Math 501: Field and Galois Theory
Lecture Notes

Lior Silberman

These are my rough notes for the 2020 course, compiled December 19, 2020. They are posted for traditional academic reuse (with attribution) but are otherwise copyright by Lior Silberman, and are specifically excluded from the terms of UBC Policies LR12 and 81.

Contents

CHAPTER 1

Introduction

Lior Silberman, `lior@Math.UBC.CA`, `https://www.math.ubc.ca/~lior/`
Office: Math Annex 1112
Phone: 604-827-3031

For administrative details see the syllabus.

1.1. About the course

Course plan.

1.2. Motivating problems

Duplicating the cube, trisecting the angle, squaring the circle.
Insolubility of the quintic.
Cyclotomic extensions and Fermat's Last Theorem

1.3. Background: definitions and propositions

1.3.1. Set Theory.

NOTATION 1. We write $\emptyset$ for the empty set, $[n] = \{0, \ldots, n-1\}$ for the standard set of size n.

NOTATION 2. For a set A write:

$$\bigcup A \stackrel{\text{def}}{=} \{x \mid \exists y \in A : x \in y\}, \qquad \bigcap A \stackrel{\text{def}}{=} \{x \mid \forall y \in A : x \in y\},$$

$$\mathcal{P}(A) = \{a \mid a \subseteq A\}.$$

For two sets A, B we write $A \cup B$, $A \cap B$ for $\bigcup\{A, B\}$ and $\bigcap\{A, B\}$ respectively. Also write

$$A \setminus B \stackrel{\text{def}}{=} \{x \in A \mid x \notin B\} \qquad A \Delta B \stackrel{\text{def}}{=} (A \setminus B) \cup (B \setminus A),$$

$$A \times B \stackrel{\text{def}}{=} \{x \mid \exists a \in A, b \in B : x = (a, b)\}.$$

DEFINITION 3. A *relation* on a set S is any subset $R \subset S \times S$. We write xRy for $(x, y) \in R$, and for $A \subset S$ also $R[A] = \{y \mid \exists x \in A : (x, y) \in R\}$. We call a relation:

(1) *Reflexive* if $\forall x \in S : xRx$;
(2) *Symmetric* if $\forall x, y \in S : xRy \leftrightarrow yRx$;
(3) *Transitive* if $\forall x, y, z \in S : (xRy \wedge yRz) \to xRz$;

If $S' \subset S$ we write $R\restriction_{S'}$ for the *induced relation* $R \cap S' \times S'$.

DEFINITION 4. A *partial order* is a reflexive and transitive relation. A *linear order* is a partial order in every two elements are comparable (for every distinct $x, y \in S$ exactly one of xRy and yRx holds). A subset A of a partially ordered set S is called a *chain* if $R\restriction_A$ is a linear order on A.

If $(S, \leq)$ is a partial order and $A \subset S$ we say $m \in S$ is an *upper bound* for A if for any $a \in A$ we have $a \leq m$. We say $m \in S$ is *maximal* if for any $m' \in S$ such that $m \leq m'$ we have $m = m'$. Note that maximal elements are not necessarily upper bounds for S (why?).

AXIOM 5 (Zorn's Lemma). *Let $(S, \leq)$ be a partial order such that every chain in S has an upper bound. Then S has maximal elements.*

Definition 6. A *function* is a set f of ordered pairs such that $\forall x, y, y'\ ((x,y) \in f \wedge (x,y') \in f) \to y = y'$. For a function f write $\mathrm{Dom}(f) = \{x \mid \exists y : (x,y) \in f\}$, $\mathrm{Ran}(f) = \mathrm{Im}(f) = \{y \mid \exists x : (x,y) \in f\}$ for its domain and range (image), respectively, and if $x \in \mathrm{Dom}(f)$ write $f(x)$ for the unique y such that $(x,y) \in f$. Say that f is a function *from* X *to* Y if $\mathrm{Dom}(f) = X$ and $\mathrm{Ran}(f) \subset Y$, in which case we write $f : X \to Y$. Write Y^X for the set of functions from X to Y.

Given a function f and $A \subset \mathrm{Dom}(f)$ write $f[A]$ for the *image* $\{f(x) \mid x \in A\}$ and $f\restriction_A$ for the *restriction* $\{(x,y) \in f \mid x \in A\}$. This is a function with domain A and range $f[A]$.

Say that a function f is *injective* if $\forall x, x' : (f(x) = f(x')) \to (x = x')$; say that $f : X \to Y$ is *surjective* if $f[X] = Y$, *bijective* if it is injective and surjective.

Axiom 7 (Axiom of Choice). *Let X be a set. Then there exists a function c with domain X such that for all $\emptyset \neq x \in X$ we have $c(x) \in x$.*

Fact 8. *Under the usual (Zermelo–Frenkel) axioms of set theory, AC is equivalent to Zorn's Lemma.*

Notation 9. Let A be a function with domain I. We write:

$$\bigcup_{i \in I} A(i) \stackrel{\mathrm{def}}{=} \bigcup \mathrm{Ran}(A), \qquad \bigcap_{i \in I} A(i) \stackrel{\mathrm{def}}{=} \bigcap \mathrm{Ran}(A)$$

and

$$\times_{i \in I} A(i) \stackrel{\mathrm{def}}{=} \{f \mid f \text{ is a function with domain } I \text{ and } \forall i \in I : f(i) \in A(i)\} \subset \mathcal{P}\left(I \times \bigcup_{i \in I} A(i)\right).$$

Note that the axiom of choice is the following assumption: let A be a function on I such that for all $i \in I$, $A(i)$ is non-empty. Then $\times_{i \in I} A_i$ is non-empty.

Definition 10. For two sets A, B write $|A| \leq |B|$ if there exists an injective function $f : A \to B$, $|A| = |B|$ if these exists a bijection between A and B. Both relations are clearly transitive and reflexive. The second is clearly symmetric.

Theorem 11 (Comparing cardinals).
1. *(Cantor-Schroeder-Bernstein)$|A| \leq |B|$ and $|B| \leq |A|$ together imply $|A| = |B|$.*
2. *(Corollary of Zorn's Lemma) Given A, B at least one of$|A| \leq |B|$ and $|B| \leq |A|$ holds.*

Notation 12. For a set A and a cardinal κ We set $\binom{A}{\kappa} = \{x \in \mathcal{P}(A) \mid |x| = \kappa\}$ (read "A choose κ").

1.3.2. Group theory.

1.3.2.1. *Basics.*

Definition 13. A *group* is a quadruplet $(G, e, \iota, \cdot)$ where G is a set, $e \in G$, $\iota : G \to G$, $\cdot : G \times G \to G$ and:

1. $\forall g, h, k \in G : (g \cdot h) \cdot k = g \cdot (h \cdot k)$ (associative law).
2. $\forall g \in G : e \cdot g = g$ (identity)
3. $\forall g \in G : \iota(g) \cdot g = e$ (inverse)

Call the group G *Abelian* (or *commutative*) if for all $g, h \in G$, $g \cdot h = h \cdot g$.

Remark 14. We will identify the group and its underlying set without fear of confusion.

Example 15. The *symmetric group* on the set X is the set S_X of all bijections $X \to X$, with the composition operation and the compositional inverse. The identity element is the identity map.

Notation 16. Write S_n for $S_{[n]}$ ("the symmetric group on n letters").

Lemma 17. *Let G be a group, $g, h \in G$. Then $g \cdot e = g$, $g \cdot \iota(g) = e$, and the equations $gx = h$ and $xg = h$ have unique solutions. In particular the identity elements and inverses are unique; we will henceforth write g^{-1} for $\iota(g)$.*

Definition 18. A non-empty subset $H \subset G$ is a *subgroup* if $e \in H$ and if $\iota(H), H \cdot H \subset H$. In that case we write $H < G$, and $(H, e, \iota\restriction_H, \cdot\restriction_{H \times H})$ is a group. The subgroup H is *normal* (denoted $H \lhd G$) if for all $g \in G$, ${}^gH = gHg^{-1} = H$.

When $H < G$ write $G/H = \{gH \mid g \in G\}$, $H\backslash G = \{Hg \mid g \in G\}$, and $[G : H]$ for the cardinality of either of these sets , the *index* of H in G.

Exercise 19. The set G/H, $H\backslash G$ are equinumerous since ι induces a bijection between them.

Definition 20. For $S \subset G$ the subgroup generated by S is the subgroup $\langle S\rangle = \bigcap\{H < G \mid S \subset H\}$.

Lemma 21. *The intersection of any non-empty set of subgroups of G is a subgroup of G. $\langle S\rangle$ is the set of all* words *in the elements of S, that is the set of all elements of the form $s_1^{\epsilon_1} \cdots s_r^{\epsilon_r}$ where $s_i \in S$, $\epsilon_i \in \{\pm 1\}$ (the empty product is e by definition).*

Theorem 22 (Lagrange). *Let $H < G$. Then there is a set-theoretic bijection between $H \times G/H$ and G. In particular, if $|G|$ is finite then $|H| \mid |G|$.*

Lemma 23. *If N is normal in G iff $G/N = N\backslash G$ iff setting $aN \cdot bN \stackrel{def}{=} abN$ defines a group structure on G/N. We write q_N for the map $g \mapsto gN$.*

Definition 24. Let H, G be groups. A map $f\colon H \to G$ is a *group homomorphism* if $f(ab) = f(a)f(b)$ for all $a, b \in H$. This implies that $f(e_H) = e_G$ and that $f \circ \iota_H = \iota_G \circ f$. The set of homomorphisms will be denoted $\mathrm{Hom}(H, G)$. The *kernel* of $f \in \mathrm{Hom}(H, G)$ is the set $\mathrm{Ker}(f) = \{h \in H \mid f(h) = e_G\}$. The *image* of f is the set $\mathrm{Im}(f) = \mathrm{Ran}(f)$. When $N \lhd G$ the map q_H is a group homomorphism called the *quotient map*.

Exercise 25. Let $f \in \mathrm{Hom}(H, G)$. Then f is a monomorphism iff it is injective, an epimorphism iff it is surjective, and an isomorphism iff it is bijective.

Example 26. Given a group G, the set of isomorphisms $G \to G$ is itself a group under composition, the *automorphism group* of G, denoted $\mathrm{Aut}(G)$.

Exercise 27. S_X is isomorphic to S_Y iff $|X| = |Y|$.

Proposition 28 (Isomorphism theorems). *Let $f \in \mathrm{Hom}(H, G)$. Then $\mathrm{Ker}(f) \lhd H$, $\mathrm{Im}(f) < G$. Moreover there is a unique isomorphism $\bar{f}\colon H/\mathrm{Ker}(f) \to \mathrm{Im}(f)$ such that $\bar{f} \circ q_{\mathrm{Ker}(f)} = f$.*

Lemma 29. *Let $H, N < G$ with N normal. Then $HN < G$, N is normal in HN, $H \cap N$ is normal in H, and $HN/N \simeq H/H \cap N$.*

Finally, let $N \lhd G$. Then q_N induces an order- and normality-preserving bijection between subgroups of G containing N and subgroups of G/N. If $N < H < G$ and $H \lhd G$ as well then $G/H \simeq (G/N)/(N/H)$.

Lemma-Definition 30. *For $g \in G$ the* conjugation *map $\gamma_g(x) = gxg^{-1}$ is an automorphism of G. The map $g \mapsto \gamma_g$ is a homomorphism $G \mapsto \mathrm{Aut}(G)$ whose image $\mathrm{Inn}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$ called the subgroup of* inner automorphisms. *We call the quotient $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$ the* outer automorphism group.

Definition 31. Given groups N, H their (external) *direct product* is the group with underlying set $N \times H$ and coordinatewise operations. Given groups N, H and a homomorphism $f\colon H \to \mathrm{Aut}(N)$ their (external) *semidirect product* $N \ltimes_f H$ is the group with underlying set $N \times H$ and multiplication given by $(n', h') \cdot (n, h) = \left(n' n^{f(h)}, hh'\right)$.

Lemma-Definition 32. *Let $N, H \subset G$ be subgroups. We say NH is the (internal)* semidirect product *of N, H if H normalizes N and $H \cap N = \{1\}$, equivalently if there is f such that the map $N \ltimes_f H \to G$ given by $(n, h) \mapsto nh$ is an injection. We say the product is* direct *if f is trivial, equivalently if N, H commute or if N normalizes H as well.*

Example 33. The *infinite cyclic groups* is the additive group of $\mathbb{Z}$; the *finite cyclic groups* are its quotients $C_n \simeq (\mathbb{Z}/n\mathbb{Z}, +)$, $n \in \mathbb{Z}_{\geq 1}$.

Lemma 34. *If $x \in G$ then $\langle x\rangle$ is isomorphic to a cyclic group. The order of $\langle x\rangle$ is called the* order *of x and is equal to the smallest $n \geq 1$ such that $x^n = e$.*

Notation 35. We write C_n for the cyclic group of order n, $D_{2n} = C_2 \ltimes C_n$ for the dihedral group of order $2n$ ($\{\pm 1\} \in (\mathbb{Z}/n\mathbb{Z})^\times$ acting on $(\mathbb{Z}/n\mathbb{Z}, +)$ by multiplication).

EXERCISE 36. The set T of *transpositions* generates S_n. There is a unique homomorphism $\mathrm{sgn}\colon S_n \to C_2$ taking the non-identity value on every transposition. Its kernel is the *alternating group* A_n, which is generated by the set of 3-cycles.

DEFINITION 37. A group G is *simple* if it is non-trivial and has no normal subgroup other than $G, \{e\}$.

