gamma = \frac{-1+\sqrt{17}}{2}.$$

2.5. **Separability.**

Definition 72. A poly. $P \in K[X]$ is called *separable* if $|\mathrm{Root}_P(E)| = \deg P$ (i.e. no multiple root) when P splits in E/K (this def'n is independent of E by Lem. 55).

[16] This (or the previous Ex.) is a basic example of *Class Field Theory*, which gives a correspondence

$$\text{irred. } P \in \mathbb{Z}[X] \ \longrightarrow\ \text{"decomposition law" for } P \bmod p \in \mathbb{F}_p[X].$$

In turn, this law ("local" behaviour at each p) characterises the splitting field of P over $\mathbb{Q}$ (a number field). It is believed that all number fields (the whole of $\overline{\mathbb{Q}}$) have nice decomposition laws in terms of generalisations of $\big(\mathbb{Z}/(N)\big)^\times$, namely *modular forms*.

Lemma 73. *Let $P \in K[X]$.*

(i) *Let L/K be an ext'n. If P is separable and $Q \in L[X]$ divides P in $L[X]$, then Q is separable.*

(ii) *P is separable if and only if P and $D(P)$ are coprime in $K[X]$.*

(iii) *If P is irreducible, then P is separable if and only if $D(P) \neq 0$, i.e. P is not a poly. in X^p for $p = \operatorname{char} K$. In particular, all irred. poly's are separable if $\operatorname{char} K = 0$.*

(iv) *Suppose P is separable. If $\tau : K \hookrightarrow E$ is a field hom., then $\tau P \in E[X]$ is separable. In particular P is separable as a poly. in $L[X]$ for any ext'n L/K.*

Proof. (i): As P has no multiple root when split, neither does Q.

(ii): Let E be the spl. field of P. If $P, D(P)$ are coprime, then $\exists Q, R \in K[X]$ with $PQ + D(P)R = 1$ in $K[X]$ (recall Prop. 15(ii)), which remains true in $E[X]$, so $P, D(P)$ have no common root in E, hence P has no multiple root by Prop. 61(ii). If P and $D(P)$ had a common factor in $K[X]$, then they have a common root in E, hence a multiple root (Prop. 61(ii)).

(iii): As $\deg D(P) < \deg P$ and P is irred., P and $D(P)$ are coprime unless $D(P) = 0$.

(iv): τP and $\tau D(P) = D(\tau P)$ are coprime in $E[X]$ (send $PQ + D(P)R = 1$ by τ). □

Lecture 18 (13 Nov, Tu.)

Definition 74. An algebraic ext'n F/K is called *separable* (resp. *normal*) if for every $\alpha \in F$ its min. poly. P_α over K is separable (resp. splits in F).

We relate the separability with the K-hom's, as in §1.5 (Prop. 17 – Th. 18).

Lemma 75. *Let $F/K, E/K$ be two extensions of K. Let $K \subset L \subset F$ and $\alpha \in F$ be algebraic $/L$ with min. poly. P_α over L. Then:*

$$|\operatorname{Hom}_K\big(L(\alpha), E\big)| \leq \deg P_\alpha \cdot |\operatorname{Hom}_K(L, E)|,$$

where the equality holds if and only if $|\operatorname{Root}_{\tau P_\alpha}(E)| = \deg P_\alpha$ for all $\tau \in \operatorname{Hom}_K(L, E)$.

Proof. Immediate from Prop. 17, which gives a bijection for every $\tau \in \operatorname{Hom}_K(L, E)$:

$$\big\{\rho \in \operatorname{Hom}_K\big(L(\alpha), E\big) \;\big|\; \rho|_L = \tau\big\} \ni \rho \overset{\cong}{\longmapsto} \rho(\alpha) \in \operatorname{Root}_{\tau P_\alpha}(E). \quad \cdots(\star)$$ □

Proposition 76. *If F/K is finite, then $|\operatorname{Hom}_K(F, E)| \leq [F : K]$ for any ext'n E/K. If the equality holds for E/K, then for any intermediate field $K \subset L \subset F$ we have:*

(i) $|\operatorname{Hom}_K(L, E)| = [L : K]$, (ii) $\operatorname{Hom}_K(F, E) \ni \rho \mapsto \rho|_L \in \operatorname{Hom}_K(L, E)$ *is surjective.*

Proof. Let $F = K(\alpha_1, \dots, \alpha_n)$ (Prop. 10(ii)) and $K_i := K(\alpha_1, \dots, \alpha_i)$ so that $K = K_0 \subset K_1 \subset \cdots \subset K_{n-1} \subset K_n = F$ is a tower of simple ext'ns. By repeating Lem. 75,

$$\begin{aligned} |\mathrm{Hom}_K(F, E)| &\le [F : K_{n-1}] \cdot |\mathrm{Hom}_K(K_{n-1}, E)| \\ &\le \cdots \le [F : K_{n-1}][K_{n-1} : K_{n-2}] \cdots [K_{i+1} : K_i] \cdot |\mathrm{Hom}_K(K_i, E)| \\ &\le \cdots \le [F : K_{n-1}] \cdots [K_1 : K] = [F : K]. \qquad \text{(Tower Law Prop. 8)} \end{aligned}$$

If the equality holds, every $\le$ has to be $=$. For $K \subset L \subset F$, choose $\alpha_1, \dots, \alpha_n$ so that $L = K_i$. Then $[F : L] \cdot |\mathrm{Hom}_K(L, E)| = [F : K]$, hence (i) by Tower Law, and the condition in Lem. 75 shows that LHS of $(\star)$ is $\neq \emptyset$ for every step from $L = K_i$ to F, hence (ii). □

Theorem 77. *Let F/K be a finite ext'n.*

(i) *TFAE: (a) $\exists$ an ext'n E/K with $|\mathrm{Hom}_K(F, E)| = [F : K]$.*
(b) F/K is separable.
(c) $F = K(\alpha_1, \dots, \alpha_n)$ and the min. poly. Q_i of α_i over K is separable $(1 \le \forall i \le n)$.
(d) $F = K(\alpha_1, \dots, \alpha_n)$ and the min. poly. P_i of α_i over $K(\alpha_1, \dots, \alpha_{i-1})$ is separable $(1 \le \forall i \le n)$.

(ii) *If $K \subset L \subset F$, then F/K : separable $\iff$ $F/L, L/K$: both separable.*

(iii) *TFAE: (a) F/K is Galois.*
(b) F/K is separable and normal.
(c) $F = K(\alpha_1, \dots, \alpha_n)$ and the min. poly. Q_i of α_i over K is separable and splits in F $(1 \le \forall i \le n)$.

Proof. (i): (a)⇒(b): For every $\alpha \in F$ we have

$$|\operatorname{Root}_{P_\alpha}(E)| \overset{\text{Prop.14}}{=} |\mathrm{Hom}_K\big(K(\alpha), E\big)| \overset{\text{Prop.76}}{=} [K(\alpha) : K] \overset{\text{Prop.7(ii)}}{=} \deg P_\alpha.$$

(b)⇒(c): clear. (c)⇒(d): $P_i \mid Q_i$, so use Lem. 73(i). (d)⇒(a): Take E/K s.t. $Q_1 \cdots Q_n$ splits in E. We show that every $\le$ in the proof of Prop. 76 is $=$ by checking the condition in Lem. 75. For every $\tau \in \mathrm{Hom}_K(K_{i-1}, E)$, we have τP_i separable by Lem. 73(iv). As $\tau P_i \mid \tau Q_i = Q_i$ and Q_i splits in E, so does τP_i, thus $|\operatorname{Root}_{\tau P_i}(E)| = \deg P_i$.

(ii): Choose $\alpha_1, \dots, \alpha_n$ with $L = K_i$ and use (b)⇔(d).

(iii): Same proof as (i), in which we can take E to be F everywhere. □

Now we revisit §§1.5-1.7. For every finite sep. ext'n F/K, the assertions Th. 18 and Lem. 19 hold with $\mathbb{C}$ replaced by some field E, by Th. 77(i)(a), and Prop. 76(ii).

Theorem 78. (PET) *Every finite separable ext'n is simple.*

Proof. By Th. 77(i)(b)⇒(a) and Th. 20. □

Proposition 79. *The following hold without "inside $\mathbb{C}$": Cor. 26 and Prop. 42 with the condition "P is a product of separable poly's"; Cor. 35.*

Proof. Th. 77(iii) plays the role of Prop. 24(i)⇔(iii)⇔(iv). The latter part of the proof of Cor. 35 runs as: "by the surjection (Prop. 76(ii)) $G \to \mathrm{Hom}_K(L,F)$, $(\star)$ is equivalent to say that every $\tau \in \mathrm{Hom}_K(L,F)$ maps L into L. Since $|\mathrm{Hom}_K(L,F)| = [L:K]$ (Prop. 76(i)), L/K is Galois (note Lem. 22(iii))." For Cor. 26 and 42, replace $\mathbb{C}$ with F, and Lem. 19 with Prop. 76(ii). □

Remark. (oral) Cyclotomic ext'ns (Prop. 28, Cor. 29) were discussed in Prop. 70, hence everything in §1 not involving Kummer ext'ns and discriminants were generalised. Kummer theory (for cyclic deg. N ext'ns) is false when $\mathrm{char}\, K \mid N$, so *Artin-Schreier theory* (Ex. Sheet 3.10, 4.11) is needed, and discriminants wouldn't work when $\mathrm{char}\, K = 2$.

For example, applying Prop. 42(i) to finite fields gives:

Proposition 80. *Let $P \in \mathbb{F}_p[X]$ be a monic separable poly. of deg. n. If $P = Q_1 \cdots Q_m$ is the irred. factorisation in $\mathbb{F}_p[X]$ and $\deg Q_i = n_i$ (so $n = \sum n_i$), then $\mathrm{Fr}_p \in \mathrm{Gal}(P)$ has cycle type $(n_1, \ldots, n_m)$ when viewed as an el't of S_n (see Prop. 42).*

Remark. The injection $\mathrm{Gal}(P) \hookrightarrow S_n$ in Prop. 42 is only defined up to conjugation in S_n, but the cycle types are exactly the conjugacy classes in S_n, so are well-def'd.

Proof. Let $\mathbb{F}_q$ be the spl. field of P over $\mathbb{F}_p$. As $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p) = \{\mathrm{id}, \mathrm{Fr}_p, \mathrm{Fr}_p^2, \ldots, \mathrm{Fr}_p^{N-1}\}$ if $q = p^N$ (Th. 68), the conjugates of $\alpha \in \mathbb{F}_q$ over $\mathbb{F}_p$ are $\{\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{d-1}}\}$ for some $d \mid N$, which are permuted cyclically by Fr_p. Now $P = Q_1 \cdots Q_m$, and each Q_i, being irred., is the min. poly. of its root $\alpha_i \in \mathbb{F}_q$. Thus P splits in $\mathbb{F}_q[X]$ as:

$$\begin{aligned} P(X) = (X-\alpha_1)(X-\alpha_1^p)(X-\alpha_1^{p^2})\cdots(X-\alpha_1^{p^{n_1-1}}) \qquad & (\leftarrow Q_1) \\ \cdot\,(X-\alpha_2)(X-\alpha_2^p)\cdots(X-\alpha_2^{p^{n_2-1}}) \qquad & (\leftarrow Q_2) \\ \cdots\,(X-\alpha_m)(X-\alpha_m^p)\cdots(X-\alpha_m^{p^{n_m-1}}), \qquad & (\leftarrow Q_m) \end{aligned}$$

and Fr_p acts on these n roots by a permutation with cycle type $(n_1, \ldots, n_m)$. □

Lecture 19 (15 Nov, Th.)

2.6. **Example II: Symmetric Function Theorem.** Let K be a field and $n \geq 1$.

Recall: (Def. 43) $F := K(X_1, \ldots, X_n)$: the field of rational functions in n variables (the field of fractions for $K[X_1, \ldots, X_n]$). As used in proof of Prop. 42, the symmetric group $G := S_n$ acts on F by permuting $X_1, \ldots, X_n$, i.e. $G \subset \mathrm{Aut}_K(F)$. The fixed field F^G is the subfield consisting of all *symmetric* rational fu'ns in $X_1, \ldots, X_n$.

Definition 81. Let K, n, F, G be as above. For $1 \leq i \leq n$, let

$$s_i := \sum_{\{\lambda_1,\ldots,\lambda_i\} \subset \{1,\ldots,n\}} X_{\lambda_1} \cdots X_{\lambda_i} \in F^G$$

be the *i-th elementary symmetric polynomials*.

Proposition 82. (Rational Symmetric Function Theorem) *Let K, n, F, G be as above, and $L := K(s_1, \dots, s_n) \subset F$ be the subfield of F consisting of all rat'l fu'ns in $s_1, \dots, s_n$ with coeff. in K. Then $F^G = L$, i.e. all symmetric fu'ns are in L.*

Proof. As $s_1, \dots, s_n \in F^G$, we have $L \subset F^G$. As $X_1, \dots, X_n$ are the roots of

$$P(X) := (X - X_1) \cdots (X - X_n) = X^n - s_1 X^{n-1} + s_2 X^{n-2} - \cdots + (-1)^n s_n \in L[X],$$

$F = L(X_1, \dots, X_n)$ is a splitting field of P, finite over L. So F/F^G is also finite.
Path I: As F is a spl. field of P over L and P has no multiple roots, F/L is Galois and $\mathrm{Gal}(P) = \mathrm{Gal}(F/L)$ injects to G (permutations of X_i) by Prop. 79 (Cor. 26, Prop. 42). In particular F/L is simple (Th. 20), hence so is F/F^G. Now Prop. 33(ii) says F/F^G is Galois with $G = \mathrm{Gal}(F/F^G)$, and $F^G = L$ follows from

$$|G| = |\mathrm{Gal}(F/F^G)| = [F : F^G] \leq [F : L] = |\mathrm{Gal}(F/L)| \leq |G|.$$

Path II: We build from first principles. As $G \subset \mathrm{Aut}_{F^G}(F)$, we have:

$$n! = |G| \leq |\mathrm{Aut}_{F^G}(F)| \overset{\text{Th.20}}{\leq} [F : F^G] \leq [F : L]. \quad \cdots (*)$$

But a spl. field of P has degree at most $n!$ — more explicitly, let $L_i := L(X_1, \dots, X_i)$ for $1 \leq i \leq n$, so that $L = L_0 \subset L_1 \subset \cdots \subset L_n = F$. Then X_i is a root of

$$P_i(X) := \frac{P(X)}{(X - X_1) \cdots (X - X_{i-1})} = (X - X_i) \cdots (X - X_n) \in L_{i-1}[X], \quad \cdots (\star)$$

which has deg. $n - i + 1$, hence $L_i = L_{i-1}(X_i)/L_{i-1}$ has at most deg. $n - i + 1$. Thus $[F : L] \leq n(n-1) \cdots 2 \cdot 1 = n!$, hence $(*)$ implies $[F : L] = n!$ and $F^G = L$. □

Remark. Ex. Sheet 3.9, 3,11, 3,18* : similar to Paths I/II (finding fixed fields inside $K(X)$).

