GRADUATE ALGEBRA: NUMBERS, EQUATIONS, SYMMETRIES

JENIA TEVELEV

CONTENTS

§1. ALGEBRAIC FIELD EXTENSIONS

§1.1. **Field extensions.** We almost never focus on a single field In algebra. Indeed, rings can be understood by describing their ideals or modules. But fields have no proper ideals and modules over a field are vector spaces, the subject of linear algebra. Instead, a typical situation is to have two fields

$$K \subset F.$$

Then F is called a *field extension* of K: we extend K by adjoining new elements, for example roots of polynomial equations

$$\mathbb{R} \subset \mathbb{C}, \quad \mathbb{Q} \subset \mathbb{Q}(\sqrt{2}), \quad \dots$$

Another notation for a field extension is F/K: F is a field *over* K.

DEFINITION 1.1.1. A field F over K can be viewed as a vector space over K by using addition in F to add vectors and using multiplication in F to define scalar multiplication λx for $\lambda \in K$ and $x \in F$. Its dimension is called the *degree* of F over K:

$$[F : K] := \dim_K F.$$

If $[F : K] < \infty$ then F is called a *finite extension* of K.

For example, $[\mathbb{C} : \mathbb{R}] = 2$. The basis of $\mathbb{C}$ over $\mathbb{R}$ is given by 1 and i. We also have $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. The basis is given by 1 and $\sqrt{2}$. Indeed,

- 1 and $\sqrt{2}$ are linearly independent over $\mathbb{Q}$, i.e. $a + b\sqrt{2} \neq 0$ if a or b is not equal to zero. This is because $\sqrt{2}$ is irrational, $\sqrt{2} \neq -a/b$.
- 1 and $\sqrt{2}$ generate $\mathbb{Q}(\sqrt{2})$ as a vector space over $\mathbb{Q}$. Apriori, an element of $\mathbb{Q}(\sqrt{2})$ is a fraction $\frac{a+b\sqrt{2}}{c+d\sqrt{2}}$ with $a, b, c, s \in \mathbb{Q}$. However, multiplying the numerator and denominator by $c - d\sqrt{2}$ we can rewrite this fraction as a linear combination of 1 and $\sqrt{2}$.

DEFINITION 1.1.2. Consider a field extension $K \subset F$. An element $\alpha \in F$ is called *algebraic* over K if α is a root of a non-trivial polynomial with coefficients in K. An element which is not algebraic is called *transcendental*.

- $i \in \mathbb{C}$ is a root of $x^2 + 1 \in \mathbb{Q}[x]$, so i is algebraic over $\mathbb{Q}$.
- $\pi \in \mathbb{R}$ is transcendental over $\mathbb{Q}$ (Lindemann's Theorem).
- $x \in \mathbb{C}(x)$ is transcendental over $\mathbb{C}$. (Why?)

DEFINITION 1.1.3. Consider a field extension $K \subset F$. Let $\alpha \in F$ be algebraic. A polynomial $f(x) \in K[x]$ is called a *minimal polynomial* of α if $f(x)$ is a monic polynomial of minimal possible degree such that $f(\alpha) = 0$.

Let us point out one persistent notational ambiguity. If x is a variable then $K[x]$ denotes the algebra of polynomials and $K(x)$ denotes the field of rational functions (i.e. ratios of polynomials) in variable x. But given a field extension $K \subset F$ and an element $\alpha \in F$, $K[\alpha]$ denotes the minimal subring of F generated by K and by α and $K(\alpha)$ denotes the minimal subfield of F generated by K and by α. These objects are related as follows:

THEOREM 1.1.4. *Consider a field extension $K \subset F$. Let $\alpha \in F$. Consider a unique surjective homomorphism $\phi : K[x] \to K[\alpha]$ that sends x to α.*

- *If α is transcendental then ϕ is an isomorphism, which induces an isomorphism of fields $K(x) \simeq K(\alpha)$. In particular, $[K(\alpha) : K] = \infty$.*
- *If α is algebraic then $\operatorname{Ker}\phi$ is generated by the minimal polynomial $f(x)$, which is irreducible and unique. Let $n = \deg f(x)$. Then $[K(\alpha) : K] = n$. Moreover, $K[\alpha] = K(\alpha)$ and $1, \alpha, \ldots, \alpha^{n-1}$ form a K-basis of $K(\alpha)$.*

Proof. $\operatorname{Ker}\phi$ is an ideal of all polynomials that vanish at α. $\operatorname{Ker}\phi = 0$ if and only if α is transcendental (by definition). In this case

$$K[x] \simeq K[\alpha] \subset F.$$

Any injective homomorphism of a domain into a field extends to the injective homomorphism of its field of fractions. So in our case ϕ extends to the injective homomorphism $K(x) \to F$, and its image is obviously $K(\alpha)$.

If α is algebraic then, since $K[x]$ is a PID, $\operatorname{Ker}\phi$ is generated by a unique monic polynomial $f(x)$, hence a minimal polynomial is unique. Since

$$K[x]/\operatorname{Ker}\phi \simeq K[\alpha]$$

injects in F, which is a domain, $K[x]/\operatorname{Ker}\phi$ is also a domain, hence $f(x)$ is irreducible and $\operatorname{Ker}\phi = (f)$ is a maximal ideal. So $K[x]/\operatorname{Ker}\phi$ is a field. Therefore, $K[\alpha]$ is a field. Therefore, $K[\alpha] = K(\alpha)$.

Finally, we notice that $1, \alpha, \ldots, \alpha^{n-1}$ are linearly independent over K (otherwise we can find a smaller degree polynomial vanishing at α) and span $K[\alpha]$ over K. Indeed, since $f(x) = x^n + \ldots$ vanishes at α, we can rewrite α^n as a linear combination of smaller powers of α. An easy argument by induction shows that we can rewrite any α^m for $m > n$ as as a linear combination of $1, \alpha, \ldots, \alpha^{n-1}$. □

An often used corollary:

COROLLARY 1.1.5. *If α is algebraic over K then $[K(\alpha) : K]$ is equal to the degree of the minimal polynomial of α.*

The number $[K(\alpha) : K]$ is also often called the *degree of α over K*.

EXAMPLE 1.1.6. $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 4$. This calculation involves a trick which will become much more transparent after we discuss Galois theory. The polynomial of degree 4

$$f(x) = \prod(x \pm \sqrt{2} \pm \sqrt{3}) = x^4 - 10x^2 + 1$$

obviously has $\sqrt{2} + \sqrt{3}$ as a root. To show that it is irreducible, we have to show that it has no linear and quadratic factors over $\mathbb{Q}$. If it has a linear factor then $\sqrt{2} \pm \sqrt{3} \in \mathbb{Q}$, therefore $(\sqrt{2} \pm \sqrt{3})^2 \in \mathbb{Q}$, therefore $\sqrt{6} \in \mathbb{Q}$. Then we use the standard argument: if $\sqrt{6} = a/b$ in lowest terms then $a^2 = 6b^2$, therefore $2|a$, therefore $4|a^2$, therefore $2|b$, contradiction. Suppose $f(x)$ has a quadratic factor over $\mathbb{Q}$. Its coefficients are, up to a sign, a sum and a product of two roots of $f(x)$. If the sum belongs to $\mathbb{Q}$ then $\sqrt{2}$ or $\sqrt{3}$ belong to $\mathbb{Q}$, unless the two roots are opposite, say $\sqrt{2} + \sqrt{3}$ and $-\sqrt{2} - \sqrt{3}$. But if their product is in $\mathbb{Q}$ then again $\sqrt{6} \in \mathbb{Q}$, a contradiction.

EXAMPLE 1.1.7. $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ and the minimal polynomial is $x^3 - 2$ (irreducible by the Eisenstein's criterion).

§1.2. **Multiplicativity of degree.**

LEMMA 1.2.1. *Consider a tower of field extensions*

$$K \subset F \subset L.$$

If $[F : K] = n$ *and* $[L : F] = m$ *then* $[L : K] = nm$.

Proof. It is easy to prove that if $e_1, \dots, e_m$ is a basis of L over F and $f_1, \dots, f_n$ is a basis of F over K then $\{e_i f_j\}$ is a basis of L over K. (Why?) □

This statement has interesting divisibility consequences. For example, if $K/\mathbb{Q}$ is a finite field extension containing $\sqrt{2}$, then $[K : \mathbb{Q}]$ is even because

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

§1.3. **Algebraic extensions.**

DEFINITION 1.3.1. An extension $K \subset F$ is called *algebraic* if any element of F is algebraic over K.

THEOREM 1.3.2. *(a) Any finite extension is algebraic.*
(b) Let $\alpha_1, \dots, \alpha_r \subset F$ *be algebraic over* K. *Then*

$$K(\alpha_1, \dots, \alpha_r) = K[\alpha_1, \dots, \alpha_r]$$

is finite over K. *In particular, any element of* $K(\alpha_1, \dots, \alpha_r)$ *is algebraic over* K.

Proof. If $[F : K] < \infty$ then $1, \alpha, \alpha^2, \dots$ are linearly dependent over K for any $\alpha \in F$. Therefore, some non-constant polynomial with coefficient in K vanishes at α, i.e. α is algebraic.

Now suppose that $\alpha_1, \dots, \alpha_r \subset F$ are algebraic over K. Arguing by induction on r (with the base of induction given by Theorem 1.1.4), let's assume that $K(\alpha_1, \dots, \alpha_{r-1}) = K[\alpha_1, \dots, \alpha_{r-1}]$ is finite over K. Since α_r is algebraic over K, it is also algebraic over $K(\alpha_1, \dots, \alpha_{r-1})$. Using Theorem 1.1.4, we see that

$$K(\alpha_1, \dots, \alpha_{r-1})[\alpha_r] = K(\alpha_1, \dots, \alpha_{r-1})(\alpha_r) = K(\alpha_1, \dots, \alpha_{r-1}, \alpha_r)$$

is finite-dimensional over $K(\alpha_1, \dots, \alpha_{r-1})$. Then $[K(\alpha_1, \dots, \alpha_r) : K] < \infty$ by Lemma 1.2.1. It follows from part (a) that any element of $K(\alpha_1, \dots, \alpha_r)$ is algebraic over K. □

One consequence of this theorem is that if α and β are algebraic over K then so are $\alpha + \beta$, $\alpha\beta$, and α/β. However, it can take some work to write their minimal polynomials, as Example 1.1.6 shows.

§1.4. **Adjoining roots.** In the previous section we studied a fixed extension $K \subset F$. If $\alpha \in F$ is algebraic over K then $K(\alpha)$ is isomorphic to $K[x]/(f)$, where $f(x)$ is a minimal polynomial of α. An algebraic extension

$$K \subset K(\alpha)$$

generated by one element is called a *simple extension*. Now we start with a field K and learn how to build its simple extensions and compare them. The main building block was discovered by Kronecker:

LEMMA 1.4.1. *If $f(x) \in K[x]$ is irreducible and monic then $K[x]/(f)$ is a field extension of K generated by $\alpha := x + (f)$. The minimal polynomial of α is $f(x)$.*

Proof. Since f is irreducible and $K[x]$ is a PID, $K[x]/(f)$ is a field. It is obviously generated by α. Since $f(\alpha) \equiv 0 \mod (f)$ in the quotient ring, α is a root of $f(x)$. Since $f(x)$ is irreducible over K, $f(x)$ is the minimal polynomial of α. □

DEFINITION 1.4.2. Let F and F' be field extensions of K. Then F and F' are called *isomorphic over K* if there exists an isomorphism $\phi : F \to F'$ such that $\phi|_K = \mathrm{Id}$. More generally, we can talk about *homomorphisms over K*.