FACT 38. *The groups A_n ($n \geq 5$) and $\mathrm{PSL}_n(\mathbb{F}_q)$, ($n > 2$ or $n = 2$ and $q > 3$) are simple.*

1.3.2.2. *Group actions.*
1.3.2.3. *Sylow Theorems.*

1.3.3. Ring theory. All rings in this course are commutative unless noted otherwise.
1.3.3.1. *Basics.*

DEFINITION 39. A (commutative) *ring* is a quintuple $(R, 1, 0, +, \cdot)$ consisting of a set R, two elements $0, 1 \in R$ and two binary operations $+, \cdot\colon R \times R \to R$, such that:

(1) $(R, 0, +)$ is an Abelian group;
(2) $\forall x, y, z \in R:\ (x \cdot y) \cdot z = x \cdot (y \cdot z)$ [associative law];
(3) $\forall x \in R:\ 1 \cdot x = x \cdot 1 = x$ [multiplicative identity];
(4) $\forall x, y \in R:\ x \cdot y = y \cdot x$ [commutative law];
(5) $\forall x, y, z \in R:\ x \cdot (y + z) = x \cdot y + x \cdot z \wedge (y + z) \cdot x = y \cdot x + z \cdot x$ [distributive law];
(6) $0 \neq 1$ [non-degeneracy].

LEMMA 40. *Let R be a ring.*

(1) *The neutral elements are unique.*
(2) *For any $r \in R$ we have $0 \cdot r = r \cdot 0 = 0$.*

DEFINITION 41. Let R be a ring, and let $r \in R$.

(1) Say that r is *invertible* (or that it is a *unit*) if these exists $\bar{r} \in R$ such that $r \cdot \bar{r} = \bar{r} \cdot r = 1_R$. Write $R^\times$ for the set of units.
(2) Say that r is *reducible* if $r = ab$ for some non-units $a, b \in R$, *irreducible* otherwise.
(3) Say that r is a *zero-divisor* if these exists a non-zero $s \in R$ such that $rs = 0$ or $sr = 0$.

- The ring is called an *integral domain* if the only zero-divisor is 0, a *field* if every non-zero element is invertible.

LEMMA-DEFINITION 42. *Let $r \in R$ be invertible. Then it has a unique multiplicative inverse, to be denoted r^{-1} from now on. Writing $R^\times$ for the set of invertible elements,$(R^\times, 1, \cdot)$ is an abelian group, the* multiplicative group *of R.*

EXAMPLE 43 (Rings). (1) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/m\mathbb{Z}$.
(2) For a ring R and a set X, the space of functions R^X with pointwise operations.
(3) For a ring R, the *ring of polynomials* $R[x]$.

DEFINITION 44. Let R, S be rings. The map $f\colon R \to S$ is a *ring homomorphism* if:

(1) $f(0_R) = 0_S$.
(2) $f(1_R) = 1_S$.
(3) For all $x, y \in R$, $f(x +_R y) = f(x) +_S f(y)$.
(4) For all $x, y \in S$, $f(x \cdot_R y) = f(x) \cdot_S f(y)$.

The set of homomorphisms from R to S will be denoted $\mathrm{Hom}(R, S)$.

LEMMA 45. *Let $f \in \mathrm{Hom}(R, S)$. Then f is a monomorphism iff it is injective, an epimorphism iff it is surjective, and an isomorphism iff it is bijective.*

DEFINITION 46. An additive subgroup $I \subset R$ is an *ideal* if for all $r \in R$ and $a \in I$, $ra \in I$. We write $I \lhd R$.

LEMMA 47. *There is a unique ring structure on the additive group R/I such that the quotient map $q_I\colon R \to R/I$ is a ring homomorphism.*

The kernel of any ring homomorphism is an ideal; if $f \in \mathrm{Hom}(R, S)$ then there exists a unique isomorphism $\bar{f}\colon R/\operatorname{Ker}(f) \to \operatorname{Im}(f)$ so that $f = \bar{f} \circ q_{\operatorname{Ker}(f)}$.

LEMMA-DEFINITION 48. *The intersection of a set of ideals is an ideal. The intersection of the set of ideals containing $X \subset R$ is called the* ideal generated by A *and denoted* (X).

LEMMA 49. (X) *is the set of all linear combinations* $\sum_{i=1}^{r} a_i x_i$ *where* $a_i \in R$ *and* $x_i \in X$ *(the empty combination is zero).*

LEMMA-DEFINITION 50. *Let* I, J *be ideals. Then* $\langle I \cup J \rangle = I + J \stackrel{def}{=} \{i + j \mid i \in I, j \in J\}$ *and* $IJ = \langle \{ij \mid i \in I, j \in J\} \rangle$.

PROPOSITION 51 (Chinese Remainder Theorem). *Let* $\{I_i\}_{i=1}^{r}$ *be ideals such that* $I_i + I_j = (1) = R$ *for all* $i \neq j$. *Then the obvious homomorphism* $R \mapsto \prod_{i=1}^{r} (R/I_i)$ *is an isomorphism of rings.*

LEMMA-DEFINITION 52. *Call an ideal* prime *if the product of two non-members of it is a non-member. Then an ideal* I *is prime iff* R/I *is an integral domain,* maximal *(wrt inclusion) if* R/I *is a field.*

1.3.3.2. *Unique factorization.*

DEFINITION 53. Euclidean domain, PID, UFD

LEMMA 54. *Euclidean => PID => UFD*

EXAMPLE 55. $\mathbb{Z}$, $F[x]$ for a field F.

1.3.4. Modules. Let R be a ring.

DEFINITION 56. An R-module is a quadruplet $(V, \underline{0}, +, \cdot)$ where $(V, \underline{0}, +)$ is an abelian group , and $\cdot\colon R \times V \to V$ is such that:

(1) For all $\underline{v} \in V$, we have $1_R \cdot \underline{v} = \underline{v}$.
(2) For all $\alpha, \beta \in R$ and $\underline{v} \in V$, $\alpha \cdot (\beta \cdot \underline{v}) = (\alpha\beta) \cdot \underline{v}$ ($\alpha\beta$ denotes the product in R).
(3) For all $\alpha, \beta \in R$ and $\underline{u}, \underline{v} \in V$, $(\alpha + \beta)(\underline{u} + \underline{v}) = \alpha \cdot \underline{u} + \beta \cdot \underline{u} + \alpha \cdot \underline{v} + \beta \cdot \underline{v}$ (note that the RHS is meaningful since addition is associative and commutative).

If V, W are R-modules we call a map $f\colon V \to W$ a *homomorphism of R-modules* if it is a homomorphism of abelian groups such that for all $\alpha \in R$ and $\underline{v} \in V$, $f(\alpha \cdot \underline{v}) = \alpha \cdot f(\underline{v})$. Write $\mathrm{Hom}_R(V, W)$ for the set of R-module homomorphisms from V to W (the R may be omitted when clear from context). The kernel and image of a homomorphism are its kernel and image as a map of abelian groups.

LEMMA 57. *Let* $f \in \mathrm{Hom}_R(V, W)$. *Then* f *is a monomorphism iff it is injective, an epimorphism iff it is surjective, and an isomorphism iff it is bijective.*

EXAMPLE 58. Let X be a set, R a ring. Then R^X has the structure of an R-module under the *diagonal action* of R. We usually write R^n for $R^{[n]}$.

Complex conjugation is an element of $\mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, \mathbb{C})$ but not of $\mathrm{Hom}_{\mathbb{C}}(\mathbb{C}, \mathbb{C})$.

LEMMA 59. *Let* V *be an* R*-module. Then for every* $\underline{v} \in V$ *we have* $0_R \cdot \underline{v} = \underline{0}$.

DEFINITION 60. Let V be an R-module. An additive subgroup $W \subset V$ is an R-*submodule* if for all $\alpha \in R$ and $\underline{w} \in W$, $\alpha\underline{w} \in W$.

LEMMA 61. *Let* $f \in \mathrm{Hom}_R(V, W)$. *Then* $\mathrm{Ker}(f) \subset V$ *and* $\mathrm{Im}(f) \subset W$ *are* R*-submodules.*

1.3.5. Linear algebra. Fix a field F. We introduce the following terms for F-modules:

- An F-module will be a called an F-vectorspace.
- An F-homomorphism will be called an F-linear map.
- The submodule generated by a subset of a vector space will be called the *linear span* of the subset.
- Bases and dimension, rank-nullity.
- Eigenvalues and eigenvectors
- Characteristic polynomial
- Cayley Hamilton

1.4. A bit more group theory (Lectures 2-3, 11/9/2020 + 14/9/2020)

Some examples of groups:

EXAMPLE 62. $S_X = \{f : X \to X \mid f \text{ invertible}\}$. If M is an R-module then $\mathrm{Aut}(M) = \{f \in \mathrm{Hom}_R(M, M) \mid f \text{ invertible}\}$.

In particular, if $M = R^n$ then $\mathrm{Aut}(M) = \mathrm{GL}_n(R)$ is the group of $n \times n$ invertible matrices with entries in R. Also have a group homomorphism $\det : \mathrm{GL}_n(R) \to \mathrm{GL}_1(R) = R^\times$. Its kernel is the normal subgroup $\mathrm{SL}_n(R)$. Important subgroups: $U_n(R)$ are the upper-triangular matrices with 1 on the diagonal, $T_n(R)$ are the diagonal matrices, and $B_n(R) = T_n(R) \ltimes U_n(R)$ are the upper-triangular invertible matrices.

DEFINITION 63. A group is *linear* if it can be embedded in $\mathrm{GL}_n(F)$ for a field F.

EXERCISE 64. $\mathrm{GL}_1(\mathbb{R}) \overset{\text{def}}{=} \mathrm{Aut}_R(R) \simeq R^\times$.

EXERCISE 65. $\mathrm{SL}_2(\mathbb{Z})$ is generated by the matrices $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.

1.4.1. Abelian quotients and the derived subgroup.

Fix a group G.

DEFINITION 66. A *commutator* in G is an element of the form $[x, y] = xyx^{-1}y^{-1}$ where $x, y \in G$. The *derived subgroup* of G is the group $G^{(1)} = G'$ generated by the commutators.

LEMMA-DEFINITION 67. *Let G, H be groups, $f : G \to H$ a homomorphism.*

(1) *$f(G)$ is a commutative subgroup of H if and only if the kernel of f contains G'.*
(2) *G' is a normal subgroup of G. It follows that the quotient $G^{ab} = G/G'$ is commutative.*
(3) *If $f(G)$ is commutative there is a unique homomorphism $\bar{f} : G^{ab} \to H$ so that $f = \bar{f} \circ q$ where q is the quotient map of the abelianization.*

Call G^{ab} (and the quotient map $q : G \to G^{ab}$) the abelianization of G.

1.4.2. Composition series.

DEFINITION 68. A *normal series* in a group G is a sequence of subgroups $G = G_0 \supsetneq G_1 \supsetneq G_2 \supsetneq \cdots \supsetneq G_k = \{e\}$ such that $G_{i+1} \lhd G_i$.

We think of G as being "assembled" from the successive quotients G_i/G_{i+1}.

DEFINITION 69. A normal series *refines* another if it contains all the terms of the other (and possibly more). A normal series is a *composition series* if it has no proper refinement.

EXAMPLE 70. Every finite group has a composition series (refine

- If the group G_i/G_{i+1} has a non-trivial proper normal subgroup, we can refine the series by inserting a term between G_i and G_{i+1}.
- Thus a composition series is one where every quotient is *simple*. In that case we call the quotients the *composition factors* of G.

THEOREM 71 (Jordan–Hölder). *Suppose the group G has a composition series. Then its set of composition factors (with multiplicity!) does not depend on the choice of composition series.*

1.4.3. Solvable groups.

DEFINITION 72. Call a group G *solvable* if it has a normal series with abelian quotients.

REMARK 73. A finite group is solvable iff its composition factors are cyclic p-groups.

EXAMPLE 74. Every finite p-group is solvable.

PROOF. The composition factors are simple p-groups, and the only such group is C_p. □

EXAMPLE 75. S_3 is solvable.

PROOF. The subgroup of elements of order 3 is abelian and of index 2. □

LEMMA 76. *Every group of order 12 is solvable, hence S_4 is solvable.*

Proof. Let G have order 12, and let $\mathcal{P}$ be its set of 2-Sylow subgroups. $|\mathcal{P}| \in \{1,3\}$ since it must be an odd divisor of 12. If $\mathcal{P}$ has a unique member then G has a normal subgroup of order 4. Otherwise the conjugation action of G on $\mathcal{P}$ gives a homomorphism $G \to S_3$. It is not injective since $|G| = 12 > 6 = |S_3|$, and therefore has a non-trivial kernel $N = \bigcap \mathcal{P}$ (the point stabilizer of each Sylow subgroup is itself since each is a maximal subgroup in our case). N is abelian (it has order 2 or $4 = 2^2$) And G/N is solvable (it either has order $6 = 2 \cdot 3$ or 3). □

Proposition 77. *Every group of order p^2q is solvable.*

Proof. Assume the Sylow p-subgroups are not normal. Then these are $\{P_1, \ldots, P_q\}$ and $q \equiv 1\,(p)$. It follows that $q - 1 \geq p$. Next, if the Sylow q-Subgroups are not normal then there are p^2 of them, and $p^2 \equiv 1\,(q)$. But then q divides one of $p-1$ and $p+1$ so $q \leq p+1$. We conclude $q = p+1$, which is only possible if $q = 3$, $p = 2$ and $|G| = 12$. □

Fact 78. *S_n, $n \geq 5$ is not solvable.*

Proof. $S_n \supset A_n \supset \{e\}$ is a composition series. □

Proposition 79. *Let G be a group, H a subgroup, N a normal subgroup.*

(1) *If G is solvable then so are H and G/N.*
(2) *If N and G/N are solvable then so is G.*

Proof. Let $\{G_i\}_{i=0}^{k}$ be a series as in the definition. Set $H_i = H \cap G_i$, and let $h \in H_i$ and $g \in H_{i+1}$. Then $hgh^{-1} \in H$ and $ghg^{-1} \in G_{i+1}$ so $hgh^{-1} \in H_{i+1}$. Composing the inclusion $H_i \hookrightarrow G_i$ with the quotient map $G_i \to G_i/G_{i+1}$ gives a map $H_i \to G_i/G_{i+1}$ with kernel $H_i \cap G_{i+1} = H_{i+1}$. It follows that H_i/H_{i+1} embeds in G_i/G_{i+1} and in particular that it is commutative. Next, let $q \colon G \to G/N$ be the quotient map and set $\bar{N}_i = q(G_i) = G_iN/N$. Then $\bar{N}_0 = G/N$, $\bar{N}_k = \left\{e_{G/N}\right\}$ and since G_i normalizes G_{i+1} and N it normalizes $G_{i+1}N$, so its image $\bar{N}_i$ normalizes $\bar{N}_{i+1}$. Finally, the map $G_i \to \bar{N}_i/\bar{N}_{i+1}$ is surjective and its kernel contains G_{i+1}. It follows that $\bar{N}_i/\bar{N}_{i+1}$ is a quotient of the abelian group G_i/G_{i+1} hence abelian.