In Path II, as $[F : L] = n!$, we need $[L_i : L_{i-1}] = n - i + 1$ for all i, i.e. $Z_i := \{1, X_i, X_i^2, \dots, X_i^{n-i}\}$ is a basis of L_i/L_{i-1}. Hence:

$$Z := \{z_1 \cdots z_n \mid z_i \in Z_i\} = \{X_1^{m_1} \cdots X_n^{m_n} \mid 0 \leq m_i \leq n - i\}$$

is a basis of F/L (recall the proof of Tower Law (Prop. 8)).

Now revisit $(\star)$ with $n = 3,\ K = \mathbb{Q},\ (\alpha, \beta, \gamma) = (X_1, X_2, X_3)$.

$$\begin{aligned} P(X) &= X^3 - (\alpha + \beta + \gamma)X^2 + (\alpha\beta + \beta\gamma + \gamma\alpha)X - \alpha\beta\gamma \\ &= P_1(X) \in \mathbb{Z}[s_1, s_2, s_3][X] \\ &= (X - \alpha)\big(X^2 - (s_1 - \alpha)X + \big(s_2 - \alpha(s_1 - \alpha)\big)\big), \\ &\qquad \text{the 2nd factor } = P_2(X) \in \mathbb{Z}[s_1, s_2, s_3, \alpha][X], \\ &= (X - \alpha)(X - \beta)\big(X - (s_1 - \alpha - \beta)\big), \\ &\qquad \text{the last factor } = P_3(X) \in \mathbb{Z}[s_1, s_2, s_3, \alpha, \beta][X]. \end{aligned}$$

$$\begin{array}{ccc} \mathbb{Z}[\alpha, \beta, \gamma] & \subset & \mathbb{Q}(\alpha, \beta, \gamma) = F \\ \cup & & \cup \\ \mathbb{Z}[s_1, s_2, s_3] & \subset & \mathbb{Q}(s_1, s_2, s_3) = L \end{array}$$

Theorem 83. (SFT) *Let K, n, F, G be as above, and let R be any subring of K (e.g. $R = \mathrm{Im}\,(\mathbb{Z} \to K)$, i.e. $\mathbb{Z}$ or $\mathbb{F}_p$ according to $\mathrm{char}\, K$). Then inside F, we have*

$$R[X_1, \ldots, X_n] \cap F^G = R[s_1, \ldots, s_n],$$

i.e. every symmetric poly. with coeff. in R is a poly. in $s_1, \ldots, s_n$ with coeff. in R.

Proof. Clearly $R[s_1, \ldots, s_n] \subset R[X_1, \ldots, X_n] \cap F^G$. In $(\star)$, note that $P(X) \in R[s_1, \ldots, s_n][X]$ and $(X - X_1) \cdots (X - X_{i-1}) \in R[X_1, \ldots, X_{i-1}][X]$ are both monics with coeff. in the ring

$$R[s_1, \ldots, s_n, X_1, \ldots, X_{i-1}],$$

hence by the division algorithm we have $P_i(X) \in R[s_1, \ldots, s_n, X_1, \ldots, X_{i-1}][X]$, a monic of deg. $n - i + 1$. As $P_i(X_i) = 0$, we see that X_i^{n-i+1} is an $R[s_1, \ldots, s_n, X_1, \ldots, X_{i-1}]$-linear combination of $Z_i = \{1, X_i, X_i^2, \ldots, X_i^{n-i}\}$, hence so is any higher power of X_i.

Repeating this for $1 \le i \le n$, eventually every monomial $X_1^{m_1} \cdots X_n^{m_n}$ is an $R[s_1, \ldots, s_n]$-linear comb. of Z, which is a basis of F/L. Hence every $f \in R[X_1, \ldots, X_n]$ is expressed as an $R[s_1, \ldots, s_n]$-linear comb. of Z; if moreover $f \in F^G = L$, then it must be the unique expression of f as an L-linear comb. of Z, namely $f = f \cdot 1$. Thus $f \in R[s_1, \ldots, s_n]$. □

Remark. The proof shows $R[X_1, \ldots, X_n]$ is a free $R[s_1, \ldots, s_n]$-module of rank $n!$, with a basis Z. Actually $R[s_1, \ldots, s_n]$ is isomorphic to the poly. ring (in $s_1, \ldots, s_n$) over R, i.e. every symmetric poly. is *uniquely* written as a poly. in $s_1, \ldots, s_n$ (Appendix 5).

Lecture 20 (17 Nov, Sa.)

Example. Recall (after Def. 50) the discriminant for the splitting field $F = \mathbb{Q}(X_1, \ldots, X_n)$ of P over $L = \mathbb{Q}(s_1, \ldots, s_n)$. Then Th. 83 shows

$$\Delta_P := \prod_{i<j} (X_i - X_j)^2 \in \mathbb{Z}[X_1, \ldots, X_n] \cap L = \mathbb{Z}[s_1, \ldots, s_n].$$

E.g. $P = X^2 - s_1 X + s_2 \Rightarrow \Delta_P = s_1^2 - 4s_2$ and $P = X^3 + s_2 X - s_3 \Rightarrow \Delta_P = -4s_2^3 - 27s^3$. For $P = X^4 - s_3 X + s_4$ and higher, see Ex. Sheet 4.5, 4.15*.

2.7. **Application II: Galois groups over $\mathbb{Q}$.** *Recall:* Remark (i) after Th. 71.
We prove a theorem useful for determining $\mathrm{Gal}(P)$ over $\mathbb{Q}$ for $P \in \mathbb{Z}[X]$.

Theorem 84. *Let $P \in \mathbb{Z}[X]$ be a monic separable poly. (as $P \in \mathbb{Q}[X]$) of deg. n, and let p be a prime such that $P \bmod p \in \mathbb{F}_p[X]$ is also separable. If $P \bmod p = Q_1 \cdots Q_m$ is the irred. factorisation in $\mathbb{F}_p[X]$ and $\deg Q_i = n_i$, then $\mathrm{Gal}(P)$ contains an el't with cycle type $(n_1, \ldots, n_m)$ as an el't of S_n (see Remark after Prop. 80).*

Example. Let $P = X^5 + 2X + 6$. As $P \bmod 3 = X^5 - X = X(X-1)(X+1)(X^2+1)$ in $\mathbb{F}_3[X]$, Th. 84 shows that $\mathrm{Gal}(P)$ has an el't of cycle type $(1,1,1,2)$, i.e. a transoposition. If moreover $\mathrm{Gal}(P)$ has a 5-cycle, then $\mathrm{Gal}(P) \cong S_5$ by group theory (Ex. Sheet 4.9).

Proof. By Prop. 80, STP: $\mathrm{Gal}(P \bmod p) \subset \mathrm{Gal}(P)$ inside S_n, up to conjugation.

We use the setup in §2.6. Let $F := \mathbb{Q}(X_1, \dots, X_n)$, on which $G := S_n$ acts by permuting X_i, i.e. $\rho(X_i) := X_{\rho(i)}$ for $\rho \in G$. Recall $F^G = \mathbb{Q}(s_1, \dots, s_n)$, where s_i is the i-th elementary symm. poly. (Prop. 82). Let $A := \mathbb{Z}[s_1, \dots, s_n]$, a subring of $B := \mathbb{Z}[X_1, \dots, X_n]$. Then SFT (Th. 83) says $B \cap F^G = A$.

$$\begin{array}{ccc} B & \hookrightarrow & F \\ \cup & & \cup \\ A & \hookrightarrow & L = F^G \end{array}$$

rings $\overset{\text{Frac}}{\rightharpoonup}$ fields

Note that the action of G on F restricts to its action on B (permuting X_i). Consider another set of n-variables $T_1, \dots, T_n$, and define the 2nd action of G on the ring $B[T_1, \dots, T_n] = \mathbb{Z}[X_1, \dots, X_n, T_1, \dots, T_n]$ by permuting T_i as $\rho(T_i) := T_{\rho(i)}$. We write $\underline{T}$ for $T_1, \dots, T_n$. Now take a monic of deg. $n!$ in X, with coeff. in $B[\underline{T}]$:

$$R := \prod_{\sigma \in G} R_\sigma, \quad R_\sigma := X - \sum_{i=1}^{n} \sigma(X_i) T_i = X - (X_{\sigma(1)} T_1 + \cdots + X_{\sigma(n)} T_n) \in B[\underline{T}][X].$$

Then the two actions of $\rho \in G$ permutes the factors R_σ as $R_\sigma \mapsto R_{\rho\sigma}$ and $R_\sigma \mapsto R_{\sigma\rho^{-1}}$ respectively. In particular, their product R is fixed under both actions of G.

As R is fixed by the 1st G-action, so is each coeff. of $T_1^{m_1} \cdots T_n^{m_n} X^m$ (el'ts in B), hence they are in $B \cap F^G = A$. Thus $R \in A[\underline{T}][X]$.

Lemma 85. *Let K be a field, $P := X^n - a_1 X^{n-1} + \cdots + (-1)^n a_n \in K[X]$, and E/K be a splitting field of P over K with $\mathrm{Root}_P(E) = \{\alpha_1, \dots, \alpha_n\}$. This ordering gives the injection $H := \mathrm{Gal}(P) = \mathrm{Gal}(E/K) \hookrightarrow S_n = G$. Let A, B, R and R_σ be as above.*

Define a ring hom. $\tau : B \to E$ by $\tau(X_i) = \alpha_i$. Then $\tau R \in E[\underline{T}][X]$ lies in $K[\underline{T}][X]$, and if its irred. factorisation in $K(\underline{T})[X]$ is given by $\tau R = \prod_{H\sigma \in H\backslash G} \tau R_{H\sigma}$, where $H\backslash G$ is the set of right cosets, and $R_{H\sigma} := \prod_{\rho \in H\sigma} R_\rho \in B[\underline{T}][X]$. The stabiliser of $\tau R_{H\sigma} \in K(\underline{T})[X]$ under the 2nd G-action is $\sigma^{-1} H \sigma$.

Proof. As τ is a ring hom., $\tau R = \prod_{\sigma \in G} \tau R_\sigma$ in $E[\underline{T}][X]$. As $\tau(s_i) = a_i$, we have $\tau(A) \subset K$. Since $R \in A[\underline{T}][X]$, we have $\tau R \in K[\underline{T}][X]$.

For each coset $H\sigma$, the poly. $R_{H\sigma} \in B[\underline{T}][X]$ is fixed by the 1st action of $H \subset G$. Note that the 1st action of $H \subset G$ on X_i is sent by τ to the $H = \mathrm{Gal}(E/K)$-action on α_i. Hence $\tau R_{H\sigma} \in E[\underline{T}][X]$ is fixed by the action of $H = \mathrm{Gal}(E/K)$. Therefore so is each coeff. of $T_1^{m_1} \cdots T_n^{m_n} X^m$ (el'ts in E), thus they are in $E^H = K$ (Prop. 33(i)). Hence $\tau R =$

$$\begin{array}{ccc} B & \longrightarrow & E \\ G\,(\ \cup & & \cup\ )\,H \\ A & \longrightarrow & K \end{array}$$

$\prod_{H\sigma\in H\backslash G} \tau R_{H\sigma}$ in $K[\underline{T}][X]$. We show that this is the irred. factorisation in $K(\underline{T})[X]$. If Q is a monic irred. factor of τR in $K(\underline{T})[X]$ such that $\tau R_\sigma \mid Q$ in $E(\underline{T})[X]$, then for every $\rho \in H$, we have $\tau R_{\rho\sigma} = \tau(\rho(R_\sigma)) = \rho(\tau R_\sigma) \mid \rho Q = Q$ ($\because \rho|_K = \mathrm{id}$). As each $\tau R_{\rho\sigma}$ is a distinct linear poly., their product $\tau R_{H\sigma} = \prod_{\rho\in H} \tau R_{\rho\sigma}$ must divide Q in $E(\underline{T})[X]$, hence also in $K(\underline{T})[X]$. Hence $\tau R_{H\sigma} = Q$.

Now note that the 2nd G-action of G on T_i is simply sent by τ to the G-action on T_i. Hence $\rho \in G$ sends $\tau R_{H\sigma}$ to $\tau R_{H\sigma\rho^{-1}}$, and ρ fixes it if and only if $\rho \in \sigma^{-1}H\sigma$. □

Now we finish the proof of Th. 84. Let $P = X^n - a_1X^{n-1} + \cdots + (-1)^n a_n \in \mathbb{Z}[X]$, with its spl. field $E/\mathbb{Q}$ and $\mathrm{Root}_P(E) = \{\alpha_1, \ldots, \alpha_n\}$, so that $H := \mathrm{Gal}(P) = \mathrm{Gal}(E/\mathbb{Q}) \subset G$. Define $\tau : B \to E$ as in Lem. 85 by $X_i \mapsto \alpha_i$. Then $\tau(s_i) = a_i$, hence $\tau R \in \mathbb{Z}[\underline{T}][X]$. By Gauss' Lemma (Appendix 4), the irred. factorisation of τR, a monic in $\mathbb{Z}[\underline{T}][X]$, is the same as its irred. fact'n in $\mathbb{Q}(\underline{T})[X]$, since $\mathbb{Z}[\underline{T}]$ is a UFD (Appendix 4) and $\mathbb{Q}(\underline{T})$ is its field of fractions.

Similarly for $P \bmod p \in \mathbb{F}_p[X]$, let $\mathbb{F}_q/\mathbb{F}_p$ its spl. field with the roots $\beta_1, \ldots, \beta_n \in \mathbb{F}_q$, so that $H' := \mathrm{Gal}(P \bmod p) = \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p) \subset G$. Define $\tau' : B \to \mathbb{F}_q$ as in Lem. 85 by $X_i \mapsto \beta_i$. Then $\tau(s_i) = \tau(a_i \bmod p)$, hence $\tau' R = \tau R \bmod p \in \mathbb{F}_p[\underline{T}][X]$.

$$\begin{array}{ccccc} & & E & \leftarrow & B & \rightarrow & \mathbb{F}_q & & \\ & H & \cup & & G & \cup & & \cup & H' \\ & & \mathbb{Q} & \leftarrow & A & \rightarrow & \mathbb{F}_p & & \end{array}$$

Its fact'n in $\mathbb{F}_p(\underline{T})[X]$ respects the fact'n of τR in $\mathbb{Z}[\underline{T}][X]$, i.e. each $\tau' R_{H'\sigma'} \in \mathbb{F}_p(\underline{T})[X]$ must divide the $\bmod p$ of some $\tau R_{H\sigma} \in \mathbb{Z}[\underline{T}][X]$. As the 2nd G-action (permuting T_i) is compatible with $\bmod p$, the stabiliser $\sigma'^{-1}H'\sigma'$ of the former is contained in the stabiliser $\sigma^{-1}H\sigma$ of the latter, hence $H' \subset \sigma'\sigma^{-1}H\sigma\sigma'^{-1}$. □

Remark. (oral) By considering the ring of integers $\mathcal{O}_E$ for the number field E (a splitting field of P over $\mathbb{Q}$), the subgroup $\mathrm{Gal}(P \bmod p)$ of $\mathrm{Gal}(P) = \mathrm{Gal}(E/\mathbb{Q})$ is realised as the *decomposition group* of a prime ideal $\mathfrak{p}$ of $\mathcal{O}_E$ dividing p.