LEMMA 1.4.3. *Let $K(\alpha)$ and $K(\beta)$ be algebraic extensions of K. TFAE:*

- *α and β have the same minimal polynomial.*
- *There exists and isomorphism of $K(\alpha)$ to $K(\beta)$ over K that sends α to β.*

Proof. If α and β have the same minimal polynomials then the analysis above shows that both $K(\alpha)$ and $K(\beta)$ are isomorphic to $K[x]/(f)$, where $f(x)$ is the common minimal polynomial. Notice that an induced isomorphism between $K(\alpha)$ and $K(\beta)$ simply sends α to β. □

EXAMPLE 1.4.4. Fields $\mathbb{Q}(\sqrt[3]{2})$ and $\mathbb{Q}(\omega\sqrt[3]{2})$ are isomorphic (here ω is a primitive cubic root of unity), because $\sqrt[3]{2}$ and $\omega\sqrt[3]{2}$ have the same minimal polynomial $x^3 - 2$. However, they are not equal inside $\mathbb{C}$ because $\mathbb{Q}(\sqrt[3]{2})$ is contained in $\mathbb{R}$ but the other field is not.

EXAMPLE 1.4.5. By contrast, it is easy to see that

$$\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2}-\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3}).$$

Indeed, let $\alpha = \sqrt{2}+\sqrt{3}$. Since $5 + 2\sqrt{6} = \alpha^2 \in \mathbb{Q}(\alpha)$, $\sqrt{6} \in \mathbb{Q}(\alpha)$ as well. So $2\sqrt{3}+3\sqrt{2} = \alpha\sqrt{6} \in \mathbb{Q}(\alpha)$ and $\sqrt{2} = (2\sqrt{3}+3\sqrt{2}) - 2(\sqrt{3}+\sqrt{2}) \in \mathbb{Q}(\alpha)$. So in this case the isomorphism of the Lemma sending $\sqrt{2}+\sqrt{3}$ to $\sqrt{2}-\sqrt{3}$ is an automorphism of the field $\mathbb{Q}(\sqrt{2},\sqrt{3})$.

§1.5. **Splitting fields.** Now we would like to construct a field extension which contains all roots of a polynomial.

DEFINITION 1.5.1. A field $F \supset K$ is called a *splitting field* of $f(x) \in K[x]$ if

- f splits into linear factors in $F[x]$, and
- F is generated by roots of $f(x)$.

In other words, $f(x)$ splits in F but not in any proper subfield of F.

EXAMPLE 1.5.2. As in Example 1.4.5, $\mathbb{Q}(\sqrt{3}+\sqrt{2}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$, which contains all roots of the minimal polynomial of $f(x)$ of $\sqrt{2}+\sqrt{3}$. So in this case $\mathbb{Q}(\sqrt{3}+\sqrt{2})$ is a splitting field of $f(x)$.

EXAMPLE 1.5.3. $\mathbb{Q}(\sqrt[3]{2})$ is not a splitting field of $f(x) = x^3 - 2$ because not all of the roots are real. The splitting field is $\mathbb{Q}(\sqrt[3]{2},\omega)$. It has degree 6 over $\mathbb{Q}$ by multiplicativity of degree because ω is a root of the quadratic polynomial $x^2 + x + 1$. Since $\omega \notin \mathbb{Q}(\sqrt[3]{2})$, this quadratic polynomial is irreducible over $\mathbb{Q}(\sqrt[3]{2})$.

LEMMA 1.5.4. *Any polynomial $f(x) \in K[x]$ has a splitting field. Moreover, any two splitting fields L and L' are isomorphic over K.*

Proof. We can assume that f is monic. Existence is proved by induction on degree: if $f(x)$ does not split then it has an irreducible factor $g(x)$ of degree greater than one. Lemma 1.4.1 gives an extension $K \subset L = K(\alpha)$ such that $g(x)$ has a root $\alpha \in L$. Then $f(x)/(x-\alpha) \in L[x]$ has a splitting field $F \supset L$ by inductive assumption. Then F is a splitting field of $f(x) \in K[x]$ as well.

Now we have to construct an isomorphism between two splitting fields L and L' over K. It is enough to construct an injective homomorphism $\phi : L \to L'$ that fixes K. Indeed, if $f(x) = \prod_i (x - \alpha_i)$ in L then $f(x) = \prod_i (x - \phi(\alpha_i))$ in $\phi(L)$, so $f(x)$ splits in $\phi(L)$, so $\phi(L) = L'$.

We will construct ϕ step-by-step. Choose a root $\alpha \in L$ of $f(x)$. Let $g(x)$ be the minimal polynomial of α. Then $g(x)$ divides $f(x)$, and in particular $g(x)$ splits in L'. Let β be a root of $g(x)$ in L'. Since α and β have the same minimal polynomial, $K(\alpha)$ and $K(\beta)$ are isomorphic over K. Fix one isomorphism,

$$\phi_0 : K(\alpha) \to K(\beta).$$

Now we have a diagram of field maps

$$\begin{array}{ccc} L & & L' \\ \uparrow & & \uparrow \\ K(\alpha) & \xrightarrow[\phi_0]{} & K(\beta) \end{array} \tag{1}$$

Notice that L is a splitting field of $f(x)$ over $K(\alpha)$ and L' is a splitting field of $f(x)$ over $K(\beta)$. So ideally, we would like to finish by induction by continuing to add roots of α. However, notice that the set-up is slightly different: before we were trying to show that L and L' are isomorphic over K, and now we are trying to construct an isomorphism $\phi : L \to L'$ that extends a given isomorphism $\phi_0 : K(\alpha) \to K(\beta)$. So the best thing to do is to generalize our Lemma a little bit to make it more suitable for induction. This is done in the next Lemma. □

LEMMA 1.5.5. *Suppose we have a diagram of homomorphisms of fields*

$$\begin{array}{ccc} L_1 & & L_2 \\ \uparrow & & \uparrow \\ K_1 & \xrightarrow[\psi]{} & K_2 \end{array} \tag{2}$$

where L_1 is a splitting field of $f_1(x) \in K_1[x]$ and the polynomial $f_2(x) \in K_2[x]$, obtained by applying ψ to all coefficients of $f_1(x)$, splits in L_2. Then there exists a homomorphism $\phi : L_1 \to L_2$ such that $\phi|_{K_1} = \psi$.

Proof. Choose a root $\alpha \in L_1$ of $f_1(x)$. Let $g_1(x)$ be the minimal polynomial of α. Then $g_1(x)$ divides $f_1(x)$. We have a homomorphism

$$\Psi : K_1[x] \to K_2[x]$$

that extends ψ. Then $f_2 = \Psi(f_1)$. Let $g_2 = \Psi(g_1)$. Then $g_2 | f_2$, and in particular $g_2(x)$ splits in L_2. Let β be a root of $g_2(x)$ in L_2. Let $g_2'(x) \in K_2[x]$

be an irreducible factor of $g_2(x)$ with root β. Then

$$K_1(\alpha) \simeq K_1[x]/(g_1) \quad \text{and} \quad K_2(\beta) \simeq K_2[x]/(g_2').$$

Notice that Ψ induces a homomorphism $K_1[x]/(g_1) \to K_2[x]/(g_2')$. This gives an homomorphism

$$\phi_0 : K_1(\alpha) \to K_2(\beta)$$

that sends α to β and such that $\phi_0|_{K_1} = \psi$. Now we have a commutative diagram of field maps

$$\begin{array}{ccc} L_1 & & L_2 \\ \uparrow & & \uparrow \\ K_1(\alpha) & \xrightarrow[\phi_0]{} & K_2(\beta) \\ \uparrow & & \uparrow \\ K_1 & \xrightarrow[\psi]{} & K_2 \end{array} \tag{3}$$

Notice that L_1 is a splitting field of $f_1(x)$ over $K_1(\alpha)$ and $f_2(x)$ splits in L_2. So we are in the same set-up as in the statement of the Lemma, but now $[L_1 : K_1(\alpha)] < [L_1 : K_1]$. So we can finish by induction on $[L_1 : K_1]$. □

§1.6. **Algebraic closure.**

LEMMA 1.6.1. *Let K be a field. The following are equivalent:*

- *any polynomial $f \in K[x]$ has a root in K.*
- *any polynomial $f \in K[x]$ splits in K.*
- *The only algebraic extension of K is K itself.*

Proof. Easy. □

If any of these conditions are satisfied then K is called *algebraically closed*.

DEFINITION 1.6.2. Let K be a field. A field $\bar{K}$ containing K is called an *algebraic closure* of K if

- $\bar{K}$ is algebraically closed.
- $K \subset \bar{K}$ is an algebraic extension.

For example, $\mathbb{C}$ is an algebraic closure of $\mathbb{R}$ but not of $\mathbb{Q}$ (why?)

LEMMA 1.6.3. *Let $K \subset F$ be a field extension with F algebraically closed. Then*

$$\bar{K} = \{a \in F \,|\, a \text{ is algebraic over } F\}$$

is an algebraic closure of K.

Proof. If $\alpha, \beta \in \bar{K}$ then $K(\alpha, \beta) \subset F$ is algebraic over K by Theorem 1.3.2 and $\alpha + \beta, \alpha - \beta, \alpha\beta \in \bar{K}$. So $\bar{K}$ is a field (obviously algebraic over K). Every polynomial $x^n + a_1 x^{n-1} + \ldots + a_n \in \bar{K}[x] \subset F[x]$ has a root α in F. Since $[K(a_1, \ldots, a_n) : K] < \infty$ and $[K(a_1, \ldots, a_n)(\alpha) : K(a_1, \ldots, a_n)] < \infty$, $[K(\alpha) : K] < \infty$ and therefore α is algebraic over K. □

For example, if $K = \mathbb{Q}$ and $F = \mathbb{C}$ then $\bar{K} = \bar{\mathbb{Q}} \subset \mathbb{C}$ is the field of all algebraic numbers (roots of polynomials with rational coefficients).

LEMMA 1.6.4. *For every field K, one can find a field F such that every polynomial in $K[x]$ has a root in F.*

Proof. The idea is to use a Kronecker-type construction to adjoin roots of all polynomials at once. Let $K[x_f]$ be the algebra of polynomials in variables x_f: one variable x_f for each irreducible monic polynomial $f \in k[x]$. Consider the ideal

$$I = \langle f(x_f) \rangle \subset K[x_f]$$

with one generator for each variable. Notice that each polynomial is a polynomial in its own variable. We claim that I is a proper ideal. If not then

$$1 = \sum_{i=1}^{s} g_i f_i(x_{f_i}),$$

where g_i are some polynomials that involve only finitely many variables x_f. Let L be a splitting field of the product $f_1 \dots f_s$. The formula above remains valid in $L[x_f]$. However, if we plug-in any root of f for x_f (for each f), we will get $1 = 0$, a contradiction. It follows that I is a proper ideal.