Conversely, let $N = N_0 \supset N_1 \supset \cdots \supset N_k = \{e\}$ and let $\bar{G}_0 = G/N \supset \bar{G}_1 \supset \cdots \supset \bar{G}_l = \{eN\}$ be normal series with abelian quotients in N and G/N, respectively. For $0 \leq i \leq l$ let G_i be the inverse image of $\bar{G}_i$, and for $i \leq l \leq l+k$ let $G_i = N_{i-l}$. This is a normal series and the quotients come from the two series combined. □

Example 80. Every finite p-group is solvable.

Proof. Let G be a finite p-group. Then $Z(G)$ is non-trivial and solvable, and $G/Z(G)$ is solvable by induction. □

1.4.4. Digression on group theory.

- Hall π-subgroups and π'-subgroups; Hall's Theorem
- Feit–Thompson.
- CFSG.

CHAPTER 2

Fields and Field extensions

2.1. Rings of Polynomials (Lecture 3, 16/9/2020)

DEFINITION 81. Let R be a ring. A *formal power series over R in the variable x* is a formal sum

$$f(x)=\sum_{i=0}^{\infty}a_ix^i$$

with $a_i \in R$, that is a function $a\colon \mathbb{Z}_{\geq 0}\to R$. We write $R[[x]]$ for the set of these formal power series. For $f=\sum_{i\geq 0}a_ix^i$, $g=\sum_{j\geq 0}b_jx^j$ in $R[[x]]$ and $\alpha\in R$. We make the following definitions:

$$\begin{aligned} f+g &\stackrel{\text{def}}{=} \sum_{i\geq 0}(a_i+b_i)x^i\,;\\ f\cdot g &\stackrel{\text{def}}{=} \sum_{k\geq 0}\left(\sum_{i+j=k}a_ib_j\right)x^k\,;\\ \alpha\cdot f &\stackrel{\text{def}}{=} \sum_{i\geq 0}(\alpha a_i)\,x^i\,. \end{aligned}$$

EXERCISE 82 (Supplement to PS1).
(1) These definitions give $R[[x]]$ the structure of a commutative R-algebra, *the ring of formal power series over R in the variable x*. $R[[x]]$ is an integral domain iff R is. The additive group of $R[[x]]$ is isomorphic to the countable direct product of copies of the additive group of R. $f\in R[[x]]^{\times}$ iff $a_0\in R^{\times}$.
(2) The subset $R[x]\subset R[[x]]$ of formal power series with finitely many non-zero coefficients is a subalgebra. The subset of polynomials of the form rx^0, $r\in R$, is a further subalgebra isomorphic to R and we identify the two.

DEFINITION 83. $R[x]$ is called the *ring of polynomials over R in the variable x*. For a non-zero $f\in R[x]$ set $\deg(f)=\max\{i\mid a_i\neq 0\}$ and call it the *degree* of f, call $a_{\deg(f)}$ the *leading coefficient*, and call f *monic* if $a_{\deg(f)}=1$ (we also set $\deg(0)=-\infty$).

Polynomials over integral domains are better behaved:

LEMMA 84 (Degree valuation). *Let R be an integral domain and let $f,g\in R[x]$. Then $\deg(fg)=\deg(f)+\deg(g)$ and $\deg(f+g)\leq\max\{\deg f,\deg g\}$, with equality if $\deg f\neq\deg g$. In particular:*
(1) *(zero-divisors) $fg=0$ only if one of f,g is zero.*
(2) *(units) $fg=1$ only if $\deg f=\deg g=0$ and $fg=1$ in R.*

The situation is even better over a field.

THEOREM 85 (Division with remainder). *Let F be a field, and let $f,g\in F[x]$ with $f\neq 0$. Then there exists unique $q,r\in F[x]$ with $\deg r<\deg f$ so that*

$$g=qf+r\,.$$

COROLLARY 86. *$F[x]$ is a Euclidean domain, hence a PID and a UFD. An ideal $I\lhd F[x]$ is prime iff it is maximal, iff $I=(f)$ with f irreducible.*

2.1.1. Divisors, GCD, LCM and unique factorization. Let R be a ring.

DEFINITION 87. $f, g, h \in R$.

- Say that f *divides* g, or that g is a *multiple* of f is there exists h such that $fh = g$.
- Say that f is *irreducible* if whenever $f = gh$ one of g, h is a unit, reducible if $f = gh$ for some g, h both of degree at least 1.
- Say that f is *prime* if whenever $f|gh$ we have either $f|g$ or $f|h$ (or both).
- If $f = \alpha g$ for $\alpha \in R^\times$ we say that f, g are *associate*. This is an equivalence relation. When $R = F[x]$ for a field F, every equivalence class has a unique monic member.

DEFINITION 88. Let $f, g \in F[x]$. The *greatest common divisor* of f, g is the monic polynomial h of maximal degree which divides both of them.

THEOREM 89. *Let f, g be polynomials. Then the Euclidean algorithm will compute a GCD, which can be written in the form $hf + kg$ for some $h, k \in F[x]$.*

PROPOSITION 90. *Every polynomial can be written as a product of irreducibles. A polynomial is irreducible iff it is prime. Every polynomial has a unique factorization into primes (up to associates).*

2.1.2. Irreducibility in $\mathbb{Q}[x]$. We will need a supply of irreducible polynomials.

THEOREM 91 (Gauss's Lemma). *Let $f \in \mathbb{Z}[x]$ be irreducible. Then f is irreducible in $\mathbb{Q}[x]$ as well.*

PROOF. Assume that f is reducible in $\mathbb{Q}[x]$, and let $a \in \mathbb{Z}_{\geq 1}$ be minimal such that

$$af = gh$$

For $g, h \in \mathbb{Z}[x]$ of degree at least 1 (that a exists follows from clearing denominators). If $a = 1$ we are done, so let p be a prime divisor of a. Letting bar denotes reductions mod p we have:

$$\bar{0} = \bar{g}\bar{h} \text{ in } \left(\mathbb{Z}/p\mathbb{Z}\right)[x] .$$

Since $\mathbb{Z}/p\mathbb{Z}$ is a field, we have without loss of generality that $\bar{g} = \bar{0}$, in other words that every coefficient of g is divisible by p. It then follows that

$$\frac{a}{p} f = \frac{g}{p} h \text{ in } \mathbb{Z}[x] ,$$

a contradiction to the minimality of a. □

THEOREM 92 (Eisenstein's criterion). *Let $f = \sum_{i=0}^n a_i x^i \in \mathbb{Z}[x]$ and let p be a prime such that: $p \nmid a_n$, $p|a_i$ for $0 \leq i \leq n-1$ but $p^2 \nmid a_0$. Then f is irreducible in $\mathbb{Q}[x]$.*

PROOF. Assume that $f = gh$. Say that $\deg(g) = r$, $\deg(h) = s$ with leading coefficients b_r and c_s, respectively. Then $r + s = n$ and $b_r c_s = a_n$. In particularly, both b_r and c_s are prime to p. Reducing modulu p we find $\bar{a}_n x^n = \bar{g}\bar{h}$ in $(\mathbb{Z}/p\mathbb{Z})[x]$. It follows that $\bar{g} = \bar{b}_r x^r$ and $\bar{h} = \bar{c}_s x^s$. Assuming $\deg(g), \deg(h) \geq 1$ this means that the constant coefficients of g, h are both divisible by p, which would make the constant coefficient of f divisible by p^2. Otherwise one of g, h is an integer, so f, g are associates in $\mathbb{Q}[x]$. □

EXAMPLE 93. The cyclotomic polynomial $\Phi_p(x) = \frac{x^p - 1}{x - 1} = \sum_{j=0}^{p-1} x^j$ is irreducible.

PROOF. The map $x \mapsto y+1$ and $y \mapsto x-1$ are isomorphisms of $\mathbb{Z}[x]$ and $\mathbb{Z}[y]$. It follows that it is enough to consider the irreducibility of $\Phi_p(y+1) = \frac{(y+1)^p - 1}{y} = y^{p-1} + \sum_{j=1}^{p-1} \binom{p}{j} y^{j-1}$. Since $p | \binom{p}{j}$ for $1 \leq j \leq p-1$ and $\binom{p}{1} = p$ is not divisible by p^2 we are done. □

EXERCISE 94. Establish the general version of Gauss's Lemma over a PID. Show that the $\Phi_{p^k}(x) = \frac{x^{p^k} - 1}{x^{p^{k-1}} - 1}$ is irreducible in $\mathbb{Z}[x]$.

2.2. Field extensions (Lectures 5-6, 21-23/9/2020)

DEFINITION 95. A *field extension* is a homomorphism of fields (often denoted L/K). If $\iota\colon K \to L$ is an extension one may identify K with $\iota(K)$. In that case write $L : K$. We call two extensions $\iota : K \to L$ and $\iota'\colon K' \to L'$ *isomorphic* if there exist isomorphisms $\lambda\colon K \to K'$ and $\eta\colon L \to L'$ intertwining them.

DEFINITION 96. If K is a subfield of L and $S \subset L$ we write $K(S)$ for the intersection of all subfields of L containing K and S and call this field "*K adjoin S*".

EXAMPLE 97. $\mathbb{Q}(i) : \mathbb{Q}$. $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$, $\mathbb{Q}(i, -i, \sqrt{5}, -\sqrt{5}) : \mathbb{Q}$.
$\mathbb{C} : \mathbb{R}$, $\mathbb{C} : \mathbb{Q}$.

DEFINITION 98. Let L/K be an extension. For $p = \sum_{i=0}^{d} a_i x^i \in K[x]$ and $\alpha \in L$ write $p(\alpha) = \sum_{i=0}^{d} a_i \alpha^i \in L$. Call $\alpha \in L$ *algebraic* over K if there is a non-zero $p \in K[x]$ such that $p(\alpha) = 0$, *transcendental* otherwise. Call the extension *algebraic* if every $\alpha \in L$ is algebraic over K.

LEMMA 99. *The "evaluation at α" map $\psi\colon K[x] \to L$ given by $\psi(p) = p(\alpha)$ is a ring homomorphism. It is the unique homomorphism satisfying $\psi(x) = \alpha$.*

PROOF. The ring structure of $K[x]$ is defined exactly for this purpose. $\square$

EXERCISE 100. Let $K(t) = \left\{ \frac{f}{g} \mid f, g \in F[x] \right\} / \sim$ where $\frac{f}{g} \sim \frac{f'}{g'}$ if $fg' = f'g$. Show that the obvious operation of addition and multiplication make $K(t)$ into a field.

LEMMA 101. *Let $\alpha \in L$ be transcendental over K. Then $K(\alpha) \simeq K(t)$ via the map $\frac{f(t)}{g(t)} \mapsto \frac{f(\alpha)}{g(\alpha)}$.*

COROLLARY 102. *If α is transcendental over K then* $\dim_K K(\alpha) = \infty$.

EXERCISE 103. The two subsets $\{t^n\}_{n \geq 0}, \left\{ \frac{1}{t-a} \right\}_{a \in K} \subset K(t)$ are linearly independent. In particular $\dim_K K(t) \geq \max\{|K|, \aleph_0\}$. Conversely $|K(t)| \leq \max\{|K|, \aleph_0\}$ so $\dim_K K(t) \leq \max\{|K|, \aleph_0\}$ and hence $\dim_K K(t) = \max\{|K|, \aleph_0\}$.

$\psi\colon K[x] \to L$ is an integral domain contained in $K(\alpha)$. Its kernel is therefore a prime ideal I of $K[x]$, consisting of all polynomials in $K[x]$ which vanish at α. When α is algebraic this kernel is non-trivial, and since $K[x]$ is a PID it follows that $I = (m)$ for some irreducible m and that the ideal (m) is maximal. Thus image of the map is a field, a subfield of L which contains α. It follows that the image is $K(\alpha)$ exactly and we have obtained:

LEMMA 104. *Let $\alpha \in L$ be algebraic over K. Then*
1. *Every element of $K(\alpha)$ is of the form $p(\alpha)$ for some $p \in K[x]$.*
2. *There is a unique monic irreducible polynomial $m \in K[x]$ such that $m(\alpha) = 0$, called the* minimal polynomial *of α over K.*
3. *If $p \in K[x]$ satisfies $p(\alpha) = 0$ then $m|p$.*

DEFINITION 105. Call $L : K$ *simple* if $L = K(\alpha)$ for some α.