Lecture 21 (20 Nov, Tu.)

3. Modern Galois Theory (linear algebraic approach)

Since 20c, Galois theory is not a theory of polynomials. Here we rebuild Galois theory using more linear algebra, without ever mentioning polynomials. Most notably, PET is avoided.

We forget about min. poly's etc., so only assume the following: Def. 1 (Subfields, ext'ns), Def. 2 (Finite/infinite ext'ns, degrees), Def. 12 (K-hom's, $\mathrm{Hom}_K(L, L')$). Linear algebra: Lem. 11 (Field hom's are injective), Lem. 22(i)(ii) (Rank-Nullity).

3.1. **Dedekind's and Artin's lemmas.** We start with a little more linear algebra.

Lemma 86. *Let V be a fin. dim'l K-v.s. and E/K an ext'n. Let $\mathrm{Hom}_{K\text{-vs}}(V, E)$ be the set of all K-linear maps $V \to E$, and define the addition and E-action by*

$$(\rho + \rho')(x) := \rho(x) + \rho'(x), \ \ (a\rho)(x) := a\rho(x) \quad (\forall x \in V, \ \forall \rho \in \mathrm{Hom}_{K\text{-vs}}(V, E)).$$

Then it is an E-v.s. with $\dim_E\big(\mathrm{Hom}_{K\text{-vs}}(V, E)\big) = \dim_K V$.

Proof. It satisfies the axioms of E-v.s. Let $\{e_1, \dots, e_n\}$ be a basis of V. If we define $\rho_i \in \mathrm{Hom}_{K\text{-vs}}(V, E)$ by $\rho_i(a_1e_1 + \cdots + a_ne_n) = a_i$, then every ρ is uniquely written as $\rho = \rho(e_1)\rho_1 + \cdots + \rho(e_n)\rho_n$ ($\because \rho(x) = \rho\big(\sum a_ie_i\big) = \sum a_i\rho(e_i) = \sum \rho_i(x)\rho(e_i) \in E$), hence $\{\rho_1, \dots, \rho_n\}$ is a basis of $\mathrm{Hom}_{K\text{-vs}}(V, E)$ as an E-v.s. □

Proposition 87. (Dedekind's Lemma) *Let F/K be a finite ext'n. Then for any ext'n E/K, the subset $\mathrm{Hom}_K(F, E)$ of the E-v.s. $\mathrm{Hom}_{K\text{-vs}}(F, E)$ is E-linearly independent. In particular $|\mathrm{Hom}_K(F, E)| \le [F : K]$ by Lem. 86.*

Remark. This inequality was proven twice (Th. 20, Prop. 76), and this is our third proof.

Proof. We prove that any finite subset $\{\rho_1, \dots, \rho_k\}$ of $\mathrm{Hom}_K(F, E)$ is E-linearly independent by induction on k. Let $a_1\rho_1 + \cdots + a_k\rho_k = 0 \ \cdots (*)$ be an E-linear relation. If $k = 1$, then $\rho_1 \neq 0$ implies $a_1 = 0$, hence the claim. Let $k \ge 1$. For any $x, y \in F$ we have $a_1\rho_1(x)\rho(y) + \cdots + a_k\rho_k(x)\rho(y) = a_1\rho_1(xy) + \cdots + a_k\rho_k(xy) = 0$, since ρ is a ring hom. As y is arbitrary, as a K-linear map (i.e. in $\mathrm{Hom}_{K\text{-vs}}(F, E)$):

$$a_1\rho_1(x)\rho_1 + \cdots + a_k\rho_k(x)\rho_k = 0.$$

Now multiplying $(*)$ by $\rho_k(x)$ gives $a_1\rho_k(x)\rho_1 + \cdots + a_k\rho_k(x)\rho_k = 0$, so subtracting:

$$a_1\big(\rho_1(x) - \rho_k(x)\big)\rho_1 + \cdots + a_{k-1}\big(\rho_{k-1}(x) - \rho_k(x)\big)\rho_{k-1} = 0.$$

Then all coeff. are 0 by the ind. hyp., and as x is arbitrary, we have $a_i(\rho_i - \rho_k) = 0$ for $1 \le i \le k-1$. If $a_i \neq 0$, then multiplying by a_i^{-1} gives $\rho_i = \rho_k$, contradiction. Hence $a_i = 0$ $(1 \le i \le k-1)$. Case $k = 1$ shows $a_k = 0$. □

This implies $\mathrm{Aut}_K(F) \leq [F:K]$ for finite L/K (Lem. 22(iii)).

Now recall Def. 23 (Galois ext'ns), Lem. 32 (Fixed fields). Prop. 33(i) (F/K : Galois $\Rightarrow F^G = K$) follows. We do Prop. 33(ii) next.

Proposition 88. (Artin's Lemma) *Let F/K be any ext'n. If G is a finite subroup of $\mathrm{Aut}_K(F)$, then F/F^G is Galois and $G = \mathrm{Gal}(F/F^G)$.*

Proof. Let $G = \{\rho_1, \dots, \rho_n\}$ ($\rho_1 = \mathrm{id}$), and write $\boldsymbol{\rho}(x) := \big(\rho_1(x), \dots, \rho_n(x)\big) \in F^n$ for $x \in F$. For $\boldsymbol{x} = (x_1, \dots, x_n) \in F^n$ and $\rho \in G$, write $\rho(\boldsymbol{x}) := \big(\rho(x_1), \dots, \rho(x_n)\big)$. Then $\rho(a\boldsymbol{x}) = \rho(a)\rho(\boldsymbol{x})$ since ρ is a ring hom., and the components of $\rho\big(\boldsymbol{\rho}(x)\big) = \big(\rho\rho_1(x), \dots, \rho\rho_n(x)\big) \in F^n$ are a permutation of those of $\boldsymbol{\rho}(x)$. Hence if $a_1\boldsymbol{\rho}(x_1)+\cdots+a_k\boldsymbol{\rho}(x_k) = 0 \ \cdots(*)$ for $a_1, \dots, a_k \in F$, then $\rho(a_1)\boldsymbol{\rho}(x_1) + \cdots + \rho(a_k)\boldsymbol{\rho}(x_k) = 0 \ \cdots(\star)$ by applying ρ to $(*)$ and permuting back.

Now we prove that if $\{x_1, \dots, x_k\}$ is an F^G-linearly indep. subset of F, then $\{\boldsymbol{\rho}(x_1), \dots, \boldsymbol{\rho}(x_k)\}$ is F-linearly indep. in F^n (which would imply $k \leq n$). Use induction on k. If $k = 1$, then $\boldsymbol{\rho}(x_1) \neq 0$ since $x_1 \neq 0$, so OK. Assume an F-linear relation $(*)$. Replacing all a_i by a_i/a_k when $a_k \neq 0$, we can assume $a_k = 0$ or 1. Then as $\rho(a_k) = a_k$ for all $\rho \in G$, $(*) - (\star)$ gives

$$\big(a_1 - \rho(a_1)\big)\boldsymbol{\rho}(x_1) + \cdots + \big(a_{k-1} - \rho(a_{k-1})\big)\boldsymbol{\rho}(x_{k-1}) = 0.$$

Ind. hyp. shows all coeff. are 0, and since ρ was arbitrary, we have $a_i \in F^G$ $(1 \leq i \leq k-1)$. Now the first component of $(*)$ reads $a_1x_1 + \cdots + a_kx_k = 0$, and the F^G-linear independence of $\{x_1, \dots, x_k\}$ implies all a_i are 0.

Thus F/F^G is finite with $[F:F^G] \leq n = |G|$. Since we had $|G| \leq |\mathrm{Aut}_{F^G}(F)| \leq [F:F^G]$ already, $|\mathrm{Aut}_{F^G}(F)| = [F:F^G]$ and $G = \mathrm{Gal}(F/F^G)$. □

Remark. The proofs of these two lemmas (Prop. 87, 88) had similar structures — starting from a linear relation $(*)$, we produced more linear relations using the fact that ρ is a ring hom.

3.2. **Towers of extensions.** We've almost reproved FTGT (Th. 34) — it remains to prove that if $K \subset L \subset F$ and F/K is Galois, then so is F/L. To deal with the towers, the best way is to generalise the notion of ext'ns.

Definition 89. Let K be a field. We call a pair (F, τ) of a field F and a ring hom. $\tau : K \to F$ an *extension* of K, and denote by F_τ.

A *morphism* $\rho : F_\tau \to F'_{\tau'}$ of ext'ns is a ring hom. $\rho : F \to F'$ such that $\rho\tau = \tau'$. We denote the set of all morphisms from F_τ to $F'_{\tau'}$ by $\mathrm{Hom}(F_\tau, F'_{\tau'})$. If ρ is bijective, then ρ^{-1} is also a morphism, and we call ρ an *isomorphism*. An *automorphism* of F_τ is an isom. from F_τ to itself, and $\mathrm{Aut}(F_\tau)$ is the group of all autom. of F_τ.

Lecture 22 (22 Nov, Th.)

Remark. As K and $\tau(K)$ are isomorphic fields (Lem. 11), $F/\tau(K)$ is an ext'n in our previous sense. If $F_\tau, F'_{\tau'}$ are ext'ns in our old sense, (i.e. τ, τ' are inclusion maps), then $\rho\tau = \tau'$ means $\rho|_K = \mathrm{id}$, i.e. mor's are just K-hom's. Every mor. is injective (Lem. 11), and τ is itself a mor. $\tau : K_{\mathrm{id}} \to F_\tau$. If ρ is an autom. of F_τ then $\rho|_{\tau(K)} = \mathrm{id}$, hence $\mathrm{Aut}(F_\tau) = \mathrm{Aut}_{\tau(K)}(F)$.

Remark. (oral) As this def'n does not require the ext'ns to be supersets of K, it resolves the ambiguity on the identification of K with $\tau(K)$ (with a notational burden). This is the def'n adopted by Bourbaki, and is closer to the categorical framework in alg. geometry (scheme theory).

Let K be a field.

Definition 90. Let F_τ be an ext'n of K. We consider F as a K-v.s. by letting $x \in K$ act on F via multiplication by $\tau(x)$ in F. We say F_τ is *finite* if it is a fin. dim'l K-v.s., and let $[F_\tau] := \dim_K F$ be its *degree*. A finite ext'n F_τ is *Galois* if $|\mathrm{Aut}(F_\tau)| = [F_\tau]$.

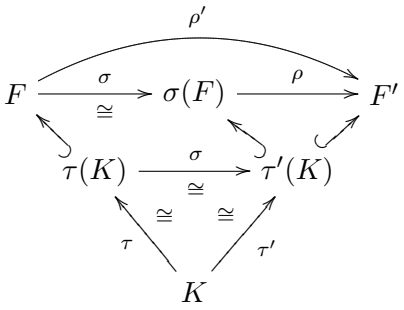
Remark. We have $[F_\tau] = [F : \tau(K)]$. If $[F_\tau] = 1$, then τ is bijective and $F = \tau(K)$. Mor's are injective K-linear maps, so $\mathrm{Aut}(F_\tau) = \mathrm{Hom}(F_\tau, F_\tau)$ for finite F_τ by Rank-Nullity (Lem. 22(ii)).

Lemma 91. *Let $\sigma \in \mathrm{Hom}(F_\tau, F'_{\tau'})$. Then $\sigma(F), F'$ are ext'ns of $\tau'(K)$ in our previous sense, and we have a bijection*

$$\mathrm{Hom}_{\tau'(K)}\big(\sigma(F), F'\big) \ni \rho \overset{\cong}{\longmapsto} \rho' := \rho\sigma \in \mathrm{Hom}(F_\tau, F'_{\tau'}).$$

If F_τ is finite, then $|\mathrm{Hom}(F_\tau, F'_{\tau'})| \le [F_\tau]$ for any $F'_{\tau'}$.

Proof. In the diagram $\hookrightarrow$ indicate inclusion maps. Ring hom's $\rho : \sigma(F) \to F'$ and $\rho' : F \to F'$ correspond bijectively by $\rho' = \rho\sigma,\ \rho = \rho'\sigma^{-1}$. Since $\sigma\tau = \tau'$, we have $\rho|_{\tau'(K)} = \mathrm{id} \iff \rho\tau' = \tau' \iff \rho\sigma\tau = \tau' \iff \rho'\tau = \tau'$. When F_τ is finite, so is the ext'n $\sigma(F)_\sigma$ of $\tau(K)$, hence so is $\sigma(F)/\tau'(K)$. So the 2nd claim follows from the 1st and Prop. 87, by choosing any σ. □



Definition 92. Let L_τ be an ext'n of K, and F_σ an ext'n of L: $K \xrightarrow{\tau} L \xrightarrow{\sigma} F$. Then $\sigma\tau : K \to F$ is an ext'n $F_{\sigma\tau}$ of K. We call this a *tower* L_τ, F_σ of ext'ns.

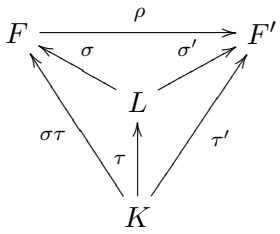
Proposition 93. *Let L_τ, F_σ be a tower.*

(i) *If $F'_{\tau'}$ is an ext'n of K, then the set $\mathrm{Hom}(F_{\sigma\tau}, F'_{\tau'})$ is a disjoint union of $\mathrm{Hom}(F_\sigma, F'_{\sigma'})$ for each $\sigma' \in \mathrm{Hom}(L_\tau, F'_{\tau'})$. In particular $\mathrm{Aut}(F_\sigma)$ is a subgroup of $\mathrm{Aut}(F_{\sigma\tau})$.*

(ii) *$F_{\sigma\tau}$: finite $\iff$ L_τ, F_σ : finite. When it holds, we have $[F_{\sigma\tau}] = [F_\sigma][L_\tau]$.*

(iii) *Suppose L_τ, F_σ are finite. If $F_{\sigma\tau}$ is Galois, then so is F_σ.*

Proof.



(i): If $\rho \in \mathrm{Hom}(F_{\sigma\tau}, F'_{\tau'})$, then $\sigma' = \rho\sigma : L \to F'$ is an ext'n $F'_{\sigma'}$ of L, and $\rho \in \mathrm{Hom}(F_\sigma, F'_{\sigma'})$. Then $\sigma'\tau = \rho\sigma\tau = \tau'$ shows $\sigma' \in \mathrm{Hom}(L_\tau, F'_{\tau'})$. Conversely, if $\sigma' \in \mathrm{Hom}(L_\tau, F'_{\tau'})$ and $\rho \in \mathrm{Hom}(F_\sigma, F'_{\sigma'})$, then $\rho\sigma\tau = \sigma'\tau = \tau'$ shows $\rho \in \mathrm{Hom}(F_{\sigma\tau}, F'_{\tau'})$.

(ii)(same as Prop. 8): ($\Rightarrow$): If $S \subset L$ is K-lin. indep., then so is $\sigma(S) \subset F$, hence $|S| = |\sigma(S)| < \infty$. If $S \subset F$ is L-lin. indep., then it is K-lin. indep., hence $|S| < \infty$.