Let M be a maximal ideal containing I. Then $F := K[x_f]/M$ is a field that contains K. We claim that any irreducible polynomial $f \in K[x]$ has a root in F. Indeed, $f(x_f) \in M$, and therefore $x_f + M$ is a root of f in F. □

THEOREM 1.6.5. *Any field K has an algebraic closure. It is unique up to an isomorphism over K.*

Proof. Applying Lemma 1.6.4 inductively gives an infinite tower of fields

$$K = F_0 \subset F_1 \subset F_2 \subset \dots$$

such that every polynomial in $F_k[x]$ has a root in F_{k+1}. Then $F = \cup_i F_i$ is an algebraically closed field as any polynomial in $F[x]$ in fact belongs to some $F_k[x]$, and therefore has a root in $F_{k+1} \subset F$. Applying Lemma 1.6.3 gives an algebraic closure $\bar{K} \subset F$.

Let $\bar{K}$, $\bar{K}_1$ be two algebraic closures of K. It suffices to show that there exists a homomorphism $\phi : \bar{K} \to \bar{K}_1$ over K. Indeed, $\phi(\bar{K})$ is then another algebraic closure of K contained in $\bar{K}_1$. Since $\bar{K}_1$ is algebraic over $\phi(\bar{K})$, it must be equal to it.

Finally, we construct ϕ using Zorn's lemma. Consider a poset of pairs (F, ϕ), where $K \subset F \subset \bar{K}$ and $\phi : F \to \bar{K}_1$ is a homomorphism over K. We say that $(F, \phi) \leq (F_1, \phi_1)$ if $F \subset F_1$ and ϕ is the restriction of ϕ_1 to F. Then every chain

$$(F_1, \phi_1) \leq (F_2, \phi_2) \leq (F_3, \phi_3) \leq \dots$$

has an upper bound (F, ϕ) (take $F = \cup F_i$ and the map $\phi : F \to \bar{K}_1$ induced by ϕ_i's). By Zorn's lemma, our poset has a maximal element (F, ϕ) but then F must be equal to $\bar{K}$. Indeed, if F is properly contained in $\bar{K}$ then take any $\alpha \in \bar{K} \setminus F$. By Lemma 1.5.5, we can extend ϕ to a homomorphism $F(\alpha) \to \bar{K}_1$. □

The same argument shows the following:

PROPOSITION 1.6.6. *Suppose we have a diagram of homomorphisms of fields*

$$\begin{array}{ccc} & & L_1 \\ & & \uparrow \\ & & \hookrightarrow \\ K_1 & \xrightarrow[\psi]{} & K_2 \end{array}$$

where L_1 is algebraic over K_1 and K_2 is algebraically closed. Then there exists a homomorphism $\phi : L_1 \to K_2$ such that $\phi|_{K_1} = \psi$.

§1.7. **Finite fields.**

THEOREM 1.7.1. *For any prime p and positive integer n, there exists a field $\mathbb{F}_{p^n}$ with p^n elements. Moreover, any two such fields are isomorphic. We can embed $\mathbb{F}_{p^m}$ in $\mathbb{F}_{p^n}$ if and only if m divides n.*

Proof. Let K be a splitting field of the polynomial $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$. Since $f'(x) = -1$ is coprime to $f(x)$, there are exactly p^n roots. Recall that $F : K \to K$, $F(x) = x^p$ is a Frobenius homomorphism. In particular, if α and β are roots of $f(x)$ then $\pm\alpha \pm \beta$ and $\alpha\beta$, and α/β are roots as well. It follows that K has p^n elements and all of them are roots of $f(x)$.

Suppose K is a field with p^n elements. The group of units K^* is Abelian of order $p^n - 1$, and therefore $x^{p^n-1} = 1$ for any $x \in K^*$.[1] It follows that K is a splitting field of $x^{p^n} - x$. But any two splitting fields of the same polynomial are isomorphic by Lemma 1.5.4.

If $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$ then the latter field is a vector space (of some dimension r) over the former. It follows that

$$p^n = (p^m)^r = p^{mr}.$$

It follows that m divides n.

Finally, suppose that m divides n. Then $p^m - 1 | p^n - 1$ and by the same argument $x^{p^m-1} - 1 | x^{p^n-1} - 1$. It follows that the splitting field of $x^{p^m} - x$ is contained in the splitting field of $x^{p^n} - x$. □

§1.8. **Exercises.**

[1] Recall that in fact this analysis implies that K^* is a cyclic group. Indeed, otherwise we would have $x^r = 1$ for any $x \in K^*$ and $r < p^n - 1$. However, the polynomial can not have more roots than its degree.

Homework 1

In this set we fix a field extension $K \subset F$ unless specified otherwise.

1. (a) Show that $\alpha \in F$ is algebraic over K if and only if F contains a finite-dimensional K-vector *subspace* L such that $\alpha \cdot L \subset L$. (b) If the conditions of (a) are satisfied, let $A : L \to L$ be a K-linear operator of multiplication by α. Show that its minimal polynomial in the sense of linear algebra is equal to the minimal polynomial of α in field-theoretic sense.

2. Consider field extensions $E \subset F \subset K$. Suppose that F is algebraic over E and K is algebraic over F. Show that K is algebraic over E.

3. (a) Show that $f(x) = x^3+x^2+x+3$ is irreducible over $\mathbb{Q}$. (b) Consider the field $F = \mathbb{Q}(\alpha)$, where α is a root of $f(x)$. Express $\frac{1}{2-\alpha+\alpha^2}$ as a $\mathbb{Q}$-linear combination of 1, α, and α^2.

4. Find the degree (over $\mathbb{Q}$) of the splitting field of (a) $x^4+x^3+x^2+x+1$. (b) x^4-2.

5. (a) Suppose $[F : K] = 2$ and $\operatorname{char} K \neq 2$. Show that there exists $D \in K$ such that $F = K(\sqrt{D})$. (b) Show that (a) can fail if $[F : K] = \operatorname{char} K = 2$.

6. For all positive integers n and m, compute the degree $[\mathbb{Q}(\sqrt{n}, \sqrt{m}) : \mathbb{Q}]$.

7. Let $K \subset F$ be an algebraic extension and let R be a subring of F that contains K. Show that R is a field.

8. Let $f(x) \in K[x]$ be a polynomial of degree 3. Show that if $f(x)$ has a root in a field extension $K \subset F$ of degree 2 then $f(x)$ has a root in K.

9. Let $\alpha, \beta \in F$ be algebraic over K, let $f(x)$ and $g(x)$ be their minimal polynomials, and suppose that $\deg f$ and $\deg g$ are coprime. Prove that $f(x)$ is irreducible in $K(\beta)[x]$.

10. Let $K \supset \mathbb{Q}$ be a splitting field of a cubic polynomial $f(x) \in \mathbb{Q}[x]$. Show that if $[K : \mathbb{Q}] = 3$ then $f(x)$ has 3 real roots.

11. Let $F = K(\alpha)$ and suppose that $[F : K]$ is odd. Show that $F = K(\alpha^2)$.

12. Let $f(x) \in K[x]$ be an irreducible polynomial and let $g(x) \in K[x]$ be any non-constant polynomial. Let $p(x)$ be a non-constant polynomial that divided $f(g(x))$. Show that $\deg f$ divides $\deg p$.

13. Show that the polynomial $x^5 - t$ is irreducible over the field $\mathbb{C}(t)$ (here t is a variable). Describe a splitting field.

14. Let $\mathbb{F}_q$ be a finite field with q elements. Compute $\sum_{a \in \mathbb{F}_q} a^k$ for $k > 0$.

15. (a) Show that the algebraic closure of $\mathbb{F}_p$ is the union of its finite subfields: $\bar{\mathbb{F}}_p = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}$. (b) Show that $\overline{\mathbb{F}}_p$ contains proper infinite subfields.

16. A complex number $\alpha \in \mathbb{C}$ is called *constructible* if $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is a power of 2. Assume without proof that α is constructible if and only if one can construct α (as a vector on the plane) using the ruler and the compass. (a) Show that $\cos 20^\circ$ is not constructible. (b) Show that trisection of an angle is not always possible using the ruler and the compass.

17. Let K_1, K_2 be subfields of a field K. Then *the composite field* K_1K_2 of K_1 and K_2 is the smallest subfield of K containing K_1 and K_2. Show that

$$[K_1K_2 : F] \leq [K_1 : F][K_2 : F],$$

with equality iff some basis of K_2 over F is linearly independent over K_1.

§2. GALOIS THEORY

Let $K \subset F$ be an algebraic extension. For convenience, in this section we fix an algebraic closure $\bar{K}$ of K and assume that $F \subset \bar{K}$.

§2.1. **Separable extensions.**

DEFINITION 2.1.1. An element $\alpha \in F$ is called *separable* over K if its minimal polynomial has no multiple roots.

LEMMA 2.1.2. *Let $\alpha \in F$ and let $f(x)$ be its minimal polynomial. Then α is not separable if and only if $\operatorname{char} K = p$ and $f'(x) \equiv 0$. In this case $f(x) = g(x^p)$ for some polynomial $g(x)$.*

Proof. Indeed, $f(x)$ has a multiple root if and only the g.c.d. of $f(x)$ and $f'(x)$ has positive degree. Since $f(x)$ is irreducible, this is only possible if $f'(x) \equiv 0$. But then $\operatorname{char} K = p$ and $f(x) = g(x^p)$ for some $g(x) \in K[x]$. □

DEFINITION 2.1.3. An algebraic extension F/K is called *separable* if any $\alpha \in F$ is separable over K.

THEOREM 2.1.4. *Let F/K be an algebraic extension. Suppose that F is generated over K by elements α_i, $i \in I$. Then the following conditions are equivalent:*

(1) *F/K is separable.*
(2) *α_i is separable for any $i \in I$.*

If, in addition, F/K is finite then this is equivalent to

(3) *The number of different embeddings $F \to \bar{K}$ over K is equal to $[F : K]$, the maximum possible number.*

Proof. (1) obviously implies (2). Next we assume that F/K is finite and show that (2) implies (3). In this case F is generated by finitely many α_i's, so we can assume that $I = \{1, \dots, r\}$ is a finite set. Then we have the tower

$$K = F_0 \subset F_1 \subset F_2 \subset \ldots \subset F_r = F,$$

where $F_k = K(\alpha_1, \dots, \alpha_k)$. Each α_k is separable over K and hence separable over F_{k-1}. We have $F_k = F_{k-1}(\alpha_k)$, and therefore the number of different embeddings of F_k in $\bar{K}$ over F_{k-1} is equal to $[F_k : F_{k-1}]$. But any homomorphism $F \to \bar{K}$ can be constructed step-by-step by extending the inclusion $K \subset \bar{K}$ to fields F_k in the tower. It follows that the number of different embeddings $F \to \bar{K}$ over K is equal to

$$[F : F_{r-1}][F_{r-1} : F_{r-2}] \dots [F_1 : K] = [F : K].$$

Moreover, the same reasoning shows that this is the maximum possible number of embeddings.

Now we show that (3) implies (1) (still assuming that F/K is finite). Suppose that $\alpha \in F$ is not separable. Then the number of embeddings $K(\alpha) \to \bar{K}$ is strictly less then $[K(\alpha) : K]$, and considering the tower $K \subset K(\alpha) \subset F$ gives the contradiction. Indeed, by the above, the number of different embeddings $F \to \bar{K}$ over $K(\alpha)$ is at most $[F : K(\alpha)]$.

Finally, we show that (2) implies (1) in general. Take $\alpha \in F$. Then $\alpha \in K(\alpha_1, \dots, \alpha_k)$ for a finite subset of generators. Since $K(\alpha_1, \dots, \alpha_k)$ is finite over K, the finite extension case considered above shows that α is separable. □

§2.2. **Normal extensions.**

DEFINITION 2.2.1. An algebraic extension F/K is called *normal* if the minimal polynomial of any $\alpha \in F$ splits in $F[x]$ into the product of linear factors.