PROPOSITION 106. *Let $m \in K[x]$ be irreducible. Then there exists a simple extension $L = K(\alpha)$ with $m(\alpha) = 0$, and this extension unique up to isomorphism, which can be taken to map the images of α.*

PROOF. $K \hookrightarrow K[x]/(m)$ is such an extension, which we have already seen to be isomorphic to any such $K(\alpha)$. $\square$

COROLLARY 107. $\dim_K K(\alpha) = \dim_K (K[x]/(m)) = \deg m$.

PROOF. The polynomials of degree less than m are mapped injectively into $K[x]/(m)$ (the difference of two of them cannot be divisible by m unless zero). They are mapped surjectively by division with remainder. $\square$

Combining the previous results.

THEOREM 108. *α is algebraic over K iff* $\dim_K K(\alpha) < \infty$.

Corollary 109. *Let α be algebraic over K. Then $K(\alpha)$ is algebraic over K.*

Proof. Let $\beta \in K(\alpha)$. Then $K(\beta) \subset K(\alpha)$ so $\dim_K K(\beta) \le \dim_K K(\alpha) < \infty$. $\square$

Definition 110. Let $K \hookrightarrow L$ be an extension of fields. Call $\dim_K L$ the *degree* of the extension and denote it $[L : K]$.

Proposition 111 (Multiplicativity). *Let $K \hookrightarrow L \hookrightarrow M$. Then $[M : K] = [M : L] \cdot [L : M]$.*

Proof. Let $\{\lambda_i\}_{i\in I}$ be a basis for L over K. Let $\{\mu_j\}_{j\in J}$ be a basis for M over L. We will see that $\{\lambda_i\mu_j\}_{(i,j)\in I\times J}$ is a basis for M over K. First, assume that $\sum_{i,j} a_{ij}\lambda_i\mu_j = 0$ with $a\colon I \times J \to K$ finitely supported. Then $\sum_j \left(\sum_i a_{ij}\lambda_i\right)\mu_j = 0$. Since the μ_j are independent over L, $\sum_i a_{ij}\lambda_i = 0$ for each j. Now get $a_{ij} = 0$ for all i, j. Next, let $m \in M$. Then there exists $b\colon J \to L$ of finite support such that $\sum_j b_j\mu_j = m$. Next, for each j there exists $a_j\colon I \to K$ of finite support such that $\sum_i a_{ij}\lambda_i = b_j$. It follows that $m = \sum_{i,j} \alpha_{ij}\lambda_i\mu_j$. $\square$

Corollary 112. *Let $\alpha, \beta \in L$ be algebraic over K. Then so are $\alpha + \beta$, $-\alpha$, $\alpha\beta$, and α^{-1}.*

Proof. β is algebraic over K, hence over $K(\alpha)$, and $[K(\alpha, \beta) : K] = [K(\alpha, \beta) : K(\alpha)][K(\alpha) : K] < \infty$. $\square$

Definition 113. Let $K \hookrightarrow L$. The *algebraic closure of K in L* is the set $\{\alpha \in L \mid [K(\alpha) : K] < \infty\}$. It is a subfield of L containing every algebraic extension of K contained in L

The algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$ is called the field of *algebraic numbers*.

2.3. Straightedge and Compass constructions (Lecture 7, 30/9/2020)

2.3.1. The problem. The Greek word γεωμετρία ("geometria") means "measuring the earth", and indeed it arose from practical questions such finding areas and volumes and subdividing regions. Unlike modern geometry, which primarily focuses on *relationships* (are these two figures congruent? do these points like on a straight line?), ancient geometry primarily focsed on *constructions* (divide a line segment into equal halves; divide an angle into equal thirds; construct a disc with the same area as that of a given circle; ...), and Greek geometry considered *straightedge and compass* constructions almost exclusively.

Definition 114. A *planar figure* is a finite collection of points and curves in the plane, with two distinct distinguished points lablelled "0" and "1".

A *permitted construction* is a rule by which a point or a curve may be added to a planar figure. A *construction problem* consists of an initial planar figure, a set of permitted construction, and a desired point or curve.

A *solution* of the construction problem is a sequence of permitted constructions starting with the initial figure and ending with a figure containing the desired point or curve.

(1) For any distinct curves C_1, C_2 in the figure, add an isolated intersection point of $C_1 \cap C_2$.
(2) ("straightedge") For any distinct points P, Q add the line passing through P, Q
(3) ("compass") For any two distinct points P, Q add the circle with center P passing through Q.

Here is an example problem; see Figure 2.3.1 for a pictorial representation of the solution.

Problem 115. Given distinct points P, Q, construct the midpoint of the line segment PQ.

Solution 116. Let C_1 be the circle with centre P passing through Q, let C_2 be the circle through Q passing through P. Let R, S be the intersection points of $C_1 \cap C_2$. Let L_1 be the line through P, Q and let L_2 be the line through R, S. Let Z be the intersection point $L_1 \cap L_2$. Then Z is the desired point.

Remark 117. Traditionally one also *proves* that the construction works.

Exercise 118. Give a straightedge-and-compass construction for:

(1) Given a line L and a point P, construct a line L' through P and intersecting L at right angles.
(2) Given a line L and a point P not on L, construct a line L' through P parallel to L.
(3) Given distinct points P, Q construct a point R such that PQR is an equilateral triangle.

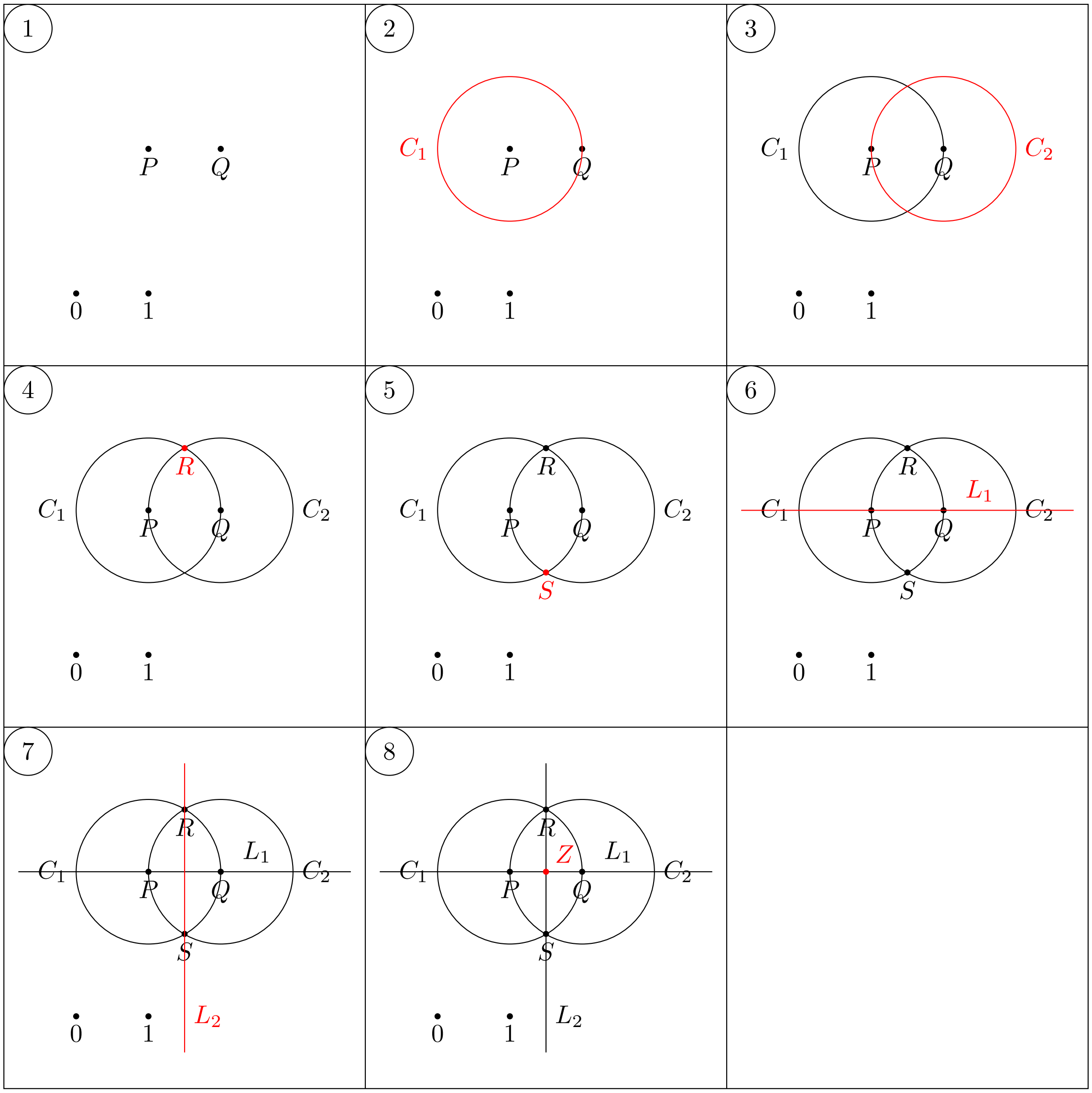

FIGURE 2.3.1. The midpoint of an interval

(4) Given distinct points P, Q construct a square with side PQ.
(5) Given distinct points P, Q construct a regular hexagon with side PQ.
(6) Given distinct points P, Q, and a point P', construct a point Q' such that the distances between P, Q and P', Q' are equal.
(7) Given lines L_1, L_2 meeting at P construct a line L_3 through P making equal angles with L_1, L_2.
(8) Given a circle C construct its centre.
(9) Given three distinct points P, Q, R construct a circle passing through all of them.

The Greeks solved these problems and many others. They failed to solve the following three:

PROBLEM 119. The classical impossibilities

(1) (Trisecting the angle) Given lines L_1, L_2 meeting at P, construct a line L_3 through P so that the angle between L_1, L_3 is one-third the angle between L_1 and L_2.
(2) (Duplicating the cube) Given a line segment PQ construct a line segment $P'Q'$ so that the cube with side $P'Q'$ has twice the volume of the cube with side PQ.

(3) (Squaring the circle) Given a circle construct a square with the same area.

For more than two thousand year mathematicians great and small tried to find constructions for these problems and failed. Eventually they were proved impossible in the 19th century. We will prove

THEOREM 120 (Wantzel 1837). (1) *It is impossible to construct two lines meeting at* 20° *(or to trisect angles except in special cases).*

(2) *It is impossible to duplicate the cube.*

We will not prove:

THEOREM 121 (Lindemann 1882). *It is impossible to square the circle.*

2.3.2. Formalization 1: the field of intervals. We concentrate on the *points* of the construction (every line and circle is determined by two points). In this equivalent view, a *figure* is a finite subset F of the plane, and there are three possible moves: one chooses four points $P, Q, R, S \in F$ with $P \neq Q$, $R \neq S$ and then adds to S either:

(1) The intersection points of the lines PQ, RS, if any; or
(2) The intersection point(s) of the line PQ and the circle with centre R through S, if any; or
(3) The intersection point(s) of the circles with centres P, R through Q, S respetively.

For example, in this view an angle is determined by three points: the vertex P and two points R, S so that the rays $\vec{PR}, \vec{PS}$ bound the angle. Together with Wantzel we will associate to every figure F a field.

For this recall that we fixed two distinct points $0, 1$ in the plane, and use this as a "unit of distance": the length of every other interval will be thought of as a multiple of the length of the fixed one. Normally ratios of lengths of intervals are thought to be real numbers, but as we shall see this is not necessary.

NOTATION 122. If I, J are line segments (bounded by points in S) we denote the pair by $I : J$.

DEFINITION 123. Say two intervals are *isometric* if they can be copied on each other (have the same length). Say two pairs are equivalent and write $I : J \sim I' : J'$ if for some (any) point P and some (any) distinct rays $\vec{\ell}_1, \vec{\ell}_2$ through P, if we copy I, I' on $\vec{\ell}_1$ starting at P (and ending at Q, Q' respectively) and J, J' on $\vec{\ell}_2$ (and ending at R, R' respectively) the lines QR and $Q'R'$ are parallel.

LEMMA 124. *For any three intervals* I, J, K *there is an interval* L*, unique up to isometry so that* $I : J \sim L : K$.

PROOF. Fix two rays $\vec{\ell}_1, \vec{\ell}_2$ (say at right angles) starting at a point P. Copy I on $\vec{\ell}_1$ ending at R and copy J, K and on $\vec{\ell}_2$ ending at Q, Q', respectively. The line QR is not parallel to $\vec{\ell}_1$ because it meets at the point R but not at the point Q. Then the line through Q' parallel to PQ is not parallel to $\vec{\ell}_1$ either and therefore meets at the point R'. We then take $L = [P, R']$ and this is unique since there is a unique line through Q' parallel to PQ. □

LEMMA-DEFINITION 125. *For intervals* I, J *define an interval* $I + J$ *by concatenating copies* I, J *along a line. This is unique up to isometry.*

For intervals I, J *define an interval* IJ *by* $IJ : J = I : 01$*. This exists and is unique by the previous Lemma.*

PROPOSITION 126. *Let* $\mathcal{F}_+$ *denote the set of isometry classes of lengths of intervals. Then* $\mathcal{F}_+$ *is a* semifield:

(1) *Addition is commutative, associative, and cancellative: if* $I + J, I + K$ *are isometric then* J, K *are isometric. For any non-isometric intervals* I, J *exactly one of the following holds: (a) there is* K *so that* $I + K = J$*; (b) there is* K *so that* $J + K = I$*. We write* $K = J - I$ *or* $I - J$ *respectively.*
(2) *Multiplication defines a group structure.*
(3) *Multiplication is associative over addition.*

OBSERVATION 127. *The* $I + J, IJ$ *and* $I - J$ *can be constructed with straightedge and compass.*

COROLLARY 128. *The set* $\mathcal{F} = \{\pm\} \times \mathcal{F}_+ \cup \{0\}$ *is a field of characteristic zero.*

NOTATION 129. Write $\mathbb{Q} \subset \mathcal{F}$ for the prime subfield, generated by the interval 01.