($\Leftarrow$): If $\{a_i\}$ is a basis of F as L-v.s., and $\{b_j\}$ is a basis of L as K-v.s., then $\{a_i\sigma(b_j)\}$ is a basis of F as K-v.s.

(iii): As $F_{\sigma\tau}$ is Galois, (ii) says $|\mathrm{Aut}(F_{\sigma\tau})| = [F_{\sigma\tau}] = [F_\sigma][L_\tau]$. Applying (i) to $F'_{\tau'} = F_{\sigma\tau}$, together with the remark after Def. 90, gives

$$|\mathrm{Aut}(F_{\sigma\tau})| = |\mathrm{Hom}(F_{\sigma\tau}, F_{\sigma\tau})| = \sum_{\sigma' \in \mathrm{Hom}(L_\tau, F_{\sigma\tau})} |\mathrm{Hom}(F_\sigma, F_{\sigma'})|.$$

But $|\mathrm{Hom}(L_\tau, F_{\sigma\tau})| \le [L_\tau]$ and $|\mathrm{Hom}(F_\sigma, F_{\sigma'})| \le [F_\sigma]$ by Lem. 91, hence both are equalities. In particular, for $\sigma' = \sigma$ we have $|\mathrm{Aut}(F_\sigma)| = [F_\sigma]$. □

This (iii) gives us the FTGT (Th. 34). Cor. 35 is proved as in the proof of Prop. 79, since $|\mathrm{Hom}(L_\tau, F_{\sigma\tau})| = [L_\tau]$ and $\mathrm{Hom}(F_\sigma, F_{\sigma'}) \neq \emptyset$ for each $\sigma' \in \mathrm{Hom}(L_\tau, F_{\sigma\tau})$ (shown above).

3.3. **Traces and norms.** We return to our old notion of ext'ns (L/K means $K \subset L$).

Definition 94. Let L/K be a finite ext'n. For $\alpha \in L$, let $m_\alpha : L \to L$ be the *multiplication by* α map $m_\alpha(\beta) := \alpha\beta$ ($\forall \beta \in L$), viewed as a K-linear transformation of the K-v.s. L. We define the *trace* $T_{L/K}(\alpha)$ and the *norm* $N_{L/K}(\alpha)$ as the trace/determinant of m_α, which are el'ts of K:

$$T_{L/K}(\alpha) := \mathrm{tr}(m_\alpha), \quad N_{L/K}(\alpha) := \det(m_\alpha).$$

If $\{\beta_1, \ldots, \beta_n\}$ is a basis of L as a K-v.s., then

$$m_\alpha(\beta_j) = \alpha\beta_j = \sum_{i=1}^{n} \beta_i a_{ij} \quad (a_{ij} \in K),$$

and m_α is rep'ted by a matrix $A := (a_{ij}) \in M_n(K)$, so $T_{L/K}(\alpha) = \mathrm{tr}(A)$ and $N_{L/K}(\alpha) = \det(A)$. By Linear Algebra:

$$\alpha \neq 0 \iff m_\alpha \text{ : invertible } \iff N_{L/K}(\alpha) = \det(m_\alpha) \neq 0.$$

Example. For a basis $\beta_1 = 1,\ \beta_2 = \sqrt{2}$ of $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, the multiplication by $\alpha = 1 + \sqrt{2}$ gives $m_\alpha(\beta_1) = \beta_1 + \beta_2$ and $m_\alpha(\beta_2) = 2\beta_1 + \beta_2$, so m_α is represented by $A = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$. Hence $T_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(1+\sqrt{2}) = 2$ and $N_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(1+\sqrt{2}) = -1$ (cf. Lemma 96(i), Prop. 98).

Lecture 23 (24 Nov, Sa.)

Lemma 95. *Let L/K be a finite ext'n.*

(i) *$T_{L/K} : L \to K$ is K-linear, and $N_{L/K} : L^\times \to K^\times$ is a (multiplicative) group hom.*
(ii) *If $[L : K] = n$ and $x \in K$, then $T_{L/K}(x) = nx$ and $N_{L/K}(x) = x^n$.*

Proof. (i): $\mathrm{tr}(A+B) = \mathrm{tr}(A)+\mathrm{tr}(B)$, $\mathrm{tr}(xA) = x\,\mathrm{tr}(A)$ $(\forall x \in K)$, $\det(AB) = \det(A)\det(B)$.
(ii): $\mathrm{tr}, \det$ of the scalar matrix xI_n. □

(a) *Traces "can see" the separability.*

Lemma 96. *Let L/K be a finite ext'n.*

(i) *If $L = K(\alpha)$ and $P_\alpha = X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n \in K[X]$ is the min. poly. of $\alpha \in L$, then $T_{L/K}(\alpha) = -a_1$, $N_{L/K}(\alpha) = (-1)^n a_n$.*
(ii) *If $K \subset L \subset F$ with F/K finite, then $T_{F/K} = T_{L/K} \circ T_{F/L}$.*[17]

Proof. (i): For the basis $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ of L/K, the matrix of m_α is $\begin{pmatrix} 0 & & & -a_n \\ 1 & \ddots & & \vdots \\ & \ddots & 0 & -a_2 \\ & & 1 & -a_1 \end{pmatrix}$, since $\alpha^n = -a_1\alpha^{n-1} - \cdots - a_{n-1}\alpha - a_n$.

(ii): Let $\{\beta_1, \dots, \beta_n\}$ be a basis of L/K, and $\{\gamma_1, \dots, \gamma_m\}$ be a basis of F/L. For $\alpha \in F$, let $(\beta_{ij}) \in M_m(L)$ be the matrix for $m_\alpha : F \to F$ (as L-v.s.), and for each β_{ij}, let $A_{ij} \in M_n(K)$ be the matrix for $m_{\beta_{ij}} : L \to L$ (as K-v.s.). Then, with respect to the K-basis $\{\gamma_1\beta_1, \dots, \gamma_1\beta_n, \gamma_2\beta_1, \dots, \gamma_2\beta_n, \dots, \gamma_m\beta_1, \dots, \gamma_m\beta_n\}$ of F, the matrix for $m_\alpha : F \to F$ (as K-v.s.) is $A = \begin{pmatrix} A_{11} & \cdots & A_{1m} \\ \vdots & \dots & \vdots \\ A_{m1} & \cdots & A_{mm} \end{pmatrix} \in M_{mn}(K)$. Thus $T_{F/K}(\alpha) = \mathrm{tr}(A) = \sum_{i=1}^m \mathrm{tr}(A_{ii}) = \sum_{i=1}^m T_{L/K}(\beta_{ii}) = T_{L/K}\big(\sum_{i=1}^m \beta_{ii}\big) = T_{L/K}\big(\mathrm{tr}(\beta_{ij})\big) = T_{L/K}\big(T_{F/L}(\alpha)\big)$. □

Proposition 97. *If F/K is finite and not separable, then $T_{F/K} = 0$ (zero map).*

Proof. Take $\alpha \in F$ such that its min. poly. P_α over K is not sep., hence $P_\alpha(X) = Q(X^p)$ for $Q \in K[X]$, where $\mathrm{char}\, K = p > 0$ (Lem. 73(iii)). Then $K \subset L := K(\alpha^p) \subset L' := K(\alpha) \subset F$ and $L' = L(\alpha)$. As P_α is irred. in $K[X]$, so is Q, hence Q is the min. poly. of α^p over K. So $[L : K] = \deg Q$ and $[L' : K] = \deg P_\alpha = p \deg Q$, hence $[L' : L] = p$ by Tower Law (Prop. 8).

Let $1 \le i \le p-1$. If $\alpha^i \in L$, then $\alpha^p \in L$ implies $\alpha \in L$, which is false. Hence $\alpha^i \notin L$ and $L(\alpha^i) = L'$, so the min. poly. of α^i over L is $X^p - (\alpha^p)^i$, thus $T_{L'/L}(\alpha^i) = 0$ by Lem. 96(i). Also $T_{L'/L}(1) = p \cdot 1 = 0$ (Lem. 95(ii)). As $\{1, \alpha, \dots, \alpha^{p-1}\}$ is a basis for L'/L and $T_{L'/L}$ is L-linear (Lem. 95(i)), we get $T_{L'/L} = 0$. Thus $T_{F/K} = T_{L/K} \circ T_{L'/L} \circ T_{F/L'} = 0$ by Lem. 96(ii). □

[17] In fact the same holds for norms; see Appendix 7.

Proposition 98. *Let F/K be separable with $[F:K]=n$. Take E/K with $\mathrm{Hom}_K(F,E)=\{\tau_1,\dots,\tau_n\}$ (it exists by Th. 77(i)(a)⇔(b); take $\mathbb{C}$ if $F\subset\mathbb{C}$). Then:*

$$T_{F/K}(\alpha)=\sum_{i=1}^{n}\tau_i(\alpha),\quad N_{F/K}(\alpha)=\prod_{i=1}^{n}\tau_i(\alpha)\quad(\forall\alpha\in F).$$

Proof. Let $\{\beta_1,\dots,\beta_n\}$ be a basis for F/K. As $\tau_1,\dots,\tau_n$ are E-lin. indep. in $\mathrm{Hom}_{K\text{-vs}}(F,E)$ by Dedekind (Prop. 87), the row vectors $\big(\tau_i(\beta_j)\big)\in E^n$ $(1\le i\le n)$ must be E-lin. indep., hence the matrix $P:=\big(\tau_i(\beta_j)\big)\in M_n(E)$ is invertible. For $\alpha\in F$, let $A:=(a_{ij})\in M_n(K)$ with $\alpha\beta_j=\sum_{k=1}^{n}\beta_k a_{kj}$. Then $\tau_i(\alpha)\tau_i(\beta_j)=\sum_{k=1}^{n}\tau_i(\beta_k)a_{kj}$ $(1\le i\le n)$. If A' is a diagonal matrix with entries $\tau_1(\alpha),\dots,\tau_n(\alpha)$, then this reads $A'P=PA$, i.e. $A'=PAP^{-1}$ in $M_n(E)$. Hence $T_{F/K}(\alpha)=\mathrm{tr}(A)=\mathrm{tr}(A'),\ N_{F/K}(\alpha)=\det(A)=\det(A')$. □

Theorem 99. *If F/K is a finite ext'n, then F/K : separable $\iff T_{F/K}\neq 0$.*

Proof. (⇐): Prop. 97. (⇒): For E/K as in Prop. 98, the proposition says $T_{F/K}:F\to K\subset E$ is just $\tau_1+\cdots+\tau_n\in\mathrm{Hom}_{K\text{-vs}}(F,E)$, which is $\neq 0$ by Dedekind (Prop. 87). □

Remark. (oral) Th. 99 and Lem. 96(ii) give an alternative proof of Th. 77(ii).

(b) *Norms and cylcic ext'ns.*

Theorem 100. (Hilbert's Theorem 90) *Let F/K be a cyclic ext'n, and σ be a generator of $\mathrm{Gal}(F/K)$. If $N_{F/K}(\alpha)=1$, then there exists $\beta\in F$ with $\alpha=\beta/\sigma(\beta)$.*

Proof. Let $[F:K]=n$. By Dedekind (Prop. 87), the subset $\{\mathrm{id},\sigma,\dots,\sigma^{n-1}\}$ of $\mathrm{Hom}_{K\text{-vs}}(F,F)$ is F-lin. indep., hence $\sum_{i=1}^{n}\big(\alpha\cdot\sigma(\alpha)\cdot\sigma^2(\alpha)\cdots\sigma^{i-1}(\alpha)\big)\sigma^i\neq 0$. So take $\gamma\in F$ such that

$$\sum_{i=1}^{n}\big(\alpha\cdot\sigma(\alpha)\cdot\sigma^2(\alpha)\cdots\sigma^{i-1}(\alpha)\big)\sigma^i(\gamma)=:\beta\neq 0.$$

Applying σ to the above gives $\sigma(\beta)=\sum_{i=1}^{n}\big(\sigma(\alpha)\cdot\sigma^2(\alpha)\cdots\sigma^{i}(\alpha)\big)\sigma^{i+1}(\gamma)$, and since $\alpha\cdot\sigma(\alpha)\cdot\sigma^2(\alpha)\cdots\sigma^{n-1}(\alpha)=N_{F/K}(\alpha)=1$ we see $\beta=\alpha\cdot\sigma(\beta)$. □

Corollary 101. (Kummer theory) *Let $\boldsymbol{\mu}_N\subset K$ with $(\mathrm{char}\,K,N)=1$ (hence K has a primitive N-th root ζ of 1 by Def. 69). If F/K is cyclic of deg. N, then $F=K(\sqrt[N]{a})$ for $a\in K$.*

Proof. As $N_{F/K}(\zeta)=\zeta^N=1$ by Lem. 95(ii), by Hilbert 90 (Th. 100) there is $\beta\in F$ with $\beta/\sigma(\beta)=\zeta$, i.e. $\sigma(\beta)=\zeta\beta$. Then $a:=\beta^N$ will do (see the proof of Th. 47). □

Remark. Lagrange resolvent $x:=\alpha+\beta\zeta+\gamma\zeta^2$ for cubics (see §1.11) is the el't satisfying $x/\sigma(x)=\zeta$ where $\sigma=(\alpha\ \beta\ \gamma)$, so is a special case of above proof. Hilbert 90 generalises Kummer theory; in turn has a generalisation to arbitrary Galois ext'ns (*Galois cohomology*).

Lecture 24 (27 Nov, Tu.)

3.4. **Infinite extensions, etc.**

(a) *What was it all about?* Let K be a field. Galois Theory $/K$ = theory of:

$$\begin{cases} \text{fields that are fin. dim. } K\text{-v.s. (}\textit{fin. ext'ns of } K\text{), and} \\ \text{morphisms, i.e. } K\textit{-hom's } (K\text{-linear ring hom's}) \text{ between them.} \end{cases}$$

Principle of Category Theory : sets of *morphisms* control the *objects*.

... FTGT : Galois groups (autom. groups $\mathrm{Aut}_K(F) = \mathrm{Hom}_K(F,F)$) control the fields.

19c (concrete) algebra		20c (abstract) algebra			
(1) Equations	$\longrightarrow$	Fields (rings)	$[\, P \in K[X]$: irred.	$\longrightarrow$	$K_P := K[X]/(P)\,]$
(2) Solutions (Roots)	$\longrightarrow$	Ring hom's	$[\, E/K$: ext'n $\mathrm{Root}_P(E)$	$\overset{\cong}{\longrightarrow}$	$\mathrm{Hom}_K(K_P, E)\,]$
			α	$\longmapsto$	$(X \bmod P \mapsto \alpha)$

Principle of Algebraic Geometry (over any ring K):

(1) Any *ring* A, finitely generated over K, is a quotient ring of a poly. ring, i.e. $A = K[X_1, \dots, X_n]/I$ with an ideal I. Here $I = (f_1, \dots, f_m)$, and f_i are *"equations"* in $X_1, \dots, X_n$ over K.

(2) A *"solution"* of these equations in a ring E is a *ring hom.* $A \to E$.