THEOREM 2.2.2. *Let F/K be algebraic and suppose that F is generated over K by elements α_i, $i \in I$. Let's also assume that $F \subset \bar{K}$. Then TFAE:*

(1) *F/K is normal.*
(2) *Minimal polynomials of α_i's split in F.*
(3) *Any embedding $F \to \bar{K}$ over K has image F.*

Proof. It is obvious that (1) implies (2).

Let $\sigma : F \to \bar{K}$ be any homomorphism over K. Then $\sigma(\alpha_i)$ is a root of the minimal polynomial of α_i for any i. It follows that $\sigma(\alpha_i) \in F$ for any α_i. Therefore $\sigma(F) \subset F$. Applying the same argument but switching the pair of embedding $F \subset \bar{K}, \sigma(F) \subset \bar{K}$ shows that $F \subset \sigma(F)$.

Finally, we show that (3) impies (1). Suppose not. Then there exists $\alpha \in F$ such that its minimal polynomial does not split in F. Then there exists an embedding $K(\alpha) \to \bar{K}$ with image not contained in F (just send α to a root of the minimal polynomial not contained in F). This embedding can be extended to an embedding $\sigma : F \to \bar{K}$ with $\sigma(F) \not\subset \bar{K}$. □

§2.3. **Main Theorem of Galois Theory.**

DEFINITION 2.3.1. $K \subset F$ is a *Galois extension* if it is separable and normal.

Using our characterizations of normal and separable extensions, this definition can be spelled out in three different ways:

- $K \subset F$ is an algebraic extension such that the minimal polynomial of any $\alpha \in F$ has no multiple roots and splits in $F[x]$ into the product of linear factors.
- If $K \subset F$ is an algebraic extension generated by elements $\alpha_i \in F$, the requirement is that the minimal polynomial of each α_i has no multiple roots and splits in $F[x]$ into the product of linear factors.
- If $[F : K] < \infty$ and $F \subset \bar{K}$ then the requirement is that there exists exactly $[F : K]$ homomorphisms $\sigma : F \to \bar{K}$ over K (that is such that $\sigma|_K = \mathrm{Id}\,|_K$), and the image of each of them is F.

DEFINITION 2.3.2. Let $K \subset F$ is a field extension. The *Galois group* $\mathrm{Gal}(F/K)$ as the group of all automorphisms $\sigma : F \to F$ such that $\sigma|_K = \mathrm{Id}\,|_K$.

COROLLARY 2.3.3. *Let $K \subset F$ be a finite Galois extension with a Galois group $G = \mathrm{Gal}(F/K)$. Then $|G| = [F : K]$*

Proof. We embed F into the algebraic closure $\bar{K}$ of K. Since F/K is separable, the number of homomorphisms $F \to \bar{K}$ over K is equal to $[F : K]$. Since F/K is normal, the image of any such homomorphism is equal to F. Therefore, $|G| = [F : K]$. □

The Main Theorem of Galois Theory completely describes all intermediate subfields in the Galois extension.

THEOREM 2.3.4. *Let $K \subset F$ be a finite Galois extension with a Galois group $G = \mathrm{Gal}(F/K)$. Then there is an inclusion-reversing bijection*

$$\{\text{subgroups } H \subset G\} \leftrightarrow \{\text{subfields } K \subset L \subset F\}$$

Namely, a subgroup H corresponds to the subfield of invariants

$$L = F^H = \{\alpha \in F \mid h(\alpha) = \alpha \text{ for every } h \in H\}$$

and a subfield $K \subset L \subset F$ corresponds to a subgroup

$$H = \mathrm{Gal}(F/L) \subset \mathrm{Gal}(F/K) = G.$$

Along the way we we also prove

THEOREM 2.3.5 (Theorem on the Primitive Element). *Every finite separable extension L/K is simple: $L = K(\gamma)$ for some $\gamma \in L$.*

Proof. We start by proving one half of the Main Theorem. The first step is to show that $F^G = K$. Indeed, F^G is clearly a field and we have

$$K \subset F^G \subset F.$$

Since F/K is a Galois extension, F/F^G is a Galois extension as well. By Corollary 2.3.3, we have $|\mathrm{Gal}(F/F^G)| = [F : F^G]$. But

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

Indeed, any automorphism of F over K belongs to G and therefore fixes F^G. And since $K \subset F^G$, any automorphism of F over F^G fixes K. It follows that $[F : F^G] = [F : K] = |G|$ and so $F^G = K$.

The second step is to take an intermediate subfield $K \subset L \subset F$. We map it to a subgroup $H = \mathrm{Gal}(F/L) \subset \mathrm{Gal}(F/K) = G$. The first step (applied to the extension $L \subset F$) implies that $F^H = L$. It follows that the map

$$\{K \subset L \subset F\} \to \{H \subset G\}$$

is one-to-one. In particular, there are finitely many intermediate subfields.

The third step is to prove the Theorem on the Primitive element. Let L/K be a finite separable extension. Write $L = K(\alpha_1, \ldots, \alpha_s)$. Let $F \supset L$ be a splitting field of the least common multiple of minimal polynomials of $\alpha_1, \ldots, \alpha_s$. Then F/K is a Galois extension and therefore has finitely many intermediate subfields by the second step. It follows that the number of intermediate subfields of L/K is also finite. Now it is clear how to choose a primitive element:

- If K is an infinite field, take $\gamma \in L$ to be any element not in the union of these intermediate subfields.
- If K is finite, take $\gamma \in L$ to be a generator of the cyclic group L^*.

And the fourth, and final, step is to show that $\mathrm{Gal}(F/F^H) = H$ for every subgroup $H \subset G$. This will show that two functions in the statement of the theorem are inverses of each other. This fact follows from Lemma 2.3.6. □

LEMMA 2.3.6. *Let F be any field and let G be a finite group of its automorphisms. Then F/F^G is a finite Galois extension with Galois group G.*

Proof. Let $\alpha \in F$ and consider its G-orbit

$$G \cdot \alpha = \{\alpha_1, \ldots, \alpha_r\} \quad \text{with} \quad \alpha = \alpha_1.$$

Consider the polynomial

$$f(x) = \prod_{i=1}^{r} (x - \alpha_r).$$

By Vieta formulas, its coefficients are elementary symmetric functions in $\alpha_1, \ldots, \alpha_r$. These coefficients don't change when we permute $\alpha_1, \ldots, \alpha_r$, therefore, they are G-invariant. It follows that $f(x) \in F^G[x]$.

Since the minimal polynomial of α over F^G divides $f(x)$, α is separable over F^G. Therefore F/F^G is separable.

Since all roots of the minimal polynomial of α are among $\{\alpha_1, \ldots, \alpha_r\}$, the extension F/F^G is normal. Therefore, F/F^G is a Galois extension. Clearly, $G \subset \mathrm{Gal}(F/F^G)$. To show that $G = \mathrm{Gal}(F/F^G)$, it suffices to show that $[F : F^G] \leq |G|$. Take any intermediate subfield $F^G \subset L \subset F$ such that $[L : F_G] < \infty$. By the Theorem on the Primitive Element, $L = F^G(\alpha)$ for some α. By the analysis above, the minimal polynomial of α has degree at most $|G|$, and therefore $[L : F^G] = [F^G(\alpha) : F^G] \leq |G|$. This implies that $[F : F^G] \leq |G|$. Indeed, suppose $\alpha_1, \ldots, \alpha_r \in F$ are linearly independent. Take $L = K(\alpha_1, \ldots, \alpha_r)$. Then $[L : K] < \infty$ and by the above $[L : K] \leq |G|$. Therefore, $r \leq |G|$. □

COROLLARY 2.3.7. *Let $H \subset G$ and let $L = F^H$ be the corresponding subfield. Then H is a normal subgroup of G if and only if L/K is a normal field extension. In this case* $\mathrm{Gal}(L/K) \simeq G/H$.

Proof. Suppose L/K is a normal extension. Then any automorphism of F over K preserves L, i.e. we have a "restriction" homomorphism

$$\mathrm{Gal}(F/K) \to \mathrm{Gal}(L/K).$$

Its kernel is obviously $\mathrm{Gal}(F/L)$. The restriction homomorphism is onto because any automorphism of L/K can be extended to an automorphism of F/K by normality of the latter extension.

In the other direction, suppose L/K is not a normal extension. Then there exists $g \in G$ such that $g(L) \neq L$. It is easy to check that gHg^{-1} is a Galois group of $F/g(L)$. Since $g(L) \neq L$, it follows by the main theorem of Galois theory that $H \neq gHg^{-1}$, i.e. H is not normal. □

REMARK 2.3.8. A simple fact that we will exploit a lot in calculations is that if F is a splitting field of a polynomial $f(x) \in K[x]$ then $\mathrm{Gal}(F/K)$ is isomorphic to a subgroup of the symmetric group permuting roots of $f(x)$.

EXAMPLE 2.3.9. Let's completely analyze "from scratch" the field extension

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3}).$$

We have an intermediate subfield $\mathbb{Q}(\sqrt{2})$ of degree 2 over $\mathbb{Q}$ and it is elementary to check that $\sqrt{3}$ is not contained in this subfield. It follows that $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ has degree 4 over $\mathbb{Q}$ and is a splitting field of the polynomial

$(x^2-2)(x^2-3)$. In particular, this extension is Galois. Let G be the Galois group. Then

$$|G| = [\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = 4$$

and G permutes roots of $(x^2-2)(x^2-3)$. But not in an arbitrary way: G can only permute roots of x^2-2 (resp. x^2-3) among themselves because these polynomials are minimal polynomials of $\sqrt{2}$ (resp. $\sqrt{3}$). So we see that

$$G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2.$$

It sends $\sqrt{2}$ to $\pm\sqrt{2}$ and $\sqrt{3}$ to $\pm\sqrt{3}$. The group G contains three proper subgroups: H_1 fixes $\sqrt{2}$, H_2 fixes $\sqrt{3}$, and H_3 can only change the sign of $\sqrt{2}$ and $\sqrt{3}$ simultaneously. But then H_3 fixes $\sqrt{6} = \sqrt{2}\sqrt{3}$. So there are exactly 3 intermediate subfields: $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, and $\mathbb{Q}(\sqrt{6})$.

Take an element $\sqrt{2}+\sqrt{3}$. Let $f(x)$ be its minimal polynomial. The Galois group G permutes the roots of $f(x)$. So these roots must be $\pm\sqrt{2} \pm \sqrt{3}$. In particular, $f(x)$ has degree 4, and therefore $\sqrt{2}+\sqrt{3}$ is a primitive element:

$$\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3}).$$

§2.4. **Fields of invariants.**

DEFINITION 2.4.1. Whenever a group G acts on a field K (resp. a ring R) by automorphisms, we say that K^G (resp. R^G) is the *field of invariants* (resp. the *ring of invariants*) of G.