2.3.3. Formalization 2: the field of a configuration. Let F be a configuration, and recall that we have two fixed points $0, 1 \in F$. Pass a line X through $0, 1$ and a line Y through 0 perpendicular to X. For any point P in the plane let $x(P)$ denote the projection of P to the line X as well as the interval $[0, x(P)]$ on it, and similarly define $y(P)$. Note that $x(P), y(P)$ are constructible by straightedge and compass.

Definition 130. For a configuration F let $\mathbb{Q}(F) = \mathbb{Q}\left(\{x(P), y(P)\}_{P\in F}\right) \subset \mathcal{F}$.

For any $I \in \mathbb{Q}(F)$ let $R \in X$ be a point so that $0R$ is isometric to I. Then, by Observation 127, $F \cup \{R\}$ is constructible from F.

Passing from F to $\mathbb{Q}(F)$ amounts to automatically adding to F all the points whose coordinates lie in the field generated by the coordinates of the points in F.

Proposition 131. *Let $k \subset \mathcal{F}$ be a subfield, and let P, Q, R, S be four points with coordinates in k. Then*

1. *the intersection point of the lines PQ, RS has coordinates and k.*
2. *The intersection point of the line PQ with the circle determined by R, S has coordinates in a quadratic extension of k.*
3. *The intersection point of the circles determined by P, Q and R, S has coordinates in a quadratic extension of k.*

Proof. We compute in coordinates in each case

1. The line through P, Q has the equation $ax + by = c$ for some $a, b, c \in k$ with a, b not both zero. The same holds for the line through QR and the intersection can be computed explicitely.
2. It is easy to check that the circle has the form $(x-p)^2 + (y-q)^2 = r^2$ with $p, q, r \in k$ and the intersection with $ax + by = c$ is determined by a quadratic equation.
3. If we have another circle of the form $(x-s)^2 + (y-t)^2 = u^2$ then we can subtract the two equations to get $(s-p)x + (t-q)y = \frac{1}{2}\left(r^2 - u^2 + s^2 + t^2 - p^2 - q^2\right)$ and we are back in the previous case.

$\square$

Corollary 132. *Let $\{0, 1\} \subset F \subset F'$ be configurations of points so that F' is constructible from F. Then $k(F')$ is algebraic over $k(F)$, and for every $\alpha \in k(F')$ we have $[k(F') : k(F)(\alpha)] = 2^r$ for some r.*

Corollary 133. *Conversely, let $k(F) = k_0 \subset k_1 \subset \cdots \subset k_r$ be a sequence of quadratic extensions. Then there is a configuration $F' \supset F$ so that the extensions $k(F')/k(F)$ and $k_r/k(F)$ are isomorphic.*

2.3.4. Proof of the main Theorems. We begin with Theorem 120

Proof that trisecting the angle is impossible. Without loss of generality suppose $F = \{0, 1, P\}$ so that we need to trisect the angle between $0P$ and 01. Wlog we may assume the angle to be less than a right angle, and let H be the line through 1 perpendicular to the axis 01. Then the intersection point $H \cap 0P$ is constructible from F, so we may assume wlog that this is P,that that $x(P) = 1$. Let $Q \in H$ be the point so that the $\angle P01 = 3\angle Q01$. Let $I = 0P \in k(F)$, $J = 0Q$. The formula $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$ gives here:

$$\frac{1}{I} = \frac{4}{J^3} - \frac{3}{J}$$

that is

$$J^3 + 3IJ^2 - 4 = 0\,.$$

Suppose now that $J \notin k(F)$ (we'll give an example momentarily). Then $[k(F)(J) : k(F)] = 3$. It follows that the line $0Q$ cannot belong to any constructible F' extension of F, because if that was true then J would belong to a quadratic extension of $k(F')$ (by Pythagoras) and then we'd have that $[k(F)(J) : k(F)]$ be a power of 2, contradiction. For definiteness take $P = \left(1, \sqrt{3}\right)$ so that $I = 2$ (this is an angle of $60°$ which is constructible). The polynomial $t^3 + 6t^2 - 4$ has no roots in $\mathbb{Z}/8\mathbb{Z}$, hence in $\mathbb{Z}$, hence in $\mathbb{Q}$, because any root in $\mathbb{Z}/8\mathbb{Z}$ must have t^3 even ($6t^2 - 4$ is even) and then t^3 and $6t^2$ are divisible by 8 while 4 isn't. $\square$

Proof that duplicating the cube is impossible. Let $F = \{0, 1\}$. Again let $I = [0, 1]$ and suppose we can construct an interval J such that $J^3 = 2I = I + I$. Letting $x \in X$ be a point so that $0x$ is isometric to J, we see that there is a constructible configuration $F' \supset F$ so that $x \in F'$. But then $[\mathbb{Q}(x) : \mathbb{Q}] = 3$ contradicts the fact that $[\mathbb{Q}(x) : \mathbb{Q}]$ must be a power of 2. $\square$

Compared to this, Lindemann's Theorem is much deeper. Suppose we could construct a square with the same area as the unit disc. Then an interval of length $\sqrt{\pi}$ would be constructible, hence an interval of length π, and it would follow that π is algebraic. However Lindemann proved that π is transcendental over $\mathbb{Q}$.

CHAPTER 3

Monomorphisms, Automorphisms, and Galois Theory

3.1. Splitting fields and normal extensions

DEFINITION 134. Let $L : K$ be an extension of fields. Say $f \in K[x]$ *splits* in L if its image in $L[x]$ is a product of linear factors there. Say that L is a *splitting field* for f over K if f splits in L be not in any intermediate field $K \subset M \subsetneq L$.

THEOREM 135 (Splitting fields). (1) *For every field K and $f \in K[x]$ there exists a splitting field L/K, in fact one with*$[L : K] \leq (\deg(f))!$.

(2) *Splitting fields are unique up to isomorphism of extensions: if $\kappa\colon K \to K'$ is an isomorphism of fields, $f \in K[x]$, and $\iota\colon K \to L$, $\iota'\colon K' \to L'$ are splitting fields for f and $\kappa(f)$ respectively, then there exists an isomorphism $\lambda\colon L \to L'$ so that (κ, λ) is an isomorphism of the extensions ι and ι'.*

PROOF. First, if $f \in K[x]$ splits in L, say $f = c\prod_i(x - \alpha_i)$, then $M = K(\{\alpha_i\})$ is a splitting field: f splits there, and any sub-extension of M where f splits contains the $\{\alpha_i\}$ hence is equal to M. It is thus enough to construct an extension where f splits (with the given bound of the degree). We prove this by induction on the degree of f. If $\deg(f) \leq 1$ there's nothing to prove. Otherwise let g be an irreducible factor of f and let $M = K(\alpha)$ where α is a root of g. By induction $\frac{f}{x-\alpha} \in M[x]$ has a splitting field. It is clear that f splits there as well. The degree bound is an exercise.

We prove the second part by a similar induction. Let $g \in K[x]$ be an irreducible factor of f and let $\alpha \in L$ be a root of g, $\alpha' \in L'$ a root of $\kappa(g)$ which is also irreducible. Then $K(\alpha) : K$ and $K'(\alpha') : K'$ are isomorphic extensions, say by (κ, κ'). Next, $L : K(\alpha)$ and $L' : K'(\alpha')$ are splitting fields for $\frac{f}{x-\alpha}$ and $\kappa'\left(\frac{f}{x-\alpha}\right) = \frac{\kappa(f)}{x-\alpha'}$ respectively so by induction there is $\lambda\colon L \to L'$ so that (κ', λ) is an isomorphism of the extensions. It follows that (κ, λ) is an isomorphism of extensions. □

EXAMPLE 136. Let $f(x) = x^6 + 5x^3 + 1 \in \mathbb{Q}[x]$. Let β be a root of f and let ω be a cube root of unity. Then $\left\{\beta^{\pm 1}\omega^a \mid a \mod 3\right\}$ are six roots of f and are disjoint, so they are all the roots. It follows that $\Sigma = \mathbb{Q}(\beta, \omega)$ is a splitting field. To find its degree let $\alpha = \frac{-5\pm\sqrt{21}}{2}$ be a root of $y^2 + 5y + 1 = 0$ and let

$$F = \mathbb{Q}(\alpha, \omega) = \mathbb{Q}(\sqrt{21}, \sqrt{-3})$$

so that $[F : \mathbb{Q}] = 4$. Then wlog β satisfies $\beta^3 = \alpha$, that is a root of $x^3 - \alpha \in F[x]$.

Suppose this polynomial had a root there, that is there are $A, B \in \mathbb{Q}(\omega)$ so that $(A + B\alpha)^3 = \alpha$. Thus $B^3\alpha^3 + 3B^2A\alpha^2 + (3BA^2 - 1)\alpha + A^3 = 0$, or in other words α is a root of $g(y) = B^3y^3 + 3B^2Ay^2 + (3BA^2 - 1)y + A^3 \in \mathbb{Q}(\omega)[y]$. On the other hand since $\alpha \notin \mathbb{Q}[\omega]$ its minimal polynomial that field is still $y^2 + 5y + 1$. It follows that $y^2 + 5y + 1 \mid g$ in $\mathbb{Q}(\omega)[x]$. Considering leading and constant cofficients this means

$$B^3y^3 + 3B^2Ay^2 + (3BA^2 - 1)y + A^3 = \left(B^3y + A^3\right)\left(y^2 + 5y + 1\right) .$$

Examining the coefficients of y^2 and y we obtaint the equations

$$3B^2A = A^3 + 5B^3$$
$$(3BA^2 - 1) = 5A^3 .$$

In the first equation, $B \neq 0$ since otherwise we'd have $\alpha = A^3 \in \mathbb{Q}(\omega)$. Dividing by B^3 we see that $\frac{A}{B} \in \mathbb{Q}(\omega)$ is a root of

$$z^3 - 3z + 5 = 0 .$$

But this polynomial is irreducible over $\mathbb{Q}$ (check that $\pm 1, \pm 5$ aren't roots), and a quadratic field can't contain a cubic subfield. We conclude that $x^3 - \alpha$ is irreducible in $F[x]$, so that $\Sigma = F(\beta)$ has degree 3 over F and degree 12 over $\mathbb{Q}$.

Definition 137. Call $L : K$ *normal* if every irreducible $f \in K[x]$ which has a root in L splits in L.

Proposition 138. *If $L : K$ is normal and M is an intermediate field then $L : M$ is normal.*

Proof. (Exercise). $\square$

Theorem 139. *L/K is normal and finite iff it is a splitting field.*

Proof. If L/K is finite it is finitely generated, say $L = K(\alpha_1, \ldots, \alpha_r)$. Let $g_i \in K[x]$ be the minimal polynomial of α_i. Then $f = \prod_i g_i$ splits in L (each g_i does by normality), while every subfield of L where f splits contains all the α_i and hence is L. For the converse let $L : K$ be the splitting field of $f \in K[x]$ and let $\alpha \in L$ have minimal polynomial g. In the splitting field M of fg (which contains a unique copy of L) let α' be another root of g. Then $K(\alpha) : K$ and $K(\alpha') : K$ are isomorphic extensions, hence of the same degree. Next, $L(\alpha) : K(\alpha)$ and $L(\alpha') : K(\alpha')$ are splitting fields for the same polynomial f (the isomorphism of $K(\alpha)$ and $K'(\alpha)$ fixes K). Thus they are isomorphic extensions and also have the same degree. It follows that $[L(\alpha) : K] = [L(\alpha') : K]$. Dividing by $[L : K]$ shows $[L(\alpha') : L] = [L(\alpha) : L] = 1$ so $\alpha' \in L$ as well so $M = L$ and g splits in L. $\square$

Definition 140. A *normal closure* of an extension of fields $L : K$ is an extension $N : L$ so that $N : K$ is normal while every proper intermediate extension of $N : L$ is not.

Proposition 141. *Every finite extension has a normal closure, unique up to isomorphism of extensions.*

Proof. Let $L : K$ be a finite extension. Then L is finitely generated, say $L = K(\alpha_1, \ldots, \alpha_r)$. Let $g_i \in K[x]$ be a minimal polynomial of α_i and let $g = \prod_i g_i$. Then N is a normal closure iff it is a splitting field for g. $\square$

Remark 142. The proposition holds for infinite algebraic extensions as well; see the section on infinite Galois theory.

Example 143. Every quadratic extension is normal.

3.2. Separability

Definition 144. Let $L : K$ be an extension. Call $f \in K[x]$ *separable* if every irreducible factor of f has distinct roots in the splitting field. Call $\alpha \in L$ *separable over* K if its minimal polynomial in $K[x]$ is separable. Call $L : K$ *separable* if every $\alpha \in L$ is separable over K, *purely inseparable* if every $\alpha \in L$ separable over K belongs to K.

Exercise 145 (PS6). A polynomial $f \in K[x]$ is separable iff it is relatively prime to its formal derivative. An irreducible polynomial is separable unless its formal derivative is zero.