E.g. solution $x, y \in \mathbb{Q}$ of $x^n + y^n = 1$ (only $xy = 0$ if $n > 2$: Fermat's Last Th'm) is equivalent to a ring hom. $\mathbb{Q}[X,Y]/(X^n + Y^n - 1) \longrightarrow \mathbb{Q}$ with $X \mapsto x,\ Y \mapsto y$.

(b) *Subfields of algebraic closures, and the absolute Galois group.*

Definition 102. Let E/K be an ext'n, and F, F' be subfields of E containing K. Their *composite field* FF' is the intersection of all subfields of E containing F, F', i.e. minimal such subfield.

If $F = K(\alpha_1, \dots, \alpha_n)$ and $F' = K(\beta_1, \dots, \beta_m)$, then $FF' = K(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m)$. So if $F/K, F'/K$ are finite then so is FF'/K.

Lemma 103. *Let F, F', E be as above with $F/K, F'/K$ finite.*

(i) *If $F/K, F'/K$ are separable (resp. Galois, soluble, abelian), then so is FF'/K.*

(ii) *Let $E = \overline{K}$ be an algebraic closure of K. Let K^{sep} (resp. $K^{\mathrm{sol}},\ K^{\mathrm{ab}},\ K^{\mathrm{cyc}}$) be the union of all finite separable (resp. soluble, abelian, cyclotomic) ext'ns of K inside $\overline{K}$. Then they are fields, hence algebraic ex'ns of K. The field K^{sep}, called a* separable closure *of K, is equal to the union of all finite Galois ext'ns of K inside $\overline{K}$.*

Proof. (i): Th. 77(i)(d)⇒(b), (iii)(c)⇒(a) imply sep./Galois cases. Now $\mathrm{Gal}(FF'/K) \ni \sigma \longmapsto (\sigma|_F, \sigma|_{F'}) \in \mathrm{Gal}(F/K) \times \mathrm{Gal}(F'/K)$ is injective, the soluble/abelian cases follow.

(ii): For each family of subfields, any two members are contained in a larger member by (i), so their union is a field (for cyclotomic, note $K(\boldsymbol{\mu}_N), K(\boldsymbol{\mu}_{N'}) \subset K(\boldsymbol{\mu}_{NN'})$). Any finite sep. ext'n $F = K(\alpha_1, \dots, \alpha_n)$ is contained in the splitting field (inside $\overline{K}$) of the product of min. poly's of α_i over K which is Galois (Prop. 79). □

Definition 104. An algebraic ext'n F/K (not necessarily finite) is called a *Galois ext'n* if it is a union of finite Galois ext'ns. Then $\mathrm{Gal}(F/K) := \mathrm{Aut}_K(F)$ is called its *Galois group*. The group $G_K := \mathrm{Gal}(K^{\mathrm{sep}}/K)$, well-def'd up to isom., is called the *absolute Galois group* of K.

By Lem. 103, for any field K, we have a sequence of Galois ext'ns

$$K \subset K^{\mathrm{cyc}} \subset K^{\mathrm{ab}} \subset K^{\mathrm{sol}} \subset K^{\mathrm{sep}} \subset \overline{K}.$$

Every finite Galois ext'n F/K has a K-isomorphic copy inside K^{sep}. If $F \subset K^{\mathrm{sep}}$, then every el't of $\mathrm{Gal}(F/K)$ can be extended to K^{sep} using Prop. 76(ii), hence $\sigma \mapsto \sigma|_F$ gives a surjection $G_K \to \mathrm{Gal}(F/K)$, so G_K is a huge group which has every Galois group over K as its quotient.

(c) *What next?*
Algebra. Insolvability of Quintics (Abel/Galois) says $K^{\mathrm{sol}} \neq \overline{K}$ in general. Little can be said about G_K for general K. On the contrary, G_K "knows a lot" about each specific field K.

Example. (i) $K = \mathbb{F}_p$. Then $\mathbb{F}_p^{\mathrm{cyc}} = \cdots = \overline{\mathbb{F}_p}$.
(ii) $K = \mathbb{Q}$. We know $\mathbb{Q}^{\mathrm{cyc}} = \mathbb{Q}^{\mathrm{ab}}$ (*the Kronecker-Weber th'm*). For every finite soluble group G, there is a Galois ext'n $F/\mathbb{Q}$ with $\mathrm{Gal}(F/\mathbb{Q}) = G$ (Shafarevich). Is it true for arbitrary finite group? (*Inverse Galois Problem*).
(iii) $K/\mathbb{Q}$ finite (*number fields*). *Class Field Theory* desribes $\mathrm{Gal}(K^{\mathrm{ab}}/K)$, and in some cases we know K^{ab} well (in terms of *modular/elliptic functions*; this is where Abel started).

Geometry. E.g. meromorphic fun. z on the elliptic curve $w^2 = z^3 - z \ldots$ 2-to-1 map (of Riemann Surfaces) to the Riemann sphere ... the quad. ext'n $\mathbb{C}\big(z, \sqrt{z^3 - z}\big)/\mathbb{C}(z)$ (*elliptic function field*).

The analogy: finite ext'ns $\longleftrightarrow$ *covering spaces* in Alg. Topology
$\Longrightarrow G_K$ is the analogue of *fundamental groups*.
E.g. $\mathbb{F}_p$ has a cyclic deg. n ext'n for each n ... looks like:
$S^1 = \{e^{i\theta} \mid \theta \in \mathbb{R}\}$ has an n-fold cyclic covering $\theta \mapsto n\theta$ for each n.

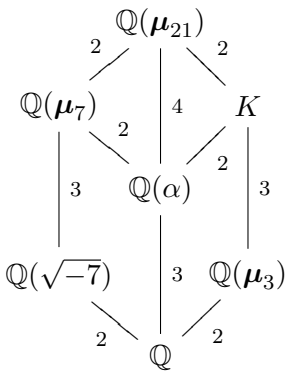
See Appendix 8 for further topics.

APPENDIX 1: ROOTS OF UNITY, RADICAL / SOLUBLE EXTENSIONS (§1.8, §1.11)

Example. Recall $\boldsymbol{\mu}_3 = \Big\{1, \dfrac{-1 \pm \sqrt{-3}}{2}\Big\}$, and $\boldsymbol{\mu}_5 = \Big\{1, \dfrac{-1 \pm \sqrt{5} \pm \sqrt{-10 \mp 2\sqrt{5}}}{4}\Big\}$, where the 1st/3rd signs should match (§1.7). How about $\boldsymbol{\mu}_7$? (Ex. Sheet 3.4, 3.7)

First look at $\mathbb{Q}(\boldsymbol{\mu}_7)$. As $\mathrm{Gal}\big(\mathbb{Q}(\boldsymbol{\mu}_7)/\mathbb{Q}\big) \cong \big(\mathbb{Z}/(7)\big)^\times \cong C_6 \cong C_2 \times C_3$ (Th. 71), there is one quadratic and one cubic subfield, corresponding to $\{1,2,4\},\ \{1,6\} \subset \big(\mathbb{Z}/(7)\big)^\times$. If $\zeta := \zeta_7$, then $\zeta + \zeta^2 + \zeta^4$ is a root of $(X - (\zeta + \zeta^2 + \zeta^4))(X - (\zeta^3 + \zeta^5 + \zeta^6)) = X^2 + X + 2$, i.e. one of $(-1 \pm \sqrt{-7})/2$. Thus $\mathbb{Q}(\zeta + \zeta^2 + \zeta^4) = \mathbb{Q}(\sqrt{-7})$. Also $\alpha := \zeta + \zeta^6$ is a root of $\big(X - (\zeta + \zeta^6)\big)\big(X - (\zeta^2 + \zeta^5)\big)\big(X - (\zeta^3 + \zeta^4)\big) = X^3 + X^2 - 2X - 1$, and the cubic field is $\mathbb{Q}(\alpha)$. Now we look at $\mathbb{Q}(\boldsymbol{\mu}_{21})$, which contains $\mathbb{Q}(\boldsymbol{\mu}_7), \mathbb{Q}(\boldsymbol{\mu}_3)$. Let $\omega := \zeta_3$. As $\mathrm{Gal}\big(\mathbb{Q}(\boldsymbol{\mu}_{21})/\mathbb{Q}\big) \cong \big(\mathbb{Z}/(21)\big)^\times \cong C_2 \times C_2 \times C_3$, it has three subgroups of order 2, which are the intersections of the three index 2 subgroups with an index 3 subgroup. The corresponding sextic fields are generated over the real cubic field $\mathbb{Q}(\alpha)$ by the three quadratic fields $\mathbb{Q}(\sqrt{-7}), \mathbb{Q}(\sqrt{21}), \mathbb{Q}(\boldsymbol{\mu}_3)$, i.e. $\mathbb{Q}(\boldsymbol{\mu}_7)$, a real field $\mathbb{Q}(\sqrt{21}, \alpha)$, and $K = \mathbb{Q}(\omega, \alpha)$. Now $K/\mathbb{Q}(\boldsymbol{\mu}_3)$ is Kummer, gen'd by α.

Procedure in Lecture 1 shows that the cubes of Lagrange resolvents x^3, y^3 for $X^3 - aX^2 + bX - c$ are the roots of $X^2 + (9ab - 2a^3 - 27c)X + (a^2 - 3b)^3$, with $xy = a^2 - 3b$, and $(\alpha, \beta, \gamma) = \big((a + x + y)/3,\ (a + x\omega^2 + y\omega)/3,\ (a + x\omega + y\omega^2)/3\big)$. Then for $X^3 + X^2 - 2X - 1$, the roots of $X^2 + \big(9 \cdot (-1) \cdot (-2) - 2 \cdot (-1)^3 - 27 \cdot 1\big)X + \big((-1)^2 - 3(-2)\big)^3 = X^2 - 7X + 7^3$ are $x^3, y^3 = \big(7 \pm \sqrt{49 - 4 \cdot 7^3}\big)/2 = \big(7 \pm 21\sqrt{-3}\big)/2 = 21\omega + 14,\ 21\omega^2 + 14$, with $xy = 7$. So $\alpha = \big(-1 + \sqrt[3]{21\omega + 14} + \sqrt[3]{21\omega^2 + 14}\big)/3$, and $K = \mathbb{Q}\big(\omega, \sqrt[3]{21\omega + 14}\big)$. Then ζ, ζ^6 are the roots of $X^2 - \alpha X + 1$. We obtain all $\boldsymbol{\mu}_7$ by replacing α with β, γ.



With this example in mind, we will simplify and extend the definitions of radical/soluble ext'ns, which would work for general finite (non-Galois) ext'ns.

Definition. We say a finite ext'n F/K is a *Kummer (*resp. *cyclic) tower* if there is a sequence of subfields $K = K_0 \subset K_1 \subset \cdots \subset K_n = F$ with K_i/K_{i-1} Kummer (resp. cyclic) for all $1 \le i \le n$. We say a finite ext'n L/K inside $\mathbb{C}$ is *radical* (resp. *soluble*) if it is contained in some Kummer (resp. cyclic) tower F/K.

Proposition. *Let $K \subset \mathbb{C}$. Then every cyclotomic ext'n $K(\boldsymbol{\mu}_N)/K$ is radical in this sense, i.e. every root of unity can be written in terms of radicals.*

Proof. Define K_N/K for $N \ge 1$ inductively by $K_0 := K$ and $K_N := K_{N-1}(\boldsymbol{\mu}_N)$. Now write $L := K_{N-1}$; so $K_N = L(\boldsymbol{\mu}_N)$. As $\mathrm{Gal}\big(L(\boldsymbol{\mu}_N)/L\big)$ is isomorphic to a subgroup of $\big(\mathbb{Z}/(N)\big)^\times$ (Prop. 28), it is an abelian group of order at most $\big|\big(\mathbb{Z}/(N)\big)^\times\big| = \varphi(N) < N$ (§2.4), hence soluble (Lem. 38(ii)), i.e. there is a sequence $\mathrm{Gal}\big(L(\boldsymbol{\mu}_N)/L\big) = G_0 \rhd G_1 \rhd \cdots \rhd G_{n-1} \rhd G_n = \{1\}$, where G_{i-1}/G_i is cyclic of order $< N$ for all $1 \le i \le n$. Let $L = L_0 \subset L_1 \subset \cdots \subset L_{n-1} \subset L_n = L(\boldsymbol{\mu}_N)$ be the corresponding sequence of subfields. Then all L_i/L_{i-1} are cyclic (Cor. 35), and as L contains $\boldsymbol{\mu}_j$ for all $1 \le j < N$, they are all Kummer (Th. 47). Thus K_N/K_{N-1} is a Kummer tower; hence so is K_N/K by induction on N. Since $K(\boldsymbol{\mu}_N) \subset K_N$ we win. $\square$

Now we extend the results in §1.8, §1.10 (radical $\Leftrightarrow$ soluble) to the non-Galois extensions. For ext'ns $F/K, F'/K$ inside $\mathbb{C}$, let FF' be the composite field of F, F' inside $\mathbb{C}$ (Def. 102).

Lemma. *Let $F/K, F'/K$ be finite ext'ns inside $\mathbb{C}$ and $K \subset L \subset F$.*

(i) *If F/K is a Kummer (resp. cyclic) tower, then so are FF'/F' and F/L.*
(ii) *F/K : radical (resp. soluble) $\iff$ $F/L, L/K$: both radical (resp. soluble).*
(iii) *A Galois ext'n is radical iff radical in the sense of Def. 39.*
(iv) *A finite ext'n is soluble iff its Galois closure (Def. 36) has a soluble Galois group. In particular, a Galois ext'n is soluble iff soluble in the sense of Def. 37.*

Proof. (i): Let $K = K_0 \subset \cdots \subset K_n = F$ with K_i/K_{i-1} Kummer (resp. cyclic), and $F_i' := K_iF'$, so that $F' = F_0' \subset \cdots \subset F_n' = FF'$. If $F' = K(\alpha)$ by PET (Th. 20) then $F_i' := K_i(\alpha)$, so $\mathrm{Gal}(F_i'/F_{i-1}') \hookrightarrow \mathrm{Gal}(K_i/K_{i-1})$ by Lem. 48. Therefore, since $K_{i-1} \subset F_{i-1}'$ and K_i/K_{i-1} is Kummer (resp. cyclic), so is F_i'/F_{i-1}' by Th. 47 (resp. clearly). Thus FF'/F' is a Kummer (resp. cyclic) tower. If we take $F' = L$, then $FF' = F$.

(ii): If F/K is radical (resp. soluble), then so is L/K. If F'/K is a Kummer (resp. cyclic) tower with $F \subset F'$, then so is F'/L by (i), hence F/L is radical (resp. soluble). Let $F/L, L/K$ be both radical (resp. soluble), and $F'/L, L'/K$ be Kummer (resp. cyclic) towers with $F \subset F'$ and $L \subset L'$. Then $F'L'/L'$ is a Kummer (resp. cyclic) tower by (i), hence so is $F'L'/K$. Thus F/K is radical (resp. soluble).

(iii): The new radical implies old radical. If L/K is old radical, it is contained in a succession F/K of cyclotomic and Kummer ext'ns. Since every cyclotomic ext'n is radical by the previous Proposition, (ii)($\Leftarrow$) shows F/K is radical, hence so is L/K.