EXAMPLE 2.4.2. The symmetric group S_n acts on the field of rational functions $K = k(x_1,\dots,x_n)$ by permuting variables. By Lemma 2.3.6, K/K^{S_n} is a Galois extension with a Galois group S_n. It is clear that K^{S_n} contains elementary symmetric functions

$$\sigma_1 = \sum_i x_i, \quad \sigma_2 = \sum_{i<j} x_i x_j, \quad \dots, \quad \sigma_n = \prod_i x_i.$$

So $K^G \supset k(\sigma_1,\dots,\sigma_n)$. By the Vieta theorem, $k(x_1,\dots,x_n)$ is a splitting field over $k(\sigma_1,\dots,\sigma_n)$ of the polynomial

$$(x-x_1)\dots(x-x_n) = x^n - \sigma_1 x^{n-1} + \dots + (-1)^n\sigma_n$$

without multiple roots. It follows that $k(x_1,\dots,x_n)/k(\sigma_1,\dots,\sigma_n)$ is a Galois extension. Let G be its Galois group. Since G acts faithfully on the set of roots of the polynomial above, we have $|G| \le n!$. On the other hand,

$$|G| = [k(x_1,\dots,x_n) : k(\sigma_1,\dots,\sigma_n)] \ge [k(x_1,\dots,x_n) : k(x_1,\dots,x_n)^{S_n}] = n!$$

Therefore, $G = S_n$ and $K^G = k(\sigma_1,\dots,\sigma_n)$. In other words, any symmetric rational function can be expressed in terms of elementary symmetric functions.

Later on we will extend this theorem to polynomial functions:

THEOREM 2.4.3 (Theorem on Symmetric Polynomials). *Let*

$$k[x_1,\dots,x_n]^{S_n} \subset [x_1,\dots,x_n]$$

be a subring of all polynomials invariant under permutations of variables. Then

$$k[x_1,\dots,x_n]^{S_n} = k[\sigma_1,\dots,\sigma_n].$$

§2.5. **Exercises.**

Homework 2

We fix a finite field extension $K \subset F$. We also assume that $F \subset \bar{K}$.

1. Let $\alpha \in F$ and let $f(x)$ be its minimal polynomial over K. Show that there exists $k \geq 0$ such that all roots of $f(x)$ in $\bar{K}$ have multiplicity p^k and α^{p^k} is separable over K.

2. (a) Show that elements of F separable over K form a field L (called a *separable closure* of K in F). We define

$$[F : K]_s := [L : K].$$

(b) Show that the separable closure of L in F is equal to L. (b) Prove that the number of different homomorphisms $F \to \bar{K}$ over K is equal to $[F : K]_s$.

3. An extension F/K is called *purely inseparable* if $[F : K]_s = 1$. Show that F/K is purely inseparable if and only if $\operatorname{char} K = p$ and F is generated over K by elements $\alpha_1, \ldots, \alpha_r$ such that the minimal polynomial of each α_i has the form $x^{p^{k_i}} - a_i$ for some $a_i \in K$ and a positive integer k_i.

4. Let $L = \bar{\mathbb{F}}_p(x, y)$ be the field of rational functions in two variables and let $K = \bar{\mathbb{F}}_p(x^p, y^p)$ be its subfield. (a) Show that L/K is an algebraic extension and compute its degree. (b) Show that there exist infinitely many pairwise different intermediate subfields between K and L. (c) Show that L cannot be expressed as $K(\alpha)$ for some $\alpha \in L$.

5. A field k is called *perfect* if either $\operatorname{char} k = 0$ or $\operatorname{char} k = p$ and the Frobenius homomorphism $F : k \to k$ is an isomorphism. Show that if k is perfect then any algebraic extension of k is separable over k and perfect.

6. Let F be a splitting field of the polynomial $f \in K[x]$ of degree n. Show that $[F : K]$ divides $n!$ (do not assume that F is separable over K).

7. Let $F \subset \bar{K}$ be a finite Galois extension of K and let $L \subset \bar{K}$ be any finite extension of K. Consider the natural K-linear map $L \otimes_K F \to \bar{K}$. (a) Show that its image is a field, in fact a composite field LF. (b) Show that LF is Galois over L. (c) Show that $\operatorname{Gal}(LF/L)$ is isomorphic to $\operatorname{Gal}(F/L \cap F)$.

8. (a) Find the minimal polynomial over $\mathbb{Q}$ of $\sqrt[2]{3} + \sqrt[3]{3}$. (b) Compute the Galois group of its splitting field.

9. Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of prime degree p. Suppose that $f(x)$ has exactly $p - 2$ real roots. Show that the Galois group of the splitting field of $f(x)$ is S_p.

10. For any $d \geq 2$, prove existence of an irreducible polynomial in $\mathbb{Q}[x]$ of degree d with exactly $d - 2$ real roots (Hint: take some obvious reducible polynomial with exactly $d - 2$ real roots and perturb it a little bit to make it irreducible).

11. Let G be any finite group. Show that there exist finite extensions $\mathbb{Q} \subset K \subset F$ such that F/K is a Galois extension with a Galois group G.

12. Let F be a splitting field of the polynomial $f(x) \in K[x]$. Show that $\operatorname{Gal} F/K$ acts transitively on roots of $f(x)$ if and only if $f(x)$ is irreducible (do not assume that $f(x)$ is separable).

13. Let F be a splitting field of a biquadratic polynomial $x^4 + ax^2 + b \in K[x]$. Show that $\operatorname{Gal}(F/K)$ is isomorphic to a subgroup of D_4.

§3. First Applications of Galois Theory

§3.1. **Translations from group theory to Galois theory.** Any statement about finite groups can be translated into a statement about fields. For example,

PROPOSITION 3.1.1. *Let F/K be a finite Galois extension of degree n. Let p be a prime number. Then*

(a) *There exists an intermediate subfield $K \subset L \subset F$ such that $[L : K]$ is coprime to p and $[F : L]$ is a power of p.*
(b) *If $n = p^k$ then there exists an intermediate subfield $K \subset L \subset F$ such that L/K is Galois of degree p^{k-1} and $[F : L] = p$.*

Proof. Let G be the Galois group of F over K. In part (a), let $H \subset G$ be a p-Sylow subgroup and take $L = F^H$. In part (b), let $H \subset G$ be a cyclic group of order p contained in the center of G. (Why does it exist?) Take $L = F^H$. Since H is normal in G, L/K is Galois. □

§3.2. **Fundamental Theorem of Algebra.**

THEOREM 3.2.1. *$\mathbb{C}$ is algebraically closed.*

Proof. Since we are in $\mathrm{char} = 0$, all field extensions are separable. It suffices to show (why?) that any finite Galois extension K of $\mathbb{R}$ is either $\mathbb{R}$ or $\mathbb{C}$. We argue by induction on $[K : \mathbb{R}]$. If $[K : \mathbb{R}] = 1$ then $K = \mathbb{R}$ and there is nothing to prove. Suppose that $[K : \mathbb{R}] > 1$. By Proposition 3.1.1, we can find an intermediate subfield $\mathbb{R} \subset L \subset K$ such that $[L : \mathbb{R}]$ is odd and $[K : L]$ is a power of 2. Let $\alpha \in L$. Then the minimal polynomial of α in $\mathbb{R}[x]$ is an irreducible polynomial of odd degree. But any odd degree polynomial in $\mathbb{R}[x]$ has a real root (this is the only place where we use analysis). Therefore $L = \mathbb{R}$ and therefore $[K : \mathbb{R}]$ is a power of 2. By Proposition 3.1.1, we can find an intermediate subfield $\mathbb{R} \subset L \subset K$ such that $L/\mathbb{R}$ is Galois and $[K : L] = 2$. By inductive assumption, L is equal to $\mathbb{R}$ or to $\mathbb{C}$.

Finally, K/L is a quadratic extension. By the quadratic formula, any quadratic polynomial in $\mathbb{C}[x]$ splits and any quadratic polynomial in $\mathbb{R}[x]$ has a complex root. Therefore, $L = \mathbb{R}$ and $K = \mathbb{C}$. □

§3.3. **Quadratic extensions.** Suppose $[F : K] = 2$. Since 2 is prime, we have $F = K(\alpha)$ for any $\alpha \in F \setminus K$ by multiplicativity of degree. Let $f \in K[x]$ be the minimal polynomial of α. We have $f(x) = (x - \alpha)(x - \beta)$ in $\bar{K}$.

Case 0. F/K is unseparable. This happens if and only if $\mathrm{char}\, K = 2$ and $f(x) = x^2 - a$ for $a \in K$. One example is $\mathbb{F}_2(t^2) \subset \mathbb{F}_2(t)$.

Case 1. F/K is separable, i.e. α and β are different. Since $\alpha + \beta \in K$ by Vieta's formulas, F/K is normal and therefore Galois. The Galois group is $\mathbb{Z}_2$ (the only group of order 2). It permutes α and β. Now suppose that $\mathrm{char}\, K \neq 2$. Then an element $d = \alpha - \beta$ is not Galois-invariant. Therefore $d \notin K$ by the MTGT. Notice that $D = d^2$ is $\mathbb{Z}_2$-invariant, and therefore $D \in K$. So $F = K(d) = K(\sqrt{D})$. D is of course just the discriminant: if $f(x) = x^2 + bx + c$ then

$$(\alpha - \beta)^2 = (\alpha + \beta)^2 - 4\alpha\beta = b^2 - 4c.$$

§3.4. **Cubic extensions.** Let F/K be a cubic extension, i.e. $[F : K] = 3$. Since 3 is prime, we have $F = K(\alpha)$ for any $\alpha \in F \setminus K$ by multiplicativity of degree. Let $f \in K[x]$ be the minimal polynomial of α. We have $f(x) = (x - x_1)(x - x_2)(x - x_3)$ in $\bar{K}$, here $\alpha = x_1$.

Case 0. F/K is unseparable. This happens if and only if $\operatorname{char} K = 3$ and $f(x) = x^3 - a$ for $a \in K$. One example is $\mathbb{F}_3(t^3) \subset \mathbb{F}_3(t)$.

Let's suppose that F/K is separable, i.e. x_1, x_2, x_3 are different. There are two possibilities:

Case A. F/K is normal, i.e. $f(x)$ splits in F. In this case F/K is Galois with Galois group $\mathbb{Z}_3$ (the only group of order 3). 3 is a prime number, so there are no intermediate subfields between K and F. One example of this situation is $\mathbb{F}_3 \subset \mathbb{F}_{27}$. As a subgroup of S_3, the Galois group $\mathbb{Z}_3 \simeq A_3$ and permutes roots $\{x_1, x_2, x_3\}$ cyclically.

Case B. F/K is not normal, i.e. $f(x)$ does not split in F. In this case F/K is not Galois. One example is $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$. Let $L \subset \bar{K}$ be the splitting field of $f(x)$. Then L/K is Galois. Let $G = \operatorname{Gal}(L/K)$ be the Galois group. Since G acts on $\{x_1, x_2, x_3\}$, we have $|G| \leq 3! = 6$. On the other hand, $[L : K] \geq 2[F : K] = 6$. So in fact $[L : K] = 6$ and $G = S_3$.

The symmetric group S_3 has four proper subgroups: three subgroups generated by transpositions (ij) for $i < j$ and the alternating group A_3. By MTGT, L/K has four intermediate subfields. Since $\langle (ij) \rangle \simeq \mathbb{Z}_2$, we have $[F^{\langle (ij) \rangle} : K] = 6/2 = 3$. Since $x_k \in F^{\langle (ij) \rangle}$ for $k \neq i, j$, we have

$$F^{\langle (12) \rangle} = K(x_3), \quad F^{\langle (13) \rangle} = K(x_2), \quad F^{\langle (23) \rangle} = K(x_1).$$

Since $|A_3| = 3$, $[F^{A_3} : K] = 2$. To describe this field, let's assume that

$$\operatorname{char} K \neq 2.$$

Then the element

$$d = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3) \in F$$

is invariant under A_3 but not S_3. Therefore $d \in F^{A_3} \setminus K$ by the Main Theorem of Galois Theory. So we have

$$F^{A_3} = K(d).$$

Notice that $D = d^2$ is S_3-invariant, and therefore $D \in K$. Since $d \notin K$, D is not a square in K.