Proposition 146. *If $L : K$ is separable and M is an intermediate field then $L : M$ and $M : K$ are separable.*

Proof. (Exercise). $\square$

Proposition 147 (Construction of monomorphisms). *Let $L : K$ be finite. Then there are at most $[L : K]$ K-monomorphisms of L into a normal closure N/K. If L is generated over K by separable elements then the number of monomorphisms is precisely $[L : K]$, and conversely if the number if $[L : K]$ then the extension is separable.*

Proof. Induction on the degree. Assuming that $n = [L : K] > 1$ choose $\alpha \in L \setminus K$. Let $f \in K[x]$ be the minimal polynomial of α with roots $\{\alpha_i\}_{i=1}^{e}$ be the roots of f in N (including $\alpha_1 = \alpha$), and note that $e \leq d = \deg(f)$. Then $K(\alpha)$ has precisely e embeddings into N. By induction L has at most $\frac{n}{d} = [L : K(\alpha)]$ $K(\alpha)$-embeddings into N with α mapping to α_i. Since every embedding maps α to one of the α_i it follows that the total number of embedding is at most $e \cdot \frac{n}{d} \leq d \cdot \frac{n}{d} = n$. If we can choose $\alpha \in L$ which is not separable then we'd have $e < d$ and so the number of embedding would be strictly less than n. If L/K is generated by separable elements then we take α to be one of them so $e = d$; since $L/K(\alpha)$ is also generated by separable elements it has precisely $\frac{n}{d}$ embeddings and we are done. □

We obtain several corollaries:

THEOREM 148 (Separability). *A finite extension L/K is separable iff it is generated by separable elements. Thus:*

(1) *An extension generated by separable elements is separable.*
(2) *Let $K \hookrightarrow L \hookrightarrow M$ with L/K separable and let $\alpha \in M$ be separable over L. Then α is separable over K. In particular, M/K is separable iff M/L and L/K are.*
(3) *If M/K is an extension then the subset $L \subset M$ of elements which are separably algebraic over K is a subfield, the separable closure of K in M. If M/K is algebraic the extension M/L is purely inseparable.*

PROOF. The initial claim is immediate.

(1) let $L = K(S)$ with $S \subset L$ separably algebraic over K. For each $\alpha \in L$ there is a finite subset $T \subset S$ so that $\alpha \in K(T)$ and we may apply the Proposition to the extension $K(T) : K$.
(2) Let $f \in L[x]$ be the minimal polynomial of α and let $R = K(f)$ be the subfield generated by its coefficients. Let N/K be a normal closure of M/K. Then R has $[R : K]$ embeddings into N and each can be extended in $[R(\alpha) : R] = \deg(f)$ ways to embeddings of $R(\alpha)$. It follows that $R(\alpha)$ has $[R(\alpha) : K]$ K-embeddings into N so $R(\alpha)$ is separable and so is α.
(3) The field extension generated by the separable elements is separable, hence is equal to that set. Any element of the extension separable over the separable closure is separable over the base field.

□

EXAMPLE 149. Let $\mathrm{char}(K_0) = p$ and let $K = K_0(t)$ be the function field in one variable over K_0. Then $x^p - t \in K[x]$ is irreducible and inseparable. Indeed if L/K is a field and $s \in L$ is a root then $(x - s)^p = x^p - s^p = x^p - t$ so s is the unique root of $x^p - t$ in L. Also, any monic divisor of $x^p - t$ in $L[x]$ has the form $(x - s)^r$ for some $0 \le r \le p$. If $1 \le r < p$ then the constant coefficient of this divisor is $s^{r/p} \notin K$ (this elements generates $K(s)$ as well) so the divisor is not in $K[x]$. One can also see that $x^p - t$ is irreducible using Eisenstein's criterion in $K_0[t][x]$.

3.3. Automorphism Groups

DEFINITION 150. Let L be a field. $\mathrm{Aut}(L)$ will be the group of automorphisms of L. If $L : K$ is an extension of fields we write $\mathrm{Aut}_K(L)$ for the group of automorphisms fixing K element-wise.

EXAMPLE 151. Quadratic extensions in characteristic different from 2, $\mathbb{Q}(\sqrt[3]{2})$ and its normal closure, the inseparable extension.

LEMMA 152 (Dedekind). *Let K, L be fields. Then $\mathrm{Hom}(K, L)$ is linearly independent over L (as a subset of L^K).*

PROOF. Let $0 = \sum_{i=1}^{r} a_i f_i$ be a minimal linear combination. Then the f_i distinct and all the a_i are non-zero. We have $r \ge 2$ since $0 \notin \mathrm{Hom}(K, L)$. Let $y \in K$ be such that $f_1(y) \ne f_r(y)$ (then $y \ne 0$ as are $f_1(y)$, $f_r(y)$), and see that for all $x \in K$ we have:

$$\begin{aligned}
\sum_{i=1}^{r-1} \left(a_i \left(f_i(y) - a_i f_n(y)\right)\right) f_i(x) &= \sum_{i=1}^{r} a_i f_i(y) f_i(x) - f_n(y) \sum_{i=1}^{r} a_i f_i(x) \\
& \left(\sum_{i=1}^{r} a_i f_i\right)(yx) - f_n(y) \left(\sum_{i=1}^{r} a_i f_i\right)(x) \\
&= 0\,.
\end{aligned}$$

□

Remark 153. In fact, we have shown that if H is a group then $\mathrm{Hom}(H, L^\times)$ is linearly independent (take $H = K^\times$).

Corollary 154. *Let $[L : K] = n$. Then $\# \mathrm{Aut}_K(L) \leq n^2$.*

Proof. $\mathrm{Aut}(L) = \mathrm{Hom}(L, L)$ is a linearly independent subset of L^L, thought of as an L-vectorspace, hence also as a K-vectorspace. Now $\mathrm{Aut}_K(L)$ lies in the K-subspace of K-linear maps $L \to L$ which has dimension n^2. □

Proposition 155. *Let $[L : K] = n$. Then $\# \mathrm{Aut}_K(L) \leq n$.*

Proof. Let $\{\omega_i\}_{i=1}^n$ be a basis for L over K. Each $\sigma \in \mathrm{Aut}_K(L)$ is determined by the vector $(\sigma(\omega_i))_{i=1}^n \in L^n$, and these vectors are linearly independent over L: if $a_\sigma \in L$ are such that $\sum_\sigma a_\sigma \sigma(\omega_i) = 0$ for each i, then $\sum_\sigma a_\sigma \sigma$ is a K-linear map $L \to L$ which vanishes on a basis, hence vanishes identically, which forces all the a_σ to vanish by the Lemma. Since $\dim_L L^n = n$ we are done. □

Definition 156. For $\sigma \in \mathrm{Aut}(L)$ write $\mathrm{Fix}(\sigma) = \{x \in L \mid \sigma(x) = x\}$, a subfield of L. For $S \subset \mathrm{Aut}(L)$ write $\mathrm{Fix}(S) = \cap_{\sigma \in S} \mathrm{Fix}(\sigma)$. Note that $\mathrm{Fix}(S) = \mathrm{Fix}(\langle S \rangle)$.

Proposition 157. *Let L be a field, $G \subset \mathrm{Aut}(L)$ a finite subgroup of order n, and let $K = \mathrm{Fix}(G)$. Then $[L : K] = n$.*

Proof. To each $\omega \in L$ associate the vector $\omega^G = (\sigma(\omega))_{\sigma \in G} \in L^G$. Let $\Omega \subset L$ be a basis over K and let $\sum_{i=1}^r a_i \omega_i^G = 0$ be a minimal linear dependence in L^G over L. Then for each $\sigma \in G$ we have $\sum_i a_i \sigma(\omega_i) = 0$ with $a_i \in L^\times$. For $\tau \in G$ note that we have $\sum_i \tau(a_i)(\tau\sigma)(\omega_i) = 0$ for all σ, so $\sum_i \tau(a_i)\omega_i^G = 0$ as well. Since minimal combinations are unique up to scalar, there is $b \in L^\times$so that $\tau(a_i) = ba_i$ for all i. Then $\tau\left(a_1^{-1}a_i\right) = a_1^{-1}a_i$ for all i. Since τ was arbitrary it follows that there are $c_i \in K^\times$ so that $a_i = a_1 c_i$. Dividing by a_1 it follows that $\sum_{i=1}^r c_i \omega_i^G = 0$. In particular the co-ordinate of the identity gives $\sum_{i=1}^r c_i \omega_i = 0$, which is impossible. It follows that $\left\{\omega^G\right\}_{\omega \in \Omega} \subset L^G$ are linearly independent over L, and hence that $|\Omega| \leq |G|$, that is $[L : K] \leq |G|$. In particular ,$[L : K]$ is finite, and we then have $|G| \leq [L : K]$ as well. □

Example 158. Fix a field F and let S_n act on the function field $L = F(x_1, \ldots, x_n)$ by permuting the variables. The fixed field $K = F(x_1, \ldots, x_n)^{S_n}$ is called the *field of symmetric rational functions*. It is the fracting field of the *ring of symmetric polynomials*, further investigated in PS6. By the Proposition this is an extension of degree $n!$ whose automorhpism group is exactly S_n.

Corollary 159. *Let G be a finite group. Then there is a normal separable extension L/K with automorphism group G.*

Proof. Cayley's theorem provides an embedding into some S_n, and then we can take $F(x_1, \ldots, x_n) : F(x_1, \ldots, x_n)^G$. □

3.4. The group action

If L/K is an extension of fields, then $\mathrm{Aut}_K(L)$ acts on L, and we now investigate the orbits of this action. The key observation is that if L, M are extensions of K, $\sigma \in \mathrm{Hom}_K(L, M)$, $f \in K[x]$, and $\alpha \in L$ then $\sigma(f(\alpha)) = f(\sigma(\alpha))$. In particular, α is root of f iff $\sigma(\alpha)$ is. It follows that if $\alpha \in L$ is algebraic over K then its $\mathrm{Aut}_K(L)$-orbit is contained in the set of roots of its minimal polynomial.

Observation 160 (Meaning of normality). *Let L/K be an algebraic extension, let N/K be a normal extension and let M/N be a further extension. Assume we have a K-monomorphism $\sigma\colon L \to N$. Then every K-monomorphism $\tau \in \mathrm{Hom}_K(L, M)$ has its image in N.*

Proof. For every $\alpha \in L$, $\tau(\alpha) \in M$ is a root of the minimal polynomial of α. This polynomial already has the root $\sigma(\alpha) \in N$ and (N being normal) splits there, so that $\tau(\alpha) \in N$. □

Lemma 161. *Let $f \in K[x]$ be irreducible and let N/K be a finite normal extension. If f splits in N then $\mathrm{Aut}_K(N)$ acts transitively on the roots of f.*

PROOF. Let α, β be roots of f in N. By Theorem 139 there exist $g \in K[x]$ be such that N is the splitting field of g over K, hence also over $K(\alpha)$ and $K(\beta)$. By Theorem 135 the K-isomorphism of $K(\alpha)$ and $K(\beta)$ carrying α to β extends to an isomorphism of N to itself. $\square$

We can generalize this:

PROPOSITION 162 (Construction of monomorphisms). *Let L/K be a finite algebraic extension, let N/K be a finite normal extension and let $\sigma, \tau \in \mathrm{Hom}_K(L, N)$. Then there exists $\rho \in \mathrm{Aut}_K(N)$ so that $\tau = \rho\sigma$.*

PROOF. Again let $g \in K[x]$ be such that N is the splitting field of g. Then $\sigma, \tau \colon L \to N$ are both splitting fields for g, and are therefore isomorphic. $\square$

In short, we have seen that $\mathrm{Aut}_K(N)$ acts transitively on $\mathrm{Hom}_K(L, N)$.

THEOREM 163. *Let L/K be an algebraic extension, let N/K be a normal algebraic extension, and let $\sigma, \tau \in \mathrm{Hom}_K(L, N)$. Then there exists $\rho \in \mathrm{Aut}_K(N)$ so that $\tau = \rho\sigma$.*

PROOF. Identifying L with $\sigma(L)$ and replacing τ with $\tau \circ \sigma^{-1}$ we may assume $\sigma = \mathrm{id}$. Consider the set of functions μ whose domain is a subfield of N containing L, whose range is contained in N, and which are field monomorphisms extending τ, ordered by inclusion. Let ρ be a maximal element of the set (this exists by Zorn's Lemma). If the domain of ρ is a proper subfield M of N let $\alpha \in N \setminus M$. Let g be the minimal polynomial of α over M. Then g is irreducible in M, and hence $\rho(g)$ is irreducible in $\rho(M)$. Both $g, \rho(g)$ divide the minimal polynomial h of α over K which splits in N by normality. It follows that $\rho(g)$ has a root $\beta \in N \setminus \rho(M)$ ($\rho(g)$ is irreducible!). Now extending ρ to an isomorphism $M(\alpha) \to \rho(M)(\beta)$ contradicts the maximality of ρ, and we conclude that ρ is defined on all of N. Showing that ρ is surjective is left as an exercise. $\square$

3.5. Galois groups and the Galois correspondence

DEFINITION 164. If L/K is normal and separable we say that it is a *Galois extension,* call $\mathrm{Aut}_K(L)$ the *Galois group,* and denote it $\mathrm{Gal}(L : K)$.