(iv): Let L/K be soluble, F/K be a cyclic tower with $L \subset F$, and E/K be the Galois closure of F/K. Let $F = K(\alpha)$ by PET (Th. 20), and $\alpha = \alpha_1, \ldots, \alpha_n$ be the conjugates of α over K, so that $E = K(\alpha_1, \ldots, \alpha_n)$. Letting $K_i := K(\alpha_i)$, we have a K-isom. $\tau_i : F \to K_i$ with $\tau_i(\alpha) = \alpha_i$ (Prop. 14), hence each K_i/K is a cyclic tower (by sending the sequence of cyclic ext'ns by τ_i). So, if we define the fields $F = F_1 \subset F_2 \subset \cdots \subset F_n = E$ inductively by $F_i := K_iF_{i-1}$, then (i) shows that F_i/F_{i-1} for every i, hence E/K, is a cyclic tower. Thus $\mathrm{Gal}(E/K)$ is soluble. As the Galois closure E_L/K of L/K is contained in E, the group $\mathrm{Gal}(E_L/K)$ is a quotient of $\mathrm{Gal}(E/K)$ by Cor. 35(ii), hence soluble by Lem. 38(i)($\Rightarrow$). Conversely, if $\mathrm{Gal}(E_L/K)$ is soluble then E_L/K is a cyclic tower, so L/K is soluble. □

Theorem. *A finite ext'n inside $\mathbb{C}$ is radical if and only if it is soluble.*

Proof. Radical ext'ns are soluble. Let L/K be soluble. Then its Galois closure has a soluble Galois group by Lemma (iv), hence is radical in the old sense by Th. 49, hence also in the new sense by Lemma (iii). Therefore L/K is radical. □

Remark. (i) Lemma (i) implies: if $F/K, F'/K$ are both Kummer towers (resp. cyclic towers / radical / soluble) then so is FF'/K.
(ii) Lemma (ii)($\Leftarrow$),(iv) imply: if L/K is soluble, then $K^{\mathrm{sol}} = L^{\mathrm{sol}}$ (see Lem. 103) inside $\mathbb{C}$.
(iii) Everything works for K with $\mathrm{char}\, K = 0$ (by working inside a sufficiently large splitting field or $\overline{K}$ instead of $\mathbb{C}$), since Def. 30 (Kummer ext'ns), Prop. 31 (their Galois groups), Th. 47 (Kummer theory) are valid, in view of Def. 69, Cor. 101.

APPENDIX 2: WHY GENERAL FIELDS, AND HOW? (§2.1)

Most of the essential features of Galois Theory were covered in §1.

Motivations.

(A) *Eliminate analysis*. We used the "fundamental theorem of algebra", hence relied on real analysis. But the whole business seems to have little to do with $\mathbb{R}, \mathbb{C}$ (Birth of abstract algebra — early 20c).

(B) *Number theory*. There are *finite* fields, e.g. $\mathbb{F}_p := \mathbb{Z}/(p)$ for primes p. Any Galois Theory for these? (Yes; moreover, they have applications to Galois groups over $\mathbb{Q}$, as we will see. Also used in coding theory, etc.)

(C) *Algebraic geometry*. Discussions of "general equations" suggest that we'd like to do Galois Theory for $K(X_1, \ldots, X_n)$ (*function fields*); when $K = \mathbb{Q}$ they were isomorphic to subfields of $\mathbb{C}$, but will no longer be so for $K = \mathbb{C}$. Fields like $\mathbb{C}(X)$ occur as fields of *meromorphic functions on compact Riemann surfaces*, and Galois Theory translates itself into geometry (and $\mathbb{C}(X_1, \ldots, X_n)$ for n-dimensional manifolds [varieties]); for $K = \mathbb{F}_p$, it points to algebraic geometry over $\mathbb{F}_p$.

Problems.

Let K be an arbitrary field. All of §1 will work for extensions of K, if we have a sufficiently large field $\overline{K}/K$ (an *algebraic closure* of K, analogue of the field of all algebraic numbers $\overline{\mathbb{Q}} \subset \mathbb{C}$ for $K = \mathbb{Q}$), which plays the role of $\mathbb{C}$. But:

(A) *Set theoretic difficulty*. When K is uncountable, the construction of $\overline{K}$ requires the *axiom of choice* (in fact for any K if we want to prove its uniqueness). But Galois Theory deals mainly with *finite* extensions, so this must be unnecessary.

(B) *Generality*. We want to treat fields like

$$K_P := K[X]/(P), \quad \text{for } P \in K[X] : \text{irreducible},$$

as extensions of K, i.e. we don't want to restrict ourselves to subfields of (a particular) $\overline{K}$.

(C) *Separability*. In characteristic $p > 0$, irreducible polynomials can have multiple roots (i.e. Prop. 15(i) is false)! This happens when taking p-th power roots, e.g. $K = \mathbb{F}_p(T)$ where T is an indeterminate and $P(X) := X^p - T = \left(X - \sqrt[p]{T}\right)^p$, irreducible in $K[X]$.

Review of §1. Boldface items were for subfields of $\mathbb{C}$.

Def. 1: Subfields, extensions. Def. 2: Finite/infinite extensions, degrees.

Def. 3: Algebraic/transcendental (elements/extensions).

Prop. 4: Finite ext'ns are algebraic. Def. 5: Minimal polynomials.

Def. 6: Simple ext'ns. Prop. 7: Min. poly. are irreducible, degree of simple ext'ns.

Prop. 8: Tower Law. Def. 9: Ext'ns generated by finitely many generators.

Prop. 10: Finite $\iff$ generated by finitely many algebraic generators.

Lem. 11: Field hom's are injective.

Def. 12: K-hom's, $\mathrm{Hom}_K(L, L')$. Def. 13: $\mathrm{Root}_P(L)$, conjugates.

Prop. 14: Roots and Hom's I (simple ext'ns).

Prop. 15: Separability of irred. poly., $|\mathrm{Hom}_K(K(\alpha), \mathbb{C})| = [K(\alpha) : K]$. Def. 16: τP.

Prop. 17: Roots and Hom's II (extending K-hom's to simple ext'ns).

Th. 18: Separability $|\mathrm{Hom}_K(F, \mathbb{C})| = [F : K]$. **Lem. 19**: $\mathrm{Hom}_K(F, \mathbb{C}) \twoheadrightarrow \mathrm{Hom}_K(L, \mathbb{C})$.

Th. 20: Primitive Element Theorem. Def. 21: K-isomorphisms, K-automorphisms.

Lem. 22: If L/K finite, $\mathrm{Hom}_K(L, L) = \mathrm{Aut}_K(L)$ and $|\mathrm{Aut}_K(L)| \leq [L : K]$.

Def. 23: Galois ext'ns, Galois groups.

Prop. 24: Characterisation of Galois ext'ns (has all conjugates).

Def. 25: Splitting fields. **Cor. 26**: Splitting fields are Galois.

Def. 27: $\boldsymbol{\mu}_N$, primitive roots of unity, cyclotomic ext'ns.

Prop. 28: $\mathrm{Gal}\big(K(\boldsymbol{\mu}_N)/K\big) \hookrightarrow \big(\mathbb{Z}/(N)\big)^\times$. **Cor. 29**: Cyclotomic ext'ns are abelian.

Def. 30: Kummer ext'ns. **Prop. 31**: $\mathrm{Gal}\big(K(\sqrt[N]{a})/K\big) \hookrightarrow \mathbb{Z}/N\mathbb{Z}$.

Lem. 32: Subfields $\leftrightarrow$ subgroups, fixed fields.

Prop. 33: F/K : Galois $\iff$ $F^{\mathrm{Aut}_K(F)} = K$ for simple F/K (or any finite F/K - Prop. 88).

Th. 34: Fundamental Theorem of Galois Theory.

Cor. 35: Galois subextensions $\leftrightarrow$ normal subgroups. **Def. 36**: Galois closures.

Def. 37: Soluble groups & ext'ns. Lem. 38: Solubility & sub/quotients, abelian groups.

Def. 39: Radical ext'ns. **Th. 40**: Radical ext'ns are soluble.

Def. 41: Galois groups of polynomials.

Prop. 42: $\mathrm{Gal}(P)$ for irreducible P is a transitive subgroup of S_n.

Def. 43: Fields of rational functions. **Prop. 44**: Galois ext'ns with Galois group S_n.

Th. 45: Insolvability of Quintics. Def. 46: Cyclic ext'ns. **Th. 47**: Kummer Theory.

Lem 48: Galois groups of $K(\alpha)/K$ and $L(\alpha)/L$.

Th. 49: Soluble ext'ns inside $\mathbb{C}$ are radical.

Def. 50: $\mathrm{Gal}(P) \cap H$ for $H \lhd S_n$. discriminants.

Prop. 51: $\mathrm{Gal}(P) \subset A_n \iff$ discriminant is a square.

APPENDIX 3: ZORN'S LEMMA AND ALGEBRAIC CLOSURES (§2.2)

In order to prove the existence of the algebraic closure of an arbitrary field, it is necessary to use an axiom of set theory known as *Zorn's lemma*. It is equivalent to the Axiom of Choice (see e.g. Halmos's *Naive Set Theory*), which roughly says that we are allowed to make infinitely many choices at once. Some believe that one should avoid the Axiom of Choice wherever possible, as it is less intuitive than the other axioms of set theory. However a lot of algebra (not to say analysis) would be very awkward without it. If one is really concerned about its validity, it is worth pointing out that one can often avoid using Zorn's Lemma, at the expense of some notational complexity (for example, instead of the algebraic closure of a field one can often make do with the splitting field of a sufficiently large finite set of polynomials).

Definition. Let S be a set. A relation $\leqslant$ on S is said to be a *partial order* if it satisfies:

(i) For all $x \in S$, $x \leqslant x$;
(ii) For all $x, y, z \in S$, if $x \leqslant y$ and $y \leqslant z$ then $x \leqslant z$;
(iii) For all $x, y \in S$, if $x \leqslant y$ and $y \leqslant x$ then $x = y$.

S is said to be *totally ordered* by $\leqslant$ if moreover:

(iv) For all $x, y \in S$, either $x \leqslant y$ or $y \leqslant x$.

A *chain* is a partially ordered set $(S, \leqslant)$ is a subset $T \subset S$ which is totally ordered by $\leqslant$. If $T \subset S$ is a chain then so is any subset of T.

Example. (i) $\mathbb{N}$ and $\mathbb{R}$ are totally ordered sets (with the usual order relation).
(ii) Let $S = \{x \in \mathbb{Z} \mid x > 1\}$ ordered by reverse divisibility:

$$x \preccurlyeq y \quad \Longleftrightarrow \quad x/y \in \mathbb{Z}.$$

Then $(S, \preccurlyeq)$ is a partially ordered set. Let $m > 1$ and $T = \{m^i \mid i > 1\}$. Then T is a chain in S. So is the subset $\{n! \mid n > 1\}$.
(iii) Let X be any set, S the set of all subsets of X with inclusion as the order relation. Then S is a partially ordered set.

Definition. Let $(S, \leqslant)$ be a partially ordered set, and T any subset of S. An *upper bound* for T is an element $z \in S$ such that $x \leqslant z$ for all $x \in T$. (We don't require that $z \in T$.) An element $y \in S$ is said to be *maximal* if for any $x \in S$, $y \leqslant x$ iff $x = y$.

If S is totally ordered, then it can have at most one maximal element (easy). A general partially ordered set can have many maximal elements. In the above examples:

Example. (i) In $\mathbb{R}$ an upper bound for a subset is an upper bound in the usual sense. There are no maximal elements.
(ii) In $S = \{x \in \mathbb{Z} \mid x > 1\}$ an element $x \in S$ is maximal iff it is prime. Every chain has an upper upper bound (take the element which is smallest for the usual ordering on $\mathbb{N}$).

Zorn's Lemma. *Let S be a nonempty partially ordered set. Assume that every chain in S has an upper bound. Then S has a maximal element.*

Zorn's lemma is equivalent to two other axioms of Set Theory:

The Axiom of Choice. *Let X_i $(i \in I)$ be a collection of sets, indexed by a set I. If each X_i is nonempty then so is the Cartesian product* $\prod_{i \in I} X_i$.

The Well-Ordering Theorem. *Every set can be well-ordered, i.e. we can define a total order on it so that every non-empty subset contains a minimal element.*

For example, using Zorn's lemma one can prove that *every vector space has a basis*, by looking at the set of all linearly independent subsets, ordered by inclusion.

Theorem. (i) *For any ring R and an ideal $I \neq R$, there exists a maximal ideal which contains R. In particular (taking $I = 0$), any non-zero ring has a maximal ideal.*
(ii) *(Th. 58) For any field K, its algebraic closure $\overline{K}$ exists and is unique up to K-isomorphism. Any algebraic extension of K is K-isomorphic to a subextension of $\overline{K}/K$.*

Proof. (i): Let S be the set of all proper ideals (i.e. $\neq R$) containing I, ordered by inclusion. It is nonempty since $I \in S$. Let $T \subset S$ be a chain. Define $J := \bigcup_{I \in T} I$. We claim J is an upper bound for T. What is not obvious is that $J \in S$. As J is a union of ideals containing I, it is clearly an ideal containing I. Moreover it is a proper ideal, for if not then $1 \in J$ which is true iff $1 \in I$ for some $I \in T$, which is impossible as I is a proper ideal. Therefore $J \in S$ and so J is an upper bound for T. By Zorn's Lemma, S has a maximal element.

(ii): Consider the set Λ of all pairs $\lambda = (P, i)$ where $P \in K[X]$ is an irreducible monic and $1 \leq i \leq \deg P$. Consider a variable $X_\lambda = X_{P,i}$ for each $\lambda \in \Lambda$, and the polynomial ring $A := K[X_\lambda \mid \lambda \in \Lambda]$ in all these variables (but note that each of its elements (polynomials) involves only finitely many variables). For each irred. monic $P \in K[X]$, consider the polynomial $P'(X) := P(X) - \prod_{i=1}^{\deg P} (X - X_{P,i}) \in A[X]$, and let $x_{P,i} \in A$ be the coeff. of X^i in $P'(X)$ for $0 \leq i < \deg P$. Let I be the ideal of A generated by all $x_{P,i} \in A$ for all P.

We first show $I \neq A$. Assume $I = A$, i.e. $1 \in I$. Then:

$$\exists a_1, \ldots, a_n \in A, \ \sum_{j=1}^{n} a_j x_{P_j, i_j} = 1 \in A.$$

Let F be a splitting field of $P_1 \cdots P_n$ (Prop. 56). Then each P_j splits as $P_j(X) = \prod_{i=1}^{\deg P_j} (X - \alpha_{ji})$ in $F[X]$, with $\alpha_{ji} \in F$. Consider the "substitution" map $f : A \to F$ defined by $f(X_{P_j,i}) = \alpha_{ji}$ for $1 \leq j \leq n$ and $1 \leq i \leq \deg P_j$, and $f(X_\lambda) = 0$ for all the other X_λ. Then under this ring hom. f, the poly. $P_j'(X) \in A[X]$ is sent to $P_j(X) - \prod_i (X - \alpha_{ji}) = 0 \in F[X]$, thus we see that $f(x_{P_j,i}) = 0 \in F$ for all $1 \leq i \leq \deg P_j$. Therefore $1 = f(1) = f\big(\sum_j a_j x_{P_j,i_j}\big) = 0$ in F, a contradiction.