D is called the *discriminant* of $f(x)$. As a symmetric polynomial in roots, it can be expressed as a polynomial in coefficients of $f(x)$. Notice that $d \in K$ in Case A (because $F^{A_3} = K$), so in this case D is a square in K. We can summarize this discussion as follows:

PROPOSITION 3.4.1. *Let F/K be a cubic extension and let $f(x)$ be a minimal polynomial of $\alpha \in F \setminus K$. Let $D \in K$ be the discriminant of $f(x)$. Then*

- *if $D = 0$ then F/K is unseparable.*
- *if $D \in (K^*)^2$ and $\operatorname{char} K \neq 2$ then F/K is Galois.*
- *if $D \in K^* \setminus (K^*)^2$ then $\operatorname{char} K \neq 2$ and F/K is separable but not Galois.*

§3.5. **Galois group of a finite field.**

THEOREM 3.5.1. *$\mathbb{F}_{p^n}/\mathbb{F}_p$ is a Galois extension with Galois group*

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \simeq \mathbb{Z}_n.$$

$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is generated by the Frobenius map $F(x) = x^p$. Intermediate subfields L correspond to divisors k of n.

Proof. We already proved that $\mathbb{F}_{p^n}/\mathbb{F}_p$ is a splitting field of $f(x) = x^{p^n} - x$. Since $f'(x) = -1$, this extension is separable and therefore Galois. Since $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$, the Galois group G has order n. The Frobenius map is an element of G. If F has order d then $\alpha^{p^d} = \alpha$ for any $\alpha \in \mathbb{F}_{p^n}$. A polynomial can not have more roots than its degree, therefore $d = n$ and G is a cyclic group generated by F. Notice that subgroups $H \subset G$ correspond to divisors $k|n$. Namely, H is generated by F^k and has order n/k The last statement follows from MTGT. □

Notice that we have

$$(\mathbb{F}_{p^n})^H = \{\alpha \in \mathbb{F}_{p^n} \mid \alpha^{p^k} = \alpha\} = \mathbb{F}_{p^k}.$$

§3.6. **Exercises.**

Homework 3

1. Let $a, b \in K$ and suppose that $f(x) = x^3 + ax + b$ has no roots in K. Let F be a splitting field of $f(x)$. Assume that $\operatorname{char} K \neq 3$. Show that

$$\operatorname{Gal}(F/K) \simeq \begin{cases} S_3 & \text{if } -4a^3 - 27b^2 \text{ is not a square in } K \\ \mathbb{Z}_3 & \text{if } -4a^3 - 27b^2 \text{ is a square in } K \end{cases}$$

2. Let α be a real number such that $\alpha^4 = 5$. (a) Show that $\mathbb{Q}(i\alpha^2)$ is normal over $\mathbb{Q}$. (b) Show that $\mathbb{Q}(\alpha + i\alpha)$ is normal over $\mathbb{Q}(i\alpha^2)$. (c) Show that $\mathbb{Q}(\alpha + i\alpha)$ is not normal over $\mathbb{Q}$.

3. Consider a tower $K \subset L \subset F$. Suppose L/K and F/L are finite Galois extensions. Is it true that F/K is Galois?

4. Compute the Galois group of the polynomial (a) $x^3 - x - 1$ over $\mathbb{Q}(\sqrt{-23})$; (b) $x^3 - 2tx + t$ over $\mathbb{C}(t)$ (the field of rational functions in one variable).

5. Let L/K be a Galois extension with the Galois group S_6. (a) Find the number of intermediate subfields F between K and L such that $[L : F] = 9$. (b) Let M be the intersection of all fields F in part (a). Find $[M : K]$.

6. Let F/K be a finite Galois extension and let L be an intermediate subfield between F and K. Let H be the subgroup of $\operatorname{Gal}(F/K)$ mapping L to itself. Prove that H is the normalizer of $\operatorname{Gal}(F/L)$ in $\operatorname{Gal}(F/K)$.

7. Let $p_1, \ldots, p_r \in \mathbb{Z}$ be distinct primes and let

$$K = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_r}).$$

(a) For any non-empty subset $S \subset \{1, \ldots, r\}$, let $a_S = \prod_{i \in S} p_i$. Show that all $2^r - 1$ intermediate subfields of the form $\mathbb{Q} \subset \mathbb{Q}(\sqrt{a_S}) \subset K$ are different. (b) Compute the Galois group $\operatorname{Gal}(K/\mathbb{Q})$.

8. (continuation of the previous problem). Describe explicitly all intermediate subfields L such that either $[L : \mathbb{Q}] = 2$ or $[K : L] = 2$.

9. Let $K \subset L \subset \bar{K}$ and suppose that L/K is separable. Show that there exists the unique minimal (by inclusion) Galois extension F/K such that $L \subset F \subset \bar{K}$. Show that if L/K is finite then F/K is finite. F is called the *Galois closure of L in $\bar{K}$*.

10. Let F/K be a finite Galois extension with a Galois group G. Let $H \subset G$ be a subgroup and let $L = F^H$. Let $N = \bigcap_{g \in G} gHg^{-1}$. Characterize the field F^N in terms of the tower $K \subset L \subset F$.

11. Let F/K be a finite Galois extension with a Galois group G. Let $H \subset G$ be a subgroup and let $L = F^H$. Show that the number of fields of the form $g(L)$ for $g \in G$ is equal to $\frac{|G|}{|N_G(H)|}$.

12. Let $\mathbb{F}_{p^n}$ be a finite field with p^n elements and let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be the Frobenius map, $F(x) = x^p$. Show that F is diagonalizable (as an $\mathbb{F}_p$-linear operator) if and only if n divides $p - 1$.

13. Let F/K be a splitting field of a polynomial $f(x) = (x - a_i) \ldots (x - a_r) \in K[x]$ without multiple roots. Let

$$\Delta = \prod_{1 \leq i < j \leq n} (a_i - a_j)^2$$

be the discriminant of $f(x)$. (a) Show that $\Delta \in K$. (b) Let $G \subset S_n$ be the Galois group of F/K acting on roots of $f(x)$. Suppose $\operatorname{char} K \neq 2$. Show that $G \subset A_n$ if and only if Δ is a square in K. (c) Let $F = \mathbb{C}(x_1, \ldots, x_n)$ be the field of rational functions in n variables. Suppose A_n acts on F by even permutations of variables. Show that F^{A_n} is generated over $\mathbb{C}$ by elementary symmetric functions $\sigma_1, \ldots, \sigma_n$ in variables $x_1, \ldots, x_n$ and by $\sqrt{\Delta}$.

14. Let G be a subgroup of the group of automorphisms of $\mathbb{C}(z)$ (rational functions in one variable) generated by automorphisms $z \mapsto 1 - z$ and $z \mapsto 1/z$. Show that G has 6 elements and that the field of invariants $\mathbb{C}(z)^G$ is generated by one function. Find this function.

15. Compute the Galois group of the polynomial $x^4 - 4x^2 - 1$ over $\mathbb{Q}$.

16. Suppose $f(x) \in \mathbb{Q}[x]$ is an irreducible polynomial such that one of its complex roots has absolute value 1. Show that $f(x)$ has even degree and is palindromic: if $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ then $a_0 = a_n$, $a_1 = a_{n-1}$, etc.

17. Suppose $\operatorname{char} K \neq 2$ and let $f(x) \in K[x]$ be an irreducible polynomial of degree 5 such that its discriminant is a square in K^*. Find all possible Galois groups for its splitting field.

§4. Adjoining Radicals

§4.1. **Adjoining roots of unity.**

Definition 4.1.1. Let $\phi(n) = |\mathbb{Z}_n^*|$ be the *Euler function*, i.e. the number of elements in $\mathbb{Z}_n$ coprime to n.

Proposition 4.1.2. *Suppose n is coprime to $\operatorname{char} K$. Let F/K be the splitting field of $x^n - 1$ (in which case we say that F is obtained from K by adjoining n-th roots of unity). Then $[F : K]$ divides $\phi(n)$ and $\operatorname{Gal}(F/K)$ is isomorphic to a subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$.*

Proof. Consider

$$\mu_n = \{\alpha \in F \mid \alpha^n = 1\}.$$

Notice that μ_n is cyclic (as any finite subgroup in the multiplicative group of a field) and has order n, Indeed, since n is coprime to $\operatorname{char} K$,

$$(x^n - 1, nx^{n-1}) = 1.$$

It follows that $x^n - 1$ has no multiple roots. Let $G = \operatorname{Gal}(F/K)$. Since F is the splitting field of $x^n - 1$, G acts faithfully on μ_n. Since any element of G is an automorphism of F, the action of G on μ_n preserves multiplication. So G is isomorphic to a subgroup of

$$\operatorname{Aut}(\mu_n) \simeq \operatorname{Aut}(\mathbb{Z}_n) \simeq \mathbb{Z}_n^*,$$

which has $\phi(n)$ elements. In particular, $[F : K] = |G|$ divides $\phi(n)$. □

§4.2. **Cyclotomic fields.**

Now we explore the case $K = \mathbb{Q}$. Let $\zeta_n \in \mathbb{C}$ be a primitive n-th root of unity, for example we can take $\zeta_n = e^{2\pi i/n}$. Since any n-th root of 1 is a power of ζ_n, the splitting field of $x^n - 1$ is equal to $\mathbb{Q}(\zeta_n)$.

Definition 4.2.1. $\mathbb{Q}(\zeta_n)$ is called the *cyclotomic field* (Etymology: cyclotomy is the process of dividing the circle into equal parts, from cycl- + -tomy).

Theorem 4.2.2. *Let $\zeta = \zeta_n$. The cyclotomic field $\mathbb{Q}(\zeta)$ has degree $\phi(n)$ over $\mathbb{Q}$. The Galois group of $\mathbb{Q}(\zeta)/\mathbb{Q}$ is isomorphic to $\mathbb{Z}_n^*$. The minimal polynomial of ζ is*

$$\Phi_n(x) = \prod_{\substack{0<k<n \\ (k,n)=1}} (x - \zeta^k)$$

(the cyclotomic polynomial). We have $x^n - 1 = \prod_{d|n} \Phi_d$.

Proof. Let $f(x)$ be the minimal polynomial of ζ. We know by Prop. 4.1.2 that $\deg f = [\mathbb{Q}(\zeta) : \mathbb{Q}]$ divides $\phi(n)$ and that $\operatorname{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \subset \mathbb{Z}_n^*$.