THEOREM 165. *Let $[L : K] = n$. Then the following are equivalent:*

(1) *L/K is a Galois extension.*
(2) *$\mathrm{Aut}_K(L)$ has order n.*
(3) *The fixed field of $\mathrm{Aut}_K(L)$ is precisely K.*

PROOF. By Proposition 147 if L/K is normal and separable there are $n = [L : K]$ K-embeddings $L \to L$, which are surjective as injective endomorhpisms of a finite-dimensional vector space. Next, let $F = \mathrm{Fix}\,(\mathrm{Aut}_K(L))$, a subfield of L containing K. By Proposition 157 $[L : F] = \#\,\mathrm{Aut}_K(L)$, and since $[F : K] = \frac{[L:F]}{[L:K]} = \frac{\#\,\mathrm{Aut}_K(L)}{n}$ we see that $F = K$ iff $\#\,\mathrm{Aut}_K(L) = n$. That (3) $\Rightarrow$ (1) is left as an exercise. $\square$

THEOREM 166 (Galois Correspondence). *Let $L : K$ be a finite Galois extension. Then the inclusion-reversing maps $H \mapsto \mathrm{Fix}(H)$, $M \mapsto \mathrm{Gal}(L : M)$ between subgroups $H < \mathrm{Gal}(L : K)$ and intermediate fields $K \subset M \subset L$ are inverse to each other. Further:*

(1) *$M : K$ is normal iff $\mathrm{Gal}(L : M)$ is normal in $\mathrm{Gal}(L : K)$.*
(2) *If $M : K$ is normal then $\mathrm{Gal}(M : K) \simeq \mathrm{Gal}(L : K)/\,\mathrm{Gal}(L : M)$.*

PROOF. Clearly if $M \subset M' \subset L$ then $\mathrm{Aut}_{M'}(L) \subset \mathrm{Aut}_M(L)$: every M'-automorphism of L is an M-automorphism. Similarly, if $H \subset H'$ then every $\alpha \in L$ fixed by H' is fixed by H. Also, for any intermediate field M, $L : M$ is normal and separable hence Galois. Now for $H < \mathrm{Gal}(L : K)$ we have $H \subset \mathrm{Gal}(L : \mathrm{Fix}(H))$. By Proposition 157 $[L : \mathrm{Fix}(H)] = \#H$ and by the previous Theorem $[L : \mathrm{Fix}(H)] = \#\,\mathrm{Gal}(L : \mathrm{Fix}(H))$. It follows that $H = \mathrm{Gal}(L : \mathrm{Fix}(H))$. Similarly for an intermediate field M, the index of $\mathrm{Fix}(\mathrm{Gal}(L : M))$ in L is the same as the index of M. Since the two are contained in each other they are equal.

Finally, let $\sigma \in \mathrm{Gal}(L : K)$ and let $H < \mathrm{Gal}(L : K)$. Then the fixed field of $\sigma H \sigma^{-1}$ is exactly $\sigma\,\mathrm{Fix}(H)$. If $\mathrm{Fix}(H)$ is normal than any K-automorphism of L must leave $\mathrm{Fix}(H)$ invariant since it maps roots of polynomials to roots of polynomials, so $\sigma H \sigma^{-1}$ has the same fixed field as H and hence is equal. Conversely, if H is normal then $\mathrm{Fix}(H)$ is an invariant set for the action of $\mathrm{Gal}(L : K)$; since the orbits of the action are precisely the sets of roots of irreducible polynomials, it follows that $M = \mathrm{Fix}(H)$ is normal over K. Restricting the action of the Galois group to M we obtain a map $\mathrm{Gal}(L : K) \to \mathrm{Gal}(M : K)$. By definition, the kernel of this map is $\mathrm{Gal}(L : M)$. It is surjective since by Proposition 162 every K-automorphism of M extends to a K-automorphism of L. $\square$

Proposition 167. *Let L/K Galois extension, and let $\alpha \in L$. Let $O \subset L$ be the orbit of α under* $\mathrm{Gal}(L : K)$. *Then $f = \prod_{\beta \in O}(x - \beta)$ is the minimal polynomial of α over K.*

Proof. We have seen that O is finite in and we may then take L finite. From now on we only assume that $G = \mathrm{Aut}_K(L)$ has order $n = [K : L]$, this giving an alternative proof of the converse part of Theorem 165. First, for $\sigma \in G$ we have $\sigma(f) = \prod_{\beta \in O}(x - \sigma(\beta)) = f$ so f belongs to the fixed field of G, that is K. Note that f has distinct roots by construction, so α is separable. f is also irreducible, since a product of the form $\prod_{\beta \in S}(x - \beta)$ is G-fixed if an only if S is G-invariant set, and it follows that every irreducible in $K[x]$ which has a root in L splits in L, so L is normal. $\square$

Corollary 168. *Let $f \in K[x]$ be irreducible and have a root in L. Then* $\mathrm{Gal}(L : K)$ *acts transitively on the roots of f.*

3.6. Examples and applications

3.6.1. The primitive element Theorem.

Theorem 169. *Let L/K be a finite, separable extension. Then $L = K(\theta)$ for some $\theta \in K$.*

Proof. Assume first that K is infinite, and let N/K be a normal closure of L/K. Then N/K is finite by Proposition 141 and separable since the Proposition shows it is generated by separable elements. Since $\mathrm{Gal}(N/K)$ is finite it has finitely many subgroups, and by the Galois correspondence it follows that there are finitely many intermediate fields between N and K, hence also between L and K and the claim follows from the results of Problem Set 5. When K is finite so is L and the claim was also proved in that problem set. $\square$

3.6.2. Symmetric combination and Galois's outlook. Let $f \in K[x]$ split in $L[x]$ with roots $\{\alpha_1, \ldots, \alpha_r\}$ (counted with multiplicity). Let $s \in K[\underline{y}]^{S_r}$.

Lemma 170. *$s(\underline{\alpha}) \in K$.*

Proof. By the Newton identities (PS6), we can write s as a polynomial in the elementary symmetric polynomials, and those are exactly the coefficients of $f = a_r \prod_{i=1}^{r}(x - \alpha_i)$. $\square$

Observation 171. *This argument did not use separability!*

Example 172. The *discriminant* of f is the expression $D(f) = \prod_{i<j}(\alpha_i - \alpha_j)^2$.

Exercise 173. The discriminat can be computed directly in some cases.

3.6.3. Cyclotomic fields. See Problem Set 7.

3.6.4. The polynomial $t^4 - 2$. The splitting field is $\Sigma = \mathbb{Q}(i, \sqrt[4]{2})$, so the Galois group $G = \mathrm{Gal}(\Sigma/\mathbb{Q})$ has order 8. Let $K = \mathbb{Q}(i)$. Since $\Sigma = K(\sqrt[4]{2})$ we see that $t^4 - 2$ is still irreducible there. Now any $\sigma \in H = \mathrm{Gal}(\Sigma : K)$ must have $\sigma(\sqrt[4]{2}) = \sqrt[4]{2} \cdot i^{j(\sigma)}$ and this map $j \colon H \to \mathbb{Z}/4\mathbb{Z}$ is a surjective group homomorphism, hence an isomorphism and H. Next, let $\tau \in \mathrm{Gal}(\Sigma : \mathbb{Q}(\sqrt[4]{2}))$ be the nontrivial element. Since H is normal in G (it has index 2) we have $G = H \rtimes \langle\tau\rangle$ and it remains to determine the action. For $\sigma \in H$ we have

$$(\tau\sigma\tau)\left(\sqrt[4]{2}\right) = (\tau\sigma)\left(\sqrt[4]{2}\right) = \tau\left(i^{j(\sigma)}\sqrt[4]{2}\right) = i^{-j(\sigma)}\sqrt[4]{2} = \sigma^{-1}\left(\sqrt[4]{2}\right).$$

It follows that $\tau\sigma\tau^{-1} = \sigma^{-1}$, or in other words that $G \simeq D_8$.

3.7. Solubility by radicals

In this section all fields have characteristic zero.

Definition 174. $f \in K[x]$ separable. Then $\mathrm{Gal}(f) \stackrel{\mathrm{def}}{=} \mathrm{Gal}(\Sigma(f) : K)$ where $\Sigma(f)$ is the splitting field.

Call L/K radical *if* $L = K(\alpha_1, \ldots, \alpha_s)$ *and for each* i *there is* r_i *so that* $\alpha_i^{r_i} \in K(\alpha_1, \ldots, \alpha_{i-1})$. *Call* $f \in K[x]$ soluble by radicals *if there exists a radical extension containing* $\Sigma(f)$. *If* f *is irreducible enough to show* $K[x]/(f)$ *is contained in a radical extension.*

Theorem 175. $f \in K[x]$ *is soluble by radicals iff* $\mathrm{Gal}(f)$ *is a solvable group.*

3.7.1. Radical extensions are solvable.

Lemma 176. L/K *contained in a radical then normal closure* N/K *contained in a radical.*

Proof. Enough to show that the normal closure of a radical extension is radical. Indeed, let $L = K(\alpha_1, \ldots, \alpha_s)$ be radical, let N be the normal closure, $G = \mathrm{Gal}(N : K)$. Then $N = K\left(\{\sigma(\alpha_i) \mid \sigma \in G, 1 \leq i \leq s\}\right)$. Ordering this lexicographically with i most significant than σ exhibits this as a radical extension.

In the alternative let $r = \mathrm{lcm}\{r_1, \ldots, r_s\}$ and let $N = L(\mu_r)$. Then N is normal (contains all conjugates of the α_i) and radical. □

Lemma 177. $\mathrm{Gal}(\Sigma(t^p - 1) : K)$ *is Abelian.*

Proof. Automorphisms raise generator to a power. □

Lemma 178. *If* $\mu_n \subset K$ *then* $\Sigma(t^n - a) : K$ *is abelian.*

Proof. Galois group maps the root α to the root $\zeta\alpha$ where ζ is a root of unity. □

Proposition 179. L/K *normal and radical implies* $\mathrm{Gal}(L : K)$ *solvable.*

Proof. Induction on number of roots. Can assume r_i are all prime. Say $\alpha^p \in K$ but $\alpha \notin K$. Let $M \subset L$ be splitting field for $t^p - 1$. Then $M : K$, $M(\alpha) : M$ are normal and abelian. $L : M(\alpha)$ solvable by induction. □

Theorem 180. L/K *contained in radical extension. Then* $\mathrm{Aut}_K(L)$ *is solvable.*

Proof. $K \subset L \subset R \subset N$ where R/K is radical, N/K its normal closure. Then N/K is radical so $\mathrm{Gal}(N/K)$ is solvable. Let $H = \{\sigma \in \mathrm{Gal}(N/K) \mid \sigma(L) \subset L\}$; restriction gives a map $H \to \mathrm{Aut}_K(L)$ with kernel $\mathrm{Gal}(N : L)$. This map is surjective since every K-automorphism of L is extends to an automorphism of N since N is a splitting field of some $f \in K[x]$. Now H is solvable as a subgroup of a solvable group, and $\mathrm{Aut}_K(L)$ is solvable as a quotient of a solvable group. □

3.7.2. Insoluble polynomials.

Proposition 181. *Let* p *be prime,* $f \in \mathbb{Q}[x]$ *irreducible of degree* p *with precisely two complex roots. Then* $\mathrm{Gal}(f) \simeq S_p$.

Proof. Let $A \subset \mathbb{C}$ be the roots of f, $\Sigma = \mathbb{Q}(A)$ the splitting field, $G = \mathrm{Gal}(\Sigma : \mathbb{Q})$. Then G acts transitively on a set of size p, giving an embedding $G \hookrightarrow S_p$. If $\alpha \in A$ is any root then $[\mathbb{Q}(\alpha) : \mathbb{Q})] = p$ so $p | [\Sigma : \mathbb{Q}] = \#G$ so the image of the map contains an element of order p, which is hence a p-cycle $\sigma \in S_p$. Let $\tau \in G$ be the restriction of complex conjugation to Σ. Then τ is a 2-cycle, say $\tau = (1\,2)$. Any non-identity power of σ is also a p-cycle, and by transitivity there is one of the form $(1\,2\,\ldots\,p)$. These two together generated S_p. □

Example 182. $t^5 - 6t + 3 \in \mathbb{Q}[x]$ is irreducible by Eisenstein. Its derivative is $5t^4 - 6$ which is positive if $|t| > \left(\frac{6}{5}\right)^{1/4} = u > 1$ and negative in $|t| < \left(\frac{6}{5}\right)^{1/4}$. Since $f(-u) = -\frac{6}{5}u + 6u + 3 > 0$ and $f(u) = \frac{6}{5}u - 6u + 3 = 3 - 4.8u < 0$, it follows that f has three real roots (one in $(-\infty, -u)$, one in $(-u, u)$ and one in (u, ∞)).

3.7.3. Solvable extensions are radical.

Definition 183. Let L/K be a finite extension and let $\alpha \in L$. If L/K is Galois set $\mathrm{Tr}_K^L(\alpha) = \sum_{\sigma\in\mathrm{Gal}(L/K)} \sigma\alpha$, $N_K^L(\alpha) = \prod_{\sigma\in\mathrm{Gal}(L/K)} \sigma\alpha$. In general let $\mathrm{Tr}_K^L(\alpha)$ and $N_K^L(\alpha)$ be, respectively, the trace and determinant of multiplication by α, thought of as a K-linear map $L \to L$.

Exercise 184. (PS10 problem 3) The two definitions coincide when they intersect.

(PS10 problem 2) Let $1 < [L : K] < \infty$ be prime to $\mathrm{char}(K)$. Then $L = L_0 \oplus K$ as K-vector spaces. In particular, there exist $\alpha \in L \setminus K$ with trace zero.