Hence take a maximal ideal Q of A containing I by (i), and consider the field $\overline{K} := A/Q$, which is an extension field of K. Let $\alpha_\lambda := X_\lambda \bmod Q \in \overline{K}$. Then every irred. monic $P \in K[X]$ splits as $P(X) = \prod_i (X - \alpha_{P,i})$ in $\overline{K}[X]$. In particular α_λ is alg. $/K$, and $\overline{K}/K$ is algebraic, as every el't of $\overline{K}$ is a poly. in α_λ. If $L/\overline{K}$ is alg., for every $x \in L$ its min. poly. lies in $K(\alpha_{\lambda_1}, \ldots, \alpha_{\lambda_m})$ for some $\lambda_1, \ldots, \lambda_m$, thus x is alg. over K. As the min. poly. of x over K splits in $\overline{K}$, we have $x \in \overline{K}$. Hence $L = \overline{K}$. Therefore $\overline{K}$ is alg. closed.

Now let F/K be alg., and let S be the set of all pairs (L, τ) where L is a subext'n of F/K and $\tau \in \mathrm{Hom}_K(L, \overline{K})$. It is an ordered set if we define $(L_1, \tau_1) \leq (L_2, \tau_2) \iff L_1 \subset L_2,\ \tau_2|_{L_1} = \tau_1$. For any totally ordered subset T of S, the el't (L_T, τ_T), defined by $L_T := \bigcup_{(L,\tau) \in T} L$ and $\tau_T|_L = \tau$ for $(L, \tau) \in T$, is an upper bound of T. Thus we can take a maximal el't (M, ρ) of S by Zorn's Lemma. For all $x \in F$, we have $\mathrm{Hom}_M(M(x), \overline{K}) \neq \emptyset$ by Prop. 14, as $\overline{K}$ is alg. closed and the min. poly. of x over M splits in $\overline{K}$, therefore the maximality of (M, ρ) implies $M(x) = M$. Thus $M = F$, and F is K-isomorphic to $\rho(F) \subset \overline{K}$ by ρ. If F is an alg. closure of K, then so is $\rho(F)$, and as $\overline{K}$ is alg. over $\rho(F)$ we have $\rho(F) = \overline{K}$, i.e. ρ is a K-isomorphism. $\square$

APPENDIX 4: GAUSS' LEMMA (FROM GROUPS, RINGS & MODULES; §2.4, §2.7)

Let A be an integral domain, and $a, b, p, \ldots \in A$. We write $(a) := \{ad \mid d \in A\} \subset A$.

Definition. We say a is a *divisor* of b, or $a \mid b$, if $b \in (a)$. A *unit* is a divisor of 1, and $A^\times$ denotes the multiplicative group of all units in A. Note $A[X]^\times = A^\times$. We say a, b are *associates* if $a \mid b$ and $b \mid a$, i.e. $b = ad$ with $d \in A^\times$. An element p, not 0 nor a unit, is called *irreducible* if all its divisors are its associates and units; *prime* if $p \mid ab$ implies $p \mid a$ or $p \mid b$ for any a, b. We say A is a *unique factorisation domain (UFD)* if every el't of A, except 0 and units, is a product of primes.

Fact. If a is a unit/irreducible/prime, then so is its associate. Every prime is irreducible. A factorisation of an element into a product of primes, if exists, is unique up to associates.

Definition. Let A be a UFD and $a_1, \ldots, a_n \in A$, not all zero. For a prime p, let p^m be its maximal power dividing all of $a_1, \ldots, a_n$. Then $p^m \neq 1$ for only finitely many p up to associates, and their product, defined up to associates, is called the *greatest common divisor (GCD)* of $a_1, \ldots, a_n$. Every el't in the field of fractions K of A is written as a/b where the GCD of a, b is 1, and b is called its *denominator*. For $P \in A[X] \setminus \{0\}$, its *content* $c(P) \in A$ is the GCD of its coefficients.

Lemma. *Let A be a UFD. If $P, Q \in A[X] \setminus \{0\}$, then $c(PQ) = c(P)c(Q)$ (up to associates).*

Proof. Note $c(P) \mid P$ and $P = c(P) \cdot P'$ with $c(P') = 1$. So STP if $c(P) = c(Q) = 1$ then $c(PQ) = 1$. Let $P = \sum a_i X^i,\ Q = \sum b_j X^j$, and $PQ = \sum d_k X^k$. For a prime $p \in A$, let i, j be minimal such that $a_i, b_j \notin (p)$. Then every term in $d_{i+j} = \sum a_k b_{i+j-k}$ is in (p) except for $a_i b_j$, which is not divisible by p, hence $d_{i+j} \notin (p)$. Hence $c(PQ) = 1$. □

Gauss' Lemma. *Let A be a UFD and K be its field of fractions. Consider $A \subset A[X] \subset K[X]$.*

(i) *A prime p of A is a prime of $A[X]$. If $P \in A[X]$ is a prime of $K[X]$ and $c(P) = 1$, then it is a prime of $A[X]$.*

(ii) *The poly. ring $A[X]$ is also a UFD (hence so is $A[X_1, \ldots, X_n]$), all whose primes are as seen in* (i)*. For every monic in $A[X]$, its prime factorisation in $K[X]$ into monics gives its prime factorisation in $A[X]$.*

Proof. (i): If p is a prime of A and $p \mid PQ$ for $P, Q \in A[X]$, then $p \mid c(PQ) = c(P)c(Q)$ by the Lemma. So wlog p divides $c(P)$, hence divides P. Suppose $P \in A[X]$ is a prime of $K[X]$ and $c(P) = 1$. If $P \mid QR$ for $Q, R \in A[X]$, then wlog $Q = PS$ in $K[X]$. Clearing the denominators of S (i.e. multiply the GCD of the denom's of all its coeff's) to get $S' \in A[X]$ with $c(S') = 1$, we have $aQ = PS'$ with $a \in A$. Then $a \cdot c(Q) = 1$ by Lemma, so $c(Q) \in A^\times$, thus $P \mid Q$ in $A[X]$.

(ii): STP: every $P \in A[X]$, not a unit or 0, is a product of primes of the form seen in (i). Firstly $P = c(P) \cdot P'$ with $c(P') = 1$, and $c(P)$ is a product of primes of A, seen in (i). So assume $c(P) = 1$. Let d be the leading coeff. of P, and $P = dP_1 \cdots P_n$ be the prime fact'n in $K[X]$ into monics. Clearing the denom's of P_i to get $P_i' \in A[X]$ with $c(P_i') = 1$, we have $aP = bP_1' \cdots P_n'$ with $a, b \in A \setminus \{0\}$. These P_i' are primes of $K[X]$ of the form seen in (i). Now the Lemma (taking c) shows a, b are associates in A, hence $P = P_1' \cdots P_n'$ by replacing P_1' with its associate in $A[X]$. When $d = 1$, the leading coeff. d_i of P_i' is in $A^\times$ since $d_i \mid d$, hence $P_i = d_i^{-1} P_i' \in A[X]$. □

APPENDIX 5: ALGEBRAIC INDEPENDENCE OF ELEMENTARY SYMMETRIC POLYNOMIALS (§2.6)

The following theorem complements the Symmetric Function Theorem (Th. 83). Recall that if R is a subring of A and $x_1, \dots, x_n \in A$, then there exists a unique ring hom. from the poly. ring $f : B := R[X_1, \dots, X_n] \to A$ satisfying $f|_R = \mathrm{id}$ and $f(X_i) = x_i$ $(1 \le i \le n)$.

Theorem. *Let R be an integral domain, $B := R[X_1, \dots, X_n]$ be the poly. ring in n variables over R, and $A := R[s_1, \dots, s_n]$ be a subring of B consisting of the el'ts written as poly's in the elementary symmetric poly's $s_1, \dots, s_n$ (Def. 81) with coeff's in R.*

Then the following surjective ring hom. from B is injective, hence an isom.:

$$f : B \longrightarrow A, \quad f|_R = \mathrm{id}, \quad f(X_i) = s_i \ \ (1 \le i \le n).$$

Remark. SFT (Th. 83) says that A is the ring of all symmetric polynomials inside B, i.e. every symm. poly's are written as poly's in s_i; this theorem says they are *uniquely* written as such.

Proof. Use induction on n. There is nothing to prove when $n = 0$. Let $s'_1, \dots, s'_{n-1}$ be the elementary symm. poly's in $X_1, \dots, X_{n-1}$, and define $s'_n = 0$. Let

$$A' := R[X_n][s'_1, \dots, s'_{n-1}] \subset R[X_n][X_1, \dots, X_{n-1}] = B$$

be a subring of B consisting of the el'ts written as poly's in $s'_1, \dots, s'_{n-1}$ with coeff's in $R[X_n]$. By the ind. hyp. (for $R[X_n]$ instead of R) we have a ring isom.:

$$f' : B = R[X_n][X_1, \dots, X_{n-1}] \xrightarrow{\cong} A', \quad f'|_{R[X_n]} = \mathrm{id}, \quad f'(X_i) = s'_i \ \ (1 \le i \le n-1).$$

The def'ns (Def. 81) imply $s_i = s'_i + s'_{i-1}X_n$ $(1 \le i \le n)$, hence $s_1, \dots, s_n \in A'$. Repeatedly using $s'_j = s_j - s'_{j-1}X_n$ for $1 \le j \le i$, we get $s'_i = s_i - s_{i-1}X_n + s_{i-2}X_n^2 - \cdots + (-1)^i X_n^i$. In particular every el't of A' is a poly. in s_i with coeff. in $R[X_n]$.

Now consider the following ring hom's, both restricting to id on $R[X_n]$:

$$\varphi, \psi : B \longrightarrow A', \quad \varphi(X_i) = s_i, \quad \psi(X_i) = s'_i - s'_{i-1}X_n + \cdots + (-1)^i X_n^i \quad (1 \le i \le n-1).$$

By the above remark φ is surjective. Then $\varphi \circ f'^{-1} : A' \to A'$ sends s'_i to s_i, and $\psi \circ f'^{-1} : A' \to A'$ sends $s_i = s'_i + s'_{i-1}X_n$ to $(s'_i - \cdots + (-1)^i X_n^i) + (s'_{i-1} - \cdots + (-1)^{i-1}X_n^{i-1})X_n = s'_i$. Thus $(\psi \circ f'^{-1}) \circ (\varphi \circ f'^{-1}) = \mathrm{id}$. So $\varphi \circ f'^{-1}$ is injective, hence so is φ. Thus φ is an isom.

Now φ restricts to an isom. from $R[X_1, \dots, X_{n-1}]$ to the subring $C := R[s_1, \dots, s_{n-1}] \subset A'$, which extends to an isom. $\widetilde{\varphi} : B = R[X_1, \dots, X_{n-1}][X_n] \xrightarrow{\cong} C[T]$ with $\widetilde{\varphi}(X_n) = T$. Then $g := \varphi \circ \widetilde{\varphi}^{-1} : C[T] \xrightarrow{\cong} A'$ satisfies $g|_C = \mathrm{id}$ and $g(T) = X_n$.

Consider $h : C[T] \to A'$ defined by $h|_C = \mathrm{id}$ and $h(T) = s_n$. Then $f = h \circ \widetilde{\varphi}$, so STP h is injective. Since X_n is a root of $(X - X_1) \cdots (X - X_n) = X^n - s_1X^{n-1} + s_2X^{n-2} - \cdots + (-1)^n s_n$, we have $(-1)^{n+1}s_n = X_n^n - s_1X_n^{n-1} + \cdots + (-1)^{n-1}s_{n-1}X_n$. So let $\chi : C[T] \to C[T]$ be a ring hom. with $\chi|_C = \mathrm{id}$ and $\chi(T) = (-1)^{n+1}(T^n - s_1T^{n-1} + \cdots + (-1)^{n-1}s_{n-1}T)$. Then $h = g \circ \chi$, so STP χ is injective, but if $P \in C[T] \setminus \{0\}$ then $\chi(P) = P\big(\chi(T)\big) \neq 0$ since its leading coeff. is $\neq 0$. □

Remark. Thus A is a UFD by Gauss' Lemma when $R = \mathbb{Z}$ or $\mathbb{F}_p$. As $X_1, \dots, X_n$ are integral over A and UFD's are integrally closed, we can recover SFT (Th. 83) from Rat'l SFT (Th. 82).

APPENDIX 6: NORMAL BASIS THEOREM (§3.1)

Normal Basis Theorem. *Let F/K be a (finite) Galois ext'n and $G := \mathrm{Gal}(F/K)$. Then there exists $x \in F$ such that $\{\rho(x) \mid \rho \in G\}$ is K-linearly independent (hence a basis of F/K). A basis of this form is called a* normal basis *of F/K.*

Proof. Assume $|K| = \infty$. Let $G = \{\rho_1, \dots, \rho_n\}$ with $\rho_1 = \mathrm{id}$. If $a_1\rho_1(x) + \cdots + a_n\rho_n(x) = 0$ with $a_i \in K$, then applying $\rho \in G$ gives $a_1\rho\rho_1(x) + \cdots + a_n\rho\rho_n(x) = 0$ since $\rho(a_i) = a_i$. Hence the vectors $\big(\rho_j^{-1}\rho_1(x), \dots, \rho_j^{-1}\rho_n(x)\big) \in F^n$ for $1 \le j \le n$ are K-linearly dependent, therefore $\det\big(\rho_j^{-1}\rho_i(x)\big) \in F$ is zero. So STP: $\exists x \in F$ such that $\det\big(\rho_j^{-1}\rho_i(x)\big) \neq 0$.

First note that if $\rho \in G,\ P \in F[X]$ and $\alpha \in F$ then $\rho\big(P(\alpha)\big) = (\rho P)\big(\rho(\alpha)\big)$. By PET (Th. 20) take $\alpha \in F$ with $F = K(\alpha)$, and define

$$P(X) := \prod_{i \neq j} \frac{X - \rho_i^{-1}\rho_j(\alpha)}{\alpha - \rho_i^{-1}\rho_j(\alpha)} \in F[X].$$

Then $P\big(\rho_i^{-1}\rho_j(\alpha)\big) = \delta_{ij}$, so $(\rho_j^{-1}\rho_i P)(\alpha) = \rho_j^{-1}\rho_i P\big(\rho_i^{-1}\rho_j(\alpha)\big) = \delta_{ij}$. Now define

$$Q(X) := \det\big((\rho_j^{-1}\rho_i P)(X)\big) \in F[X].$$

Then $Q(\alpha) = \det(\delta_{ij}) = 1$, in particular $Q \neq 0$. As K is infinite, we can take $z \in K$ which is not a root of Q. Then for $x := P(z)$ we have $\rho_j^{-1}\rho_i(x) = \rho_j^{-1}\rho_i\big(P(z)\big) = \big(\rho_j^{-1}\rho_i P\big)(z)$, hence $\det\big(\rho_j^{-1}\rho_i(x)\big) = Q(z) \neq 0$, qed.