Claim 4.2.3. *$f(\zeta^k) = 0$ whenever $(k, n) = 1$.*

This implies that $f(x)$ has at least $\phi(n)$ roots, and therefore that

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg f(x) = \phi(n), \quad f(x) = \Phi_n(x), \quad \text{and} \quad \operatorname{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) = \mathbb{Z}_n^*.$$

Proof of the Claim. If p is a prime divisor of k then $\zeta^k = (\zeta^{k/p})^p$ and $\zeta^{k/p}$ is also a primitive n-th root of unity. Arguing by induction on k it suffices to show that $f(\zeta^p) = 0$ if p is prime (and does not divide n). Arguing by contradiction, suppose that $f(\zeta^p) \neq 0$. We have a factorization

$$x^n - 1 = f(x)g(x).$$

Since $f(\zeta^p) \neq 0$, $g(\zeta^p) = 0$. It follows that ζ is a root of $g(x^p)$. Therefore,

$$g(x^p) = f(x)h(x). \tag{4.2.1}$$

By Gauss lemma, polynomials $f(x)$, $g(x)$, and $h(x)$ all have integer coefficients. So we can reduce (4.2.1) modulo p:

$$\begin{aligned} g(x^p) &\equiv f(x)h(x) \mod p \\ &\equiv g(x)^p \mod p \qquad \text{(Frobenius!)} \end{aligned} \tag{4.2.2}$$

Let $\bar{f}(x)$ and $\bar{g}(x)$ be polynomials in $\mathbb{Z}_p[x]$ obtained by reducing $f(x)$ and $g(x)$ modulo p. By (4.2.2) $\bar{f}(x)$ divides $\bar{g}(x)^p$, and therefore $\bar{f}(x)$ and $\bar{g}(x)$ are not coprime. Therefore, $x^n - 1 = \bar{f}(x)\bar{g}(x)$ has a multiple root in some finite field $\mathbb{F}_{p^l}$. But since $(p, n) = 1$, $(nx^{n-1}, x^n - 1) = 1$, and therefore $x^n - 1$ has no multiple roots in $\mathbb{F}_{p^l}$. This is a contradiction. □

§4.3. **Cyclic extensions.** Any quadratic extension F/K (if $\operatorname{char} K \neq 2$) can be obtained by simply adding a quadratic root (of the discriminant)

$$F = K(\sqrt{D}).$$

It turns out that a similar description is available for any Galois extension with a cyclic Galois group:

THEOREM 4.3.1. *Fix $n \geq 2$. Suppose that $\operatorname{char} K$ does not divide n and that K contains all n-th roots of 1.*

- *Let $\alpha \in \bar{K}$ be a root of $x^n - a$ for some $a \in K$. Then $K(\alpha)/K$ is Galois, and the Galois group is cyclic of order d, where $d|n$ and $\alpha^d \in K$.*
- *If F/K is a Galois extension with a cyclic Galois group of order n then $F = K(\alpha)$ for some $\alpha \in F$ such that $\alpha^n \in K$.*

Proof. Let $\zeta \in K$ be a primitive n-th root of 1.

One direction is easy. Let α be a root of $x^n - a$ for some $a \in K$. Then $\zeta^k\alpha$ is also a root for any $1 \leq k \leq n-1$. It follows that $x^n - a$ splits in $K(\alpha)$. Since all the roots are distinct, we see that $K(\alpha)/K$ is Galois. Let G be the Galois group. For any $g \in G$, we have $g\alpha = \zeta^k\alpha$ for some unique $k \in \mathbb{Z}/n\mathbb{Z}$. This gives an injective homomorphism

$$G \to \mathbb{Z}/n\mathbb{Z}, \quad g \mapsto k.$$

Therefore, G is cyclic of order $d|n$. Let σ be a generator. Then $\sigma(\alpha) = \nu\alpha$, where $\nu^d = 1$. We have

$$\sigma(\alpha^d) = [\sigma(\alpha)]^d = \nu^d\alpha^d = \alpha^d.$$

It follows that $\alpha^d \in K$ by the Main Theorem of Galois Theory.

Now let's prove a less obvious implication. Let F/K be a Galois extension with a cyclic Galois group G of order n. Let σ be a generator of the Galois group. It suffices to prove the following:

CLAIM 4.3.2. *There exists $\alpha \in F^*$ such that $\sigma(\alpha) = \zeta\alpha$.*

Indeed, given the Claim, the G-orbit of α is

$$\{\alpha, \quad \sigma(\alpha) = \zeta\alpha, \quad \sigma^2(\alpha) = \zeta^2\alpha, \quad \ldots, \ \sigma^{n-1}(\alpha) = \zeta^{n-1}\alpha\}.$$

Since G acts transitively on the set of roots of the minimal polynomial of α, we see that this minimal polynomial is equal to

$$f(x) = (x - \alpha)(x - \zeta\alpha) \dots (x - \zeta^{n-1}\alpha).$$

In particular, $[K(\alpha) : K] = n$, and therefore $K(\alpha) = F$. Finally,

$$\sigma(\alpha^n) = \zeta^n \alpha^n = \alpha^n,$$

and therefore $\alpha^n = a \in K$ by the Main Theorem of Galois Theory (it also follows that $f(x) = x^n - a$).

It remains to prove the Claim. We have a K-linear operator $\sigma : F \to F$ such that $\sigma^n = \mathrm{Id}$ and we are trying to find an eigenvector for σ with an eigenvalue ζ. We give two proofs.

Proof A. Since $\sigma^n = \mathrm{Id}$, the minimal polynomial of σ (viewed as a K-linear operator) divides $T^n - 1$. By our assumptions, the latter polynomial is separable and splits over K. Therefore, σ is diagonalizable over K. We claim that all eigenvalues are different. Equivalently, all n-th roots of 1 appear as eigenvalues. Equivalently, any two eigenvectors with the same eigenvector are linearly dependent. Indeed, suppose $x, y \in F \setminus \{0\}$ are eigenvectors with the same eigenvalue ν. Then

$$\sigma(x/y) = \sigma(x)/\sigma(y) = (\nu x)/(\nu y) = x/y.$$

It follows that x/y is G-invariant, and therefore belongs to K by MTGT. Therefore, x and y are linearly dependent and we are done.

For practical purposes, it would be nice to find a way to produce eigenvectors explicitly. Lagrange has discovered a nice trick for doing this.

Proof B. Consider the following K-linear operator on F:

$$A = \mathrm{Id} + \zeta^{-1}\sigma + \ldots + \zeta^{-(n-1)}\sigma^{n-1}.$$

By Lemma 4.4.1 below, this operator is not identically 0. Let $\beta \in F$ be any element such that $\alpha := A(\beta) \neq 0$. Then

$$\alpha = \beta + \zeta^{-1}\sigma(\beta) + \ldots + \zeta^{-(n-2)}\sigma^{n-2}(\beta) + \zeta^{-(n-1)}\sigma^{n-1}(\beta) \qquad (4.3.1)$$

and

$$\sigma(\alpha) = \sigma(\beta) + \zeta^{-1}\sigma^2(\beta) + \ldots + \zeta^{-(n-2)}\sigma^{n-1}(\beta) + \zeta^{-(n-1)}\sigma^n(\beta) =$$
$$= \zeta\beta + \sigma(\beta) + \zeta^{-1}\sigma^2(\beta) + \ldots + \zeta^{-(n-2)}\sigma^{n-1}(\beta) = \zeta\alpha.$$

We are done! □

§4.4. **Artin's Lemma.**

LEMMA 4.4.1 (Artin).

(1) *Take a field extension F/K and let $\sigma_1, \ldots, \sigma_r$ be different automorphisms of F over K. Let $\alpha_1, \ldots, \alpha_r \in F$ and consider the following K-linear operator $A : F \to F$:*

$$A = \alpha_1\sigma_1 + \ldots + \alpha_r\sigma_r.$$

If $A = 0$ then $\alpha_1 = \ldots = \alpha_r = 0$.

(2) *In fact, more is true: let F be a field, let Γ be a group, and let $\sigma_i : \Gamma \to F^*$, for $i \in I$, be different homomorphisms. Then they are linearly independent over F: if $\alpha_1\sigma_1 + \ldots + \alpha_r\sigma_r = 0$ as a function $\Gamma \to F$ for some $\alpha_1, \ldots, \alpha_r \in F$ then in fact $\alpha_1 = \ldots = \alpha_r = 0$.*

Proof. The first part follows from the second part by taking $\Gamma = F^*$ (any automorphism $F \to F$ obviously induces a multiplicative homomorphism $F^* \to F^*$). To prove the second part, suppose we have a relation

$$\alpha_1\sigma_1 + \ldots + \alpha_r\sigma_r = 0. \tag{4.4.1}$$

We can assume that r is the minimal possible. Then $r \geq 2$ and $\alpha_i \neq 0$ for any i. Since σ_1, σ_2 are different, there exists $z \in \Gamma$ such that $\sigma_1(z) \neq \sigma_2(z)$. Then we have

$$\alpha_1\sigma_1(xz) + \ldots + \alpha_r\sigma_r(xz) = 0$$

for any $x \in \Gamma$, and therefore

$$\alpha_1\sigma_1(z)\sigma_1 + \ldots + \alpha_r\sigma_r(z)\sigma_r = 0$$

is *another* linear relation on our homomorphisms. We subtract it from (4.4.1) multiplied by $\sigma_1(z)$, which gives

$$\alpha_2(\sigma_1(z) - \sigma_2(z))\sigma_2 + \alpha_3(\sigma_1(z) - \sigma_3(z))\sigma_3 + \ldots = 0.$$

Since $\sigma_1(z) \neq \sigma_2(z)$, this is a non-trivial relation. But it has fewer than r terms, a contradiction. □

§4.5. **Norm and Trace.**

DEFINITION 4.5.1. Let F/K be a separable extension of degree n (not necessarily Galois) and let $\sigma_1, \ldots, \sigma_n : F \to \bar{K}$ be the set of all embeddings over K. Let $\alpha \in F$. We define its *trace*

$$\mathrm{Tr}_{F/K}(\alpha) = \sigma_1(\alpha) + \ldots + \sigma_n(\alpha)$$

and *norm*

$$N_{F/K}(\alpha) = \sigma_1(\alpha) \ldots \sigma_n(\alpha).$$

EXAMPLE 4.5.2. We have $N_{\mathbb{C}/\mathbb{R}}(a + ib) = (a + ib)(a - ib) = a^2 + b^2$.

One has to be careful: the norm and the trace depend on the extension F/K and not just on $\alpha \in F$. But this dependence is easy to understand:

LEMMA 4.5.3. *Let F/K and L/F be separable extensions and let $\alpha \in F$. Then*

$$\mathrm{Tr}_{L/K}(\alpha) = [L : F]\,\mathrm{Tr}_{F/K}(\alpha) \quad \text{and} \quad N_{L/K}(\alpha) = N_{F/K}(\alpha)^{[L:F]}.$$

Proof. Any embedding $L \to \bar{K}$ over K is an extension of some embedding $\sigma : F \to \bar{K}$. By separability, there are $[L : F]$ possible extensions. □

As a consequence of Artin's Lemma 4.4.1, we see that

COROLLARY 4.5.4. *The trace $\mathrm{Tr}_{F/K}(\alpha) \neq 0$ for some $\alpha \in F$.*

There are two simple ways to compute the trace and the norm:

LEMMA 4.5.5. *Let $\alpha \in \bar{K}$ be a separable element with the minimal polynomial $f(x) = x^k + a_1x^{k-1} + \ldots + a_k$. Then*

$$\mathrm{Tr}_{K(\alpha)/K}(\alpha) = -a_1 \quad \text{and} \quad N_{K(\alpha)/K}(\alpha) = (-1)^k a_k.$$

The trace gives an additive homomorphism $\mathrm{Tr}_{F/K} : F \to K$. The norm gives a multiplicative homomorphism $N_{F/K} : F^* \to K^*$.