The key step in our induction will be the following:

Proposition 185. *Let L/K be a Galois extension of prime index p, and assume $\mu_p \subset K$. Then L is radical over K.*

Proof. Let σ generate $G = \mathrm{Gal}(L/K)$ (a group of order p hence cyclic). For $\alpha \in L$ and $\zeta \in \mu_p$ consider the *Lagrange Resolvent*

$$\Theta(\alpha, \zeta) = \sum_{b(p)} \zeta^b \sigma^b(\alpha)\,.$$

Then:

$$\sigma\left(\Theta(\alpha, \zeta)\right) \quad = \quad \zeta^{-1}\Theta(\alpha, \zeta)\,.$$

If $\Theta \neq 0$ and $\zeta \neq 1$ this would show $\Theta(\alpha, \zeta) \notin K$ but $(\Theta(\alpha, \zeta))^p \in K$, finishing the proof. For α fixed let $\Theta(\alpha)$ be the vector $\left(\Theta(\alpha, \zeta_p^a)\right)_{a\in\mathbb{Z}/p\mathbb{Z}} = Z \cdot \alpha^G$ where $Z \in M_n(K)$ is the Vandermonde matrix $Z_{ab} = \zeta_p^{ab}$ and $\alpha^G = \left(\sigma^b(\alpha)\right)_b$. Note that $(Z\alpha)_0 = \mathrm{Tr}\,\alpha$ and choose $\alpha \in L \setminus K$ so that $\mathrm{Tr}(\alpha) \neq 0$. Then $\alpha^G \neq 0$ so $Z\alpha^G \neq 0$ and it follows that there is $a \neq 0$ so that $(Z\alpha)_a \neq 0$. □

Proposition 186. *("Base change") Let $T : K$ be an extension of fields, and let $L, M \subset T$ be intermediate extensions with L/K is a finite Galois extension. Let $LM \subset T$ be the field generated by L, M. Then $LM : M$ is a finite Galois extension, and restriction to L is an injective map $\mathrm{Gal}(LM : M) \to \mathrm{Gal}(L : K)$ (in particular, $[LM : M] \leq [L : K]$). Moreover, if L/K is cyclic, abelian or solvable then so is LM/M.*

Proof. Assume that L is the splitting field of the separable polynomial $f \in K[x]$. Then LM is the splitting field of f over M. It follows that $LM : M$ is a finite Galois extension. Since L is normal every $\sigma \in \mathrm{Aut}_K(LM)$ maps L to L, so restriction to L gives a map $\mathrm{Aut}_M(LM) \to \mathrm{Aut}_K(L)$. If σ belongs to the kernel of this map then $\sigma \in \mathrm{Aut}(LM)$ fixes M (assumption on the domain) and L (assumption on the image). It follows that σ is trivial. □

Theorem 187. *Let L/K be a finite solvable Galois extension. Then there exists a radical extension M of K containing L.*

Proof. Let $[L : K] = n$. We will show that $L(\mu_{n!}) : K$ is radical. It is clearly enough to show that $L(\mu_{n!}) : K(\mu_{n!})$ is radical, and by the base change proposition this is a solvable extension of degree at most n. We now prove by induction on N that if L/K is solvable, and K contains $\mu_{n!}$ then L/K is radical. For this let $G = \mathrm{Gal}(L/K)$, and let $H < G$ be normal of prime index p. Let $M = \mathrm{Fix}(H)$.Then $M : K$ is Galois, with Galois group $G/H \simeq C_p$. Since $p \leq n$, we may apply the first Proposition to see that M/K is radical. Also, $L : M$ is solvable and $[L : M]! \mid [L : K]!$ so M contains all the requisite roots of unity to apply the induction hypothesis. □

CHAPTER 4

Topics

4.1. Transcendental extensions

4.1.1. Review of linear algebra. Let K be a field, L a K-vectorspace. Recall the following:

(1) $E \subset L$ is *linearly dependent* over K if there are $n \geq 1$, a homogenous degree 1 polynomial $p(t_1, \ldots, t_n) \in K[t_1, \ldots, t_n]$ and distinct $e_1, \ldots, e_n \in E$ so that $p(e_1, \ldots, e_n) = 0$. E is *linearly independent* otherwise.
   - $\{e_1, \ldots, e_n\}$ are linearly dependent iff there is j so that $e_j \in \mathrm{Span}_K \{e_i\}_{i \neq j}$.

(2) The union of a chain of linearly independent subsets is linearly independent.
   - Call these *bases* of L.
   - Bases are *spanning*: every $\alpha \in L$ depends linearly on a finite subset of a basis.
   - By Zorn's lemma, maximal linearly independent subsets exist.

(3) Two maximally independent sets have the same cardinality.

LEMMA 188 (Steinitz Exchange Lemma). *Let $B \subset L$ be linearly independent and let $C \subset L$ be a basis. Then for any $b \in B \setminus C$ there is $c \in C \setminus B$ so that $B \setminus \{b\} \cup \{c\}$ is linearly independent.*

PROOF. $B \setminus \{b\}$ is not a basis, while C is spanning, so some $c \in C$ is not in $\mathrm{Span}_K (B \setminus \{b\})$ and hence $B \setminus \{b\} \cup \{c\}$ is linearly independent. Since $B \cap C \subset B \setminus \{b\}$, $c \notin B \cap C$ so $c \in C \setminus B$. □

THEOREM 189. *Let $B, C \subset L$ be maximal linearly independent sets. Then $|B| = |C|$.*

PROOF. Suppose one of B, C is finite, wlog C. Repeatedly apply the Lemma, replacing elements of B with elements of C. Since $B \cap C$ increases at every step this process must terminate in at most $\#C$ steps. But the process preserves the size of B only stops when $B \subset C$, and it follows that $\#B \leq \#C$, and in particular that B is finite as well, and thus by symmetry that $\#B = \#C$.

Otherwise both B, C are infinite. Then each $b \in B$ is a linear combination of a finite subset $C_b \subset C$. Now $B \subset \mathrm{Span}_K \left(\bigcup_{b \in B} C_b\right)$ and B is spanning, so $\bigcup_{b \in B} C_b$ is a spanning subset of C, that is C itself. It follows that

$$|C| = \left|\bigcup_{b \in B} C_b\right| \leq |B| \times \aleph_0 = |B|$$

since B is infinite. By symmetry we then have $|B| = |C|$. □

4.1.2. Rings of polynomials and fields of rational functions in many variables. Let K be a field, T a set disjoint from T. We would like to formally construct a ring $K[T]$ embodying the idea of "the ring of polynomials with variables in T".

LEMMA-DEFINITION 190. *A* monomial *will be a function of finite support $\alpha \colon T \to \mathbb{Z}_{\geq 0}$. Usually write $\underline{t}^\alpha$ instead. Let $K[T]$ be the formal span of the monominals. Defining multiplication in the natural way gives an integral domain so that for any commutative K-algebra A, any map $\phi \colon T \to A$ extends uniquely to $\phi \colon K[T] \to A$. Also let $K(T)$ be the associated field of fractions.*

PROOF. Details in the supplement to PS10. □

EXERCISE 191. $\dim_K K(T) = \max\{|K|, |T|, \aleph_0\}$.

4.1.3. Transcendental elements and trancendence bases. Fix a field extension L/K.

LEMMA-DEFINITION 192. *Let $\{e_i\}_{i=1}^r \subset L$. TFAE:*

1. *There exists a non-zero polynomial $p \in K[t_1, \ldots, t_n]$ so that $p(e_1, \ldots, e_n) = 0$.*
2. *There exists e_j which is algebraic over $K\left(\{e_i\}_{i \neq j}\right)$.*

In this case we say that E is algebraically dependent *over K. Otherwise we say that E is* algebraically independent. *We say an infinite set is algebraically dependent if it has an algebraically dependent subset.*

PROOF. Let p be a polynomial with the smallest number of non-zero monomials such that $p(e_1, \ldots, e_r) = 0$. Suppose wlog that t_n occurs in the polynoimal, and write it as $p \in K[t_1, \ldots, t_{n-1}][t_n]$, say $p = \sum_{k=0}^d a_k(t_1, \ldots, t_{n-1}) t_n^k$. Then $a_k(e_1, \ldots, e_{k-1}) \neq 0$ (else we could remove many monomials from p). In particular $f = \sum_{k=0}^d a_k(e_1, \ldots, e_{n-1}) t^k \in K(e_1, \ldots, e_{n-1})[t]$ is non-zero and has $f(e_n) = 0$.

Conversely suppose e_n is algebraic over $K\left(\{e_i\}_{i<n}\right)$. Then there are $a_k \in K\left(\{e_i\}_{i<n}\right)$ with a_d non-zero so that $\sum_{k=0}^d a_k e_n^k = 0$. Clearing denominators we may assume there are $b_k \in K[t_1, \ldots, t_{n-1}]$ so that $a_k = b_k(e_1, \ldots, e_{n-1})$ and then $p = \sum_{k=0}^d b_k \cdot t^d$ works. □

DEFINITION 193. An extension $K(E) : K$ is called *purely transcendental* if E is algebraically independent.

LEMMA 194. *In that case a bijection $\phi \colon T \to E$ extends to a bijection $\phi \colon K(T) \to K(E)$.*

LEMMA-DEFINITION 195. *Let $E \subset L$ be algebraically independent over K. Then TFAE:*

1. *E is a maximal algebraically independent set.*
2. *$L : K(E)$ is an algebraic extension.*

In that case we call E a transcendence basis *for L.*

PROOF. Suppose E is a maximal, and let $\alpha \in L$. Then $E \cup \{\alpha\}$ is algebraically dependent, so there are distinct $\{e_i\}_{i=1}^n \subset E$ and $p \in K[t_1, \ldots, t_n, t]$ so that $p(\underline{e}, \alpha) = 0$. Write $p = \sum_{k=0}^d a_k(\underline{t}) t^k$. Each $a_k(\underline{e})$ must be non-zero because $\{e_i\}_{i=1}^n$ are independent, and it follows that $f(\alpha) = 0$ where f is he non-zero polynomial $\sum_{k=0}^d a_k(\underline{e}) t^d \in K(E)[t]$.

Conversely, suppose that $L : K(E)$ is algebraic, and let $\alpha \in L$. Then there is $f \in K(E)[t]$ so that $f(\alpha) = 0$. Writing each coefficient of f as a rational function in the elements of E, and then the argument of the previous Lemma shows that $E \cup \{\alpha\}$ is dependent. □

PROPOSITION 196. *Every extension has a transcendence basis.*

PROOF. Let $\mathcal{F} \subset \mathcal{P}(L)$ be the family of algberaically independent subsets of L. It is non-empty since the empty set is algebraically independent.

Now for any chain \sbset$\mathcal{C} \subset \mathcal{F}$ let $\{e_i\}_{i=1}^n \subset \bigcup \mathcal{C}$. For each i there is $E_i \in \mathcal{C}$ so that $e_i \in E_i$. Now the induced linear order on $\{E_i\}_{i=1}^n \subset \mathcal{C}$ has a maximal element, so let $E \in \mathcal{C}$ contain all the E_i. Then all e_i belong to E as well, and since E is algebraically independent it follows the $\{e_i\}$ are, and hence that $\bigcup \mathcal{C}$ is independent. By Zorn's Lemma $\mathcal{F}$ contains maximal elements. □

COROLLARY 197. *Every extension can be written as a purely transcendental extension followed by an algebraic extension.*

LEMMA 198 (Finite replacement). *Let $E \subset L$ be algebraically independent and let $F \subset L$ be a transcendence basis. Suppose E is not contained in F. Then there are $e \in E \setminus F$ and $f \in F \setminus E$ such $(E \setminus \{e\}) \cup \{f\}$ is algebraically independent.*

PROOF. Let $e \in E \setminus F$ be arbitrary. Then $E \setminus \{e\}$ is algebraically independent, but is not a trascendence basis (it is not maximal). If every $a \in F$ was algebraic over $K(E \setminus \{e\})$ then every element of $K(F)$ would be algebraic over $K(E \setminus \{e\})$. Since L is algebraic over $K(F)$, this would make L algebraic over $K(E \setminus \{e\})$, a contradiction. Thus there is $f \in F$ which is transcendental over $E \setminus \{e\}$. In particular $f \notin E \cap F \subset E \setminus \{e\}$ and hence $(E \setminus \{e\}) \cup \{f\}$ is algebraically independent. □

COROLLARY 199. *If F is finite then so is E and $\#E \leq \#F$.*

PROOF. As long as E is not a subset of F we may replace an element of E with an element of F, preserving the size of E. After at most $\#F$ steps we either have $E \subset F$ (so that $\#E \subset \#F$) or $F \subset E$ (in which case $F = E$ since F is a transcendence basis, so it is a maximal algebraically independent set). $\square$

THEOREM 200. *Let $E, F \subset L$ be transcendence bases over K. Then $|E| = |F|$.*

PROOF. If at least one of E, F is finite then the corollary shows that the other is finite and that we have both inequalitys $\#E \leq \#F$ and $\#F \leq \#E$ so their sizes are equal. Suppose then that E, F are both infinite. Now each $e \in E$ is algebraic over $K(F)$, so there is a finite subset $F_e \subset F$ so that e is algebraic over F_e. Furthermore, $\bigcup_{e \in E} F_e \subset F$ is algebraically independent such that every element of e is algebraic over $K\left(\bigcup_{e \in E} F_e\right)$. As above this means that L is algebraic over this field, and thus that $\bigcup_{e \in E} F_e$ is a transcendence basis contained in F, and hence F exactly.

We then have

$$|F| = \left|\bigcup_{e \in E} F_e\right| \leq |E| \times \aleph_0 = |E|$$

since E is infinite. Symmetry also gives $|E| \leq |F|$ and we get equality. $\square$

4.2. Infinite Galois Theory

Let L/K be an extension. We recall the following definitions:

(1) L is *algebraic* over K if each $\alpha \in L$ is the zero of a polynomial $f \in K[x]$. Further:
(2) L is *normal* over K if for each $\alpha \in L$ the minimal polynomial $m_\alpha \in K[x]$ splits in L.
(3) L is *separably algebraic* over K if for each $\alpha \in L$ the minimal polynomial $m_\alpha \in K[x]$ has distinct roots in its splitting field.

We note that these definitions make sense for any extension, finite or not.