Now let $K = \mathbb{F}_q$ be finite and $[F : K] = n$. Then G is a cyclic group generated by Fr_q (Th. 68). Considering Fr_q as a linear transformation of the K-v.s. F, its minimal polynomial is $X^n - 1$, since $\{\mathrm{id}, \mathrm{Fr}_q, \mathrm{Fr}_q^2, \dots, \mathrm{Fr}_q^{n-1}\}$ is K-linearly independent by Dedekind (Prop. 87). Thus viewing F as a $K[X]$-module where X acts by Fr_q, it has a direct summand M isomorphic to $K[X]/(X^n - 1)$ by the structure th'm of fin. gen. modules over PID. But $\dim_K M = n = \dim_K F$, hence $M = F$ and $K[X]/(X^n - 1) \cong K$ as $K[X]$-modules. If x is the image of 1 under this isom. then the basis $\{X^i \mid 0 \le i < n\}$ over K is mapped to $\{\mathrm{Fr}_q^i(x) \mid 0 \le i < n\}$. □

Remark. (i) This gives another proof of the second half of FTGT (Th. 34) as follows. Let $F/K, G$ be as above. Taking a normal basis $\{\rho(x) \mid \rho \in G\}$, every $y \in F$ is written uniquely as $y = \sum_\rho a_\rho \rho(x)$ with $a_\rho \in K$. Let H be a subgroup of G. Then $y \in F^H$ iff $a_{\sigma\rho} = a_\rho$ for all $\sigma \in H$ and $\rho \in G$. Thus $[F^H : K] = |G|/|H|$, hence $[F : F^H] = |H|$ by Tower Law (Prop. 8). As $|H| \le |\mathrm{Aut}_{F^H}(F)| \le [F : F^H]$ by Lem. 22(iii) we have equalities, hence $H = \mathrm{Aut}_{F^H}(F)$.

(ii) The Normal Basis Theorem can be rephrased as follows: as a representation of the Galois group $\mathrm{Gal}(F/K)$, the K-v.s. F is an *induced* representation from the trivial representation K.

APPENDIX 7: TRANSITIVITY OF TRACES / NORMS (§3.3)

We prove an improved version of Lemma 95(ii) and Lemma 96.

Proposition. *Let F/K be a finite ext'n and $K \subset L \subset F$, with $[F:L] = m$.*

(i) *If $\alpha \in L$, then $T_{F/K}(\alpha) = mT_{L/K}(\alpha)$ and $N_{F/K}(\alpha) = N_{L/K}(\alpha)^m$.*

(ii) *If $F = L(\alpha)$ for $\alpha \in F$ and $P_\alpha = X^m - a_1X^{m-1} + a_2X^{m-2} - \cdots + (-1)^m a_m \in L[X]$ is its min. poly. over L, then $T_{F/K}(\alpha) = T_{L/K}(a_1)$ and $N_{F/K}(\alpha) = N_{L/K}(a_m)$.*

(iii) *$T_{F/K} = T_{L/K} \circ T_{F/L}$ and $N_{F/K} = N_{L/K} \circ N_{F/L}$.*

Remark. If $L = K$ then $T_{L/K} = N_{L/K} = \mathrm{id}$, hence (i) is Lem. 95(ii) and (ii) is Lem. 96(i).

Proof. Let $\{\beta_1, \dots, \beta_n\}$ (resp. $\{\gamma_1, \dots, \gamma_m\}$) be a basis of L/K (resp. F/L). Then by the proof of Tower Law (Prop. 8) $\{\gamma_1\beta_1, \dots, \gamma_1\beta_n, \gamma_2\beta_1, \dots, \gamma_2\beta_n, \dots, \gamma_m\beta_1, \dots, \gamma_m\beta_n\}$ is a basis of F/K.

(i): Let $A \in M_n(K)$ be the matrix for $m_\alpha : L \to L$ with respect to $\{\beta_j\}$, so that $T_{L/K}(\alpha) = \mathrm{tr}(A)$ and $N_{L/K}(\alpha) = \det(A)$.

Then the matrix for $m_\alpha : F \to F$, with respect to $\{\gamma_i\beta_j\}$ is $\begin{pmatrix} A & 0 & \cdots & 0 \\ 0 & A & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & A \end{pmatrix} \in M_{mn}(K)$, hence $T_{F/K}(\alpha) = m\,\mathrm{tr}(A)$ and $N_{L/K}(\alpha) = \det(A)^m$.

(ii): Take $\{\gamma_1, \dots, \gamma_m\} = \{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ as the basis of F/L. Then the matrix of the L-linear map $m_\alpha : F \to F$ with respect to $\{\gamma_i\}$ is $\begin{pmatrix} 0 & & & (-1)^{m-1}a_m \\ 1 & \ddots & & \vdots \\ & \ddots & 0 & -a_2 \\ & & 1 & a_1 \end{pmatrix} \in M_m(L)$, since $\alpha^m = a_1\alpha^{m-1} - a_2\alpha^{m-2} + \cdots + (-1)^{m-1}a_m$.

Let $A_i \in M_n(K)$ be the matrix for the K-linear map $m_{a_i} : L \to L$, with respect to $\{\beta_j\}$. Then the matrix for the K-linear map $m_\alpha : F \to F$ with respect to $\{\gamma_i\beta_j\}$ is given by $\begin{pmatrix} 0 & & & (-1)^{m-1}A_m \\ I_n & \ddots & & \vdots \\ & \ddots & 0 & -A_2 \\ & & I_n & A_1 \end{pmatrix} \in M_{mn}(K)$, hence $T_{F/K}(\alpha) = \mathrm{tr}(A_1) = T_{L/K}(a_1)$.

Also, the determinant of this matrix is equal to $(-1)^{n(mn-1)} \begin{vmatrix} (-1)^{m-1}A_m & 0 & & \\ \vdots & I_n & \ddots & \\ -A_2 & & \ddots & 0 \\ A_1 & & & I_n \end{vmatrix}$ by permuting the columns cyclically to the right n times.

Hence $N_{L/K}(\alpha) = (-1)^{n(mn-1)} \det\big((-1)^{m-1}A_m\big) = (-1)^{mn(n+1)-2n} \det(A_m) = N_{L/K}(a_m)$.

(iii): Let $\alpha \in F$ and $L' := L(\alpha)$. First assume $F = L'$. Then (ii) says $T_{L'/K}(\alpha) = T_{L/K}(a_1)$ and $N_{L'/K}(\alpha) = N_{L/K}(a_m)$. Letting $K = L$, it reads $T_{L'/L}(\alpha) = a_1$ and $N_{L'/L}(\alpha) = a_m$. Comparing these formulas gives $T_{L'/K}(\alpha) = T_{L/K}\big(T_{L'/L}(\alpha)\big)$ and $N_{L'/K}(\alpha) = N_{L/K}\big(N_{L'/L}(\alpha)\big)$. Using these, in the general case we have:

$$T_{F/K}(\alpha) \overset{\text{(i)}}{=} [F:L'] \cdot T_{L'/K}(\alpha) \overset{\text{Lem. 95(i)}}{=} T_{L/K}\big([F:L'] \cdot T_{L'/L}(\alpha)\big) \overset{\text{(i)}}{=} T_{L/K}\big(T_{F/L}(\alpha)\big)$$

$$N_{F/K}(\alpha) \overset{\text{(i)}}{=} N_{L'/K}(\alpha)^{[F:L']} \overset{\text{Lem. 95(i)}}{=} N_{L/K}\big(N_{L'/L}(\alpha)^{[F:L']}\big) \overset{\text{(i)}}{=} N_{L/K}\big(N_{F/L}(\alpha)\big). \qquad \square$$

APPENDIX 8: WHAT NEXT?

Galois Theory is related to many areas of pure mathematics.

Part II courses.

(A) *Number Fields*. Natural continuation of our study of Galois groups over $\mathbb{Q}$ leads to *algebraic number theory*. By defining the ring of integers for *number fields* (finite ext'ns of $\mathbb{Q}$), the contents of §2.4, §2.7 receive a cleaner treatment and further generalisations.

(B) *Algebraic Geometry*. The theory of finite ext'ns of fields is nothing other than 0-dimensional algebraic geometry. Algebraic manipulations of function fields (with many variables) and their subrings are imbued with geometric intuitions by the study of *algebraic varieties* (geometric objects defined as zero sets of polynomials in many variables).

(C) *Riemann Surfaces, Algebraic Topology*. 1-dim'l algebraic geometry over $\mathbb{C}$ grew out of complex analysis via theory of Riemann surfaces. The function fields over $\mathbb{C}$ appear as fields of meromorphic functions, which are at first treated by analytical methods. Geometry of complex manifolds, including their topological properties, are translated into algebraic theory of fields. Topological analogues of the field ext'ns and their Galois groups are the *covering spaces* and the *fundamental groups* in algebraic topology.

(D) *Representation Theory*. The Fundamental Theorem of Galois Theory says that the symmetry groups (automorphism groups) control mathematical objects — then in turn one can study a group by studying how it acts on various objects. *Representations* are the most important examples of this principle, namely vector spaces on which a group acts.

Further afield.

Progress in many areas of maths and physics were philosophically based on Galois Theory, but here we mention some research areas directly connected to Galois Theory.

(A) *Categories, Schemes, Toposes*. FTGT can be seen as a classification of fields in terms of objects (here Hom sets) acted on by the Galois group. This is best understood in the language of *categories*. Grothendieck pushed this idea further to revolutionise algebraic geometry by the theory of *schemes* and *toposes*, where Galois groups and fundamental groups are unified. Now Galois Theory is an example of *descent theory*, obtaining global objects by glueing local objects.

(B) *Number Theory*. There are many unsolved mysteries on the absolute Galois group of $\mathbb{Q}$, not only the inverse Galois problem. Its representations, *Galois representations*, are the main object of study in modern algebraic number theory (e.g. solution of Fermat's Last Theorem). Generalising *Class Field Theory* (the theory of abelian ext'ns of number fields), deep connections with algebraic geometry and representation theory (*modular forms*) are proposed (*the Langlands program*).

(C) *Arithmetic Geometry*. Grothendieck's reformulation of Galois Theory lead to the conjectural existence of the *motivic Galois group*, a huge extension of the absolute Galois group of a field, which controls the motives (cohomology theories) of algebraic varieties of arbitrary dim'n (as opposed to 0-dim'n in Galois Theory). The theory rests on many unsolved conjectures, but gives a dream vision of a vastly extended Galois Theory.

Review of §§2–3.

Def. 52: Characteristics, prime fields. Lem. 53: $K[X]$ is a UFD; $|\operatorname{Root}_P(K)| \leq \deg P$.

Def. 54: Splits in E, splitting fields.

Lem. 55: Splits $\iff$ $\exists K$-hom from a splitting field; $|\operatorname{Root}_P(E)|$ constant when split.

Prop. 56: Splitting field exists, unique up to K-isom.

Def. 57: Algebraically closed, alg. closures. Th. 58: Alg. closure exists, unique up to K-isom.

Lem. 59: K finite $\Rightarrow |K| = q = (\operatorname{char} K)^d$, and K is a splitting field of $X^q - X$.

Def. 60: Derivation. Prop. 61: Leibniz's law; multiple root of P = common root of $P, D(P)$.

Cor. 62: $X^N - 1$ has no multiple root unless $\operatorname{char} K \mid N$.

Lem. 63: $x \mapsto x^p$ is $\mathbb{F}_p$-hom. in char. p. Def. 64: Frobenius map Fr_p; q-th power Frob. Fr_q.

Th. 65: $\exists \mathbb{F}_q$, unique up to $\mathbb{F}_p$-isom., for each q; $\mathbb{F}_q \subset \mathbb{F}_{q'} \iff q' = q^n$.

Lem. 66: $\operatorname{Fr}_q \in \operatorname{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^n})$, order n. Lem. 67: Finite subgroups of $K^\times$ are cyclic.

Th. 68: $\mathbb{F}_{q^n}/\mathbb{F}_q$ is simple and Galois. Def. 69: Cyclotomic ext'ns, primitive roots of unity.

Prop. 70: Cyclotomic poly. $\Phi_N \in \mathbb{Z}[X]$ has all prim. N-th roots of 1 as roots ($(\operatorname{char} K, N) = 1$);
$\operatorname{Gal}\big(K(\boldsymbol{\mu}_N)/K\big) \hookrightarrow \big(\mathbb{Z}/(N)\big)^\times$, all irred. factors of Φ_N in $K[X]$ have deg. $[K(\boldsymbol{\mu}_N) : K]$.

Th. 71: Irreducibility of Cyclotomic Polynomials. Def. 72: Separable polynomials.

Lem. 73: P separable $\iff$ coprime to $D(P)$; Irred. P separable $\iff$ $D(P) \neq 0$;
Every irred. P separable in char. 0; Separability is stable under K-hom's/factors.

Def. 74: Separable/normal ext'ns. Lem. 75: Inequality from Roots & Hom's II.

Prop. 76: $|\operatorname{Hom}_K(F, E)| \leq [F : K]$ when F/K finite. If equal, then for any $K \subset L \subset F$,
$|\operatorname{Hom}_K(L, E)| = [L : K]$ and $\operatorname{Hom}_K(F, E) \twoheadrightarrow \operatorname{Hom}_K(L, E)$.

Th. 77: Characterisation of separable/Galois ext'ns; Finite F/K sep. $\iff$ $F/L, L/K$ sep.

Th. 78: Primitive Element Th'm (Finite separable $\Rightarrow$ simple).

Prop. 79: For a product of separable poly's, splitting field is Galois and Prop. 42 valid.

Prop. 80: Cycle type of Fr_p in $\operatorname{Gal}(P) \hookrightarrow S_n$. Def. 81: Elementary symmetric polynomials.

Prop. 82: Rational Symmetric Function Theorem. Th. 83: SFT.

Th. 84: $\operatorname{Gal}(P)$ for $P \in \mathbb{Z}[X]$ and factorisation of $P \bmod p$. (Lem. 85: auxiliary.)

Lem. 86: $\operatorname{Hom}_{K\text{-vs}}(V, E)$ is an E-v.s. with dim.$= \dim_K V$.

Prop. 87: Dedekind's Lemma (linear independence of K-hom's).

Prop. 88: Artin's Lemma (G finite $\Rightarrow F/F^G$ Galois with $\operatorname{Gal}(F/F^G) = G$).

Def. 89: Ext'ns/morphisms (generalised). Def. 90: Finite/Galois ext'ns, degrees.

Lem. 91: Hom sets bijective with the old Hom_K sets. Def. 92: Towers of ext'ns.

Prop. 93: Hom for towers, Tower Law, Towers & Galois ext'ns.

Def. 94: Traces/norms. Lem. 95: Trace is K-linear, norm is multiplicative.

Lem. 96: Trace/norm & min. poly.; transitivity of traces. Prop. 97: Insep. $\Longrightarrow$ trace map $= 0$.

Prop. 98: Sep. $\Longrightarrow$ trace/norm is sum/product of conjugates. Th. 99: Sep. $\iff$ trace map $\neq 0$.

Th. 100: Hilbert's Th. 90. Cor. 101: Kummer theory.

INDEX