Proof. Notice that embeddings $K(\alpha) \to \bar{K}$ just send α to all possible roots of $f(x)$. So the lemma follows from Vieta formulas. □

LEMMA 4.5.6. *Let $\alpha \in F$ and let A be a K-linear operator $F \to F$ of left multiplication by α. Then $\mathrm{Tr}_{F/K}(\alpha) = \mathrm{Tr}(A)$ and $N_{F/K}(\alpha) = \det(A)$.*

Proof. Let $e_1, \ldots, e_r$ be a basis of F over $K(\alpha)$. Then as a K-vector space, F is a direct sum of vector subspaces

$$F = K(\alpha)e_1 \oplus \ldots \oplus K(\alpha)e_r.$$

Choosing a basis of F compatible with this decomposition, we see that the matrix of A in this basis is block-diagonal with $r = [F : K(\alpha)]$ blocks, where each block is a matrix of the left multiplication by α in $K(\alpha)$. So it suffices to prove the lemma for the extension $K(\alpha)/K$. In this case we choose a basis $1, \alpha, \ldots, \alpha^{k-1}$ of $K(\alpha)$, where $k = [K(\alpha) : K]$. Let $f(x) = x^k + a_1 x^{k-1} + \ldots + a_k$ be the minimal polynomial of α. The matrix of A in this basis is

$$\begin{bmatrix} 0 & 0 & \ldots & 0 & -a_k \\ 1 & 0 & \ldots & 0 & -a_{k-1} \\ 0 & 1 & \ldots & 0 & \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & -a_1 \end{bmatrix}$$

So we are done by Lemma 4.5.5. □

§4.6. **Lagrange resolvents.** Suppose that $\mathrm{char}\, K$ does not divide n and that K contains all n-th roots of 1. Let F/K be a Galois extension with a cyclic Galois group of order n. Let σ be a generator. As we have seen before, $F = K(\alpha)$ for some $\alpha \in F$ such that $\alpha^n \in K$. Moreover, α can be computed as the following expression, called the *Lagrange resolvent*:

$$E_\zeta(\beta) = \beta + \zeta^{-1}\sigma(\beta) + \ldots + \zeta^{-(n-2)}\sigma^{n-2}(\beta) + \zeta^{-(n-1)}\sigma^{n-1}(\beta).$$

Let's push this a little bit further. As a function of β, $E_\zeta(\beta)$ is an K-linear function on F. We can define $E_{\zeta^k}(\beta)$ for any $0 \le k < n$ in the same way. For example, $E_1(\beta) = \beta + \sigma(\beta) + \ldots + \sigma^{n-1}(\beta)$. Artin's Lemma tells us that each of these resolvents is not equal to zero (for some β). This gives

COROLLARY 4.6.1. *The action of σ on F (viewed as a K-vector space) is diagonalizable with eigenvalues $1, \zeta, \ldots, \zeta^{n-1}$ and eigenvectors given by Lagrange resolvents.*

In fact, it is possible to show that we can use Lagrange resolvents *with the same β*. To see this, let's introduce a basis of F as a K-vector space and the corresponding coordinates $x_1, \ldots, x_n$. The function

$$E_1(\beta)E_\zeta(\beta)\ldots E_{\zeta^{n-1}}(\beta)$$

then can be viewed as an L-valued polynomial of degree n in n variables. Let's assume for simplicity that K is an infinite field. Then this polynomial function does not vanish for some K-values of x_i's, i.e. for some β. It follows that we can find $\beta \in F$ such that

$$E_1(\beta), E_\zeta(\beta), \ldots, E_{\zeta^{n-1}}(\beta)$$

are non-zero eigenvectors for σ with eigenvalues $1, \zeta, \ldots, \zeta^{n-1}$. It also follows that vectors

$$\beta, \sigma(\beta), \ldots, \sigma^{n-1}(\beta)$$

are linear independent. In fact, their linear independence is equivalent to linear independence of Lagrange resolvents because the transition matrix between the two systems of vectors is the Vandermonde matrix

$$\begin{bmatrix} 1 & 1 & \dots & 1 \\ 1 & \zeta & \dots & \zeta^{n-1} \\ 1 & \zeta^2 & \dots & \zeta^{2(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta^{n-1} & \dots & \zeta \end{bmatrix}$$

with non-zero determinant.

We proved the special case of the following quite general

THEOREM 4.6.2 (Normal Basis Theorem). *Let F/K be a finite Galois extension of degree n with the Galois group $G = \{e = \sigma_0, \sigma_1, \dots, \sigma_{n-1}\}$. Then there exists $\beta \in F$ such that elements*

$$\beta = \sigma_0(\beta), \sigma_1(\beta), \dots, \sigma_{n-1}(\beta)$$

form a basis of F over K.

The proof is not hard and can be found in Lang's "Algebra".

§4.7. **Solvable extensions: Galois Theorem.** Galois discovered his theory while trying to prove that a general quintic equation $x^5 + a_1x^4 + \ldots + a_5 = 0$ is not solvable in radicals. He showed that equations solvable in radicals are precisely equations given by polynomials with solvable Galois groups (hence the name: solvable group).

In this section we will assume for simplicity that

$$\operatorname{char} K = 0.$$

Alternatively, one can assume that all extensions we consider are separable and their degrees are not divisible by characteristic.

DEFINITION 4.7.1. Let F/K be a finite field extension.

- The extension F/K is called *solvable* if there exists a Galois extension L/K containing F with a solvable Galois group.
- The extension F/K is *solvable in radicals* if there exists a tower

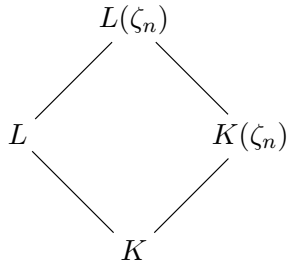
$$K = L_0 \subset L_1 \subset \ldots \subset L_r$$

such that $F \subset L_r$ and such that $L_i = L_{i-1}(\sqrt[n_i]{a_i})$ for some $a_i \in L_{i-1}$.

THEOREM 4.7.2. *F/K is solvable if and only if it is solvable in radicals.*

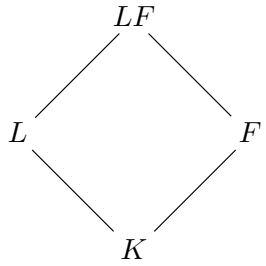
Proof. All fields appearing in the proof will be subfields of the fixed algebraic closure $\bar{K}$. Let F/K be a solvable extension. Let L/K be the Galois extension containing F with a solvable Galois group G of size n.

Let $K(\zeta_n)$ be the splitting field of $x^n - 1$. Consider the diagram of fields



By the next Lemma (proved in the homework), $L(\zeta_n)/K(\zeta_n)$ is a Galois extension and its Galois group H is isomorphic to $\mathrm{Gal}(L/L \cap K(\zeta_n))$. The latter group is a subgroup of G. So H is solvable.

LEMMA 4.7.3. *Let $L \subset \bar{K}$ be a finite Galois extension of K and let $F \subset \bar{K}$ be any finite extension of K. Consider the diagram of field extensions*



Then the composite field LF is Galois over F and the Galois group $\mathrm{Gal}(LF/F)$ is isomorphic to $\mathrm{Gal}(L/L \cap F)$.

A cyclic tower of subgroups

$$H = H_1 \supset H_2 \supset \ldots \supset H_r = \{e\}$$

gives rise to a tower of subfields

$$K(\zeta_n) = J_1 \subset J_2 \subset \ldots \subset J_r = L(\zeta_n),$$

where

$$J_i = L(\zeta_n)^{H_i}.$$

By the Main Theorem of Galois theory, $L(\zeta_n)/J_i$ is Galois with a Galois group H_i. Since H_{i+1} is normal in H_i, J_{i+1}/J_i is a Galois extension with Galois group H_i/H_{i+1}, which is cyclic.

Since J_{i+1}/J_i is a cyclic extension of degree $d|n$ (by Lagrange Theorem), and J_i contains n-th roots of unity, we can apply Theorem 4.3.1. We see that on each step $J_{i+1} = J_i(\alpha)$, where some power of α belongs to J_{i-1}. It follows that F/K is solvable in radicals.

Conversely, suppose F/K is solvable in radicals, i.e. F is contained in a field L that admits a tower

$$K \subset L_1 \subset \ldots \subset L_r = L$$

such that on each step $L_i = L_{i-1}(\alpha)$, where $\alpha^k \in L_{i-1}$ for some k. Let n be the l.c.m. of k's that appear. Consider the tower of fields

$$K \subset K(\zeta_n) \subset L_1(\zeta_n) \subset \ldots \subset L_r(\zeta_n) = M,$$

where each consecutive embedding is Galois with an Abelian Galois group on the first step (by Theorem 4.1.2) and a cyclic Galois group for the remaining steps (by Theorem 4.3.1). However, we are not quite done yet because M/K is not necessarily Galois.

Let $g_1, \ldots, g_k : M \to \bar{K}$ be the list of all embeddings over K, where g_1 is the identity. Each of the embeddings $g_i(M) \subset \bar{K}$ has the same property as above: in the corresponding tower

$$K \subset g_i(K(\zeta_n)) \subset g_i(L_1(\zeta_n)) \subset \ldots \subset g_i(M), \tag{4.7.1}$$

each consecutive embedding is Galois with an Abelian Galois group. Notice that the composite field $\mathcal{M} = g_1(M) \ldots g_k(M)$ is Galois over K and admits a tower of field extensions

$$K \subset g_1(M) \subset g_1(M)g_2(M) \subset \ldots \subset g_1(M) \ldots g_k(M) = \mathcal{M}$$

Consider the i-th step of this tower

$$N \subset Ng_i(M),$$

where $N = g_1(M) \ldots g_{i-1}(M)$. We can refine this inclusion of fields by taking a composite of (4.7.1) with N. By Lemma 4.7.3, each consecutive embedding in this mega-tower is Galois with an Abelian Galois group. By the Main Theorem of Galois Theory, this tower of subfields of $\mathcal{M}$ corresponds to an Abelian filtration of $\mathrm{Gal}(\mathcal{M}/K)$. Therefore this group is solvable. $\square$

DEFINITION 4.7.4. A polynomial $f \in K[x]$ is called

- *solvable* if its Galois group is solvable.
- *solvable in radicals* if for any root β of $f(x)$ in $\bar{K}$ there exists a tower

$$K = L_0 \subset L_1 \subset \ldots \subset L_r$$

such that $\beta \in L_r$ and such that $L_i = L_{i-1}(\sqrt[n_i]{a_i})$ for some $a_i \in L_{i-1}$.

Theorem 4.7.2 implies that these two notions are equivalent. For example, a sufficiently general polynomial $f(x) \in \mathbb{Q}[x]$ of degree n has Galois group S_n, and therefore is not solvable for $n > 4$. On the other hand, any equation of degree at most 4 is solvable in radicals because its Galois group is a subgroup of S_4, and the latter group is solvable. The proof of the Galois theorem on solvable extensions is constructive, so one can actually "solve" solvable extensions. Let's consider an equation of degree 3:

$$x^3 + a_1x^2 + a_2x + a_3 = 0 \in K[x].$$

Since we are going to apply the Galois theorem, let's assume right away that K contains a primitive cubic root of unity ω and that $\mathrm{char}\, K \neq 2, 3$.

Lets make an unnecessary but classical change of variables $x \mapsto x - a_1/3$. This kills a_1, which simplifies calculations, So we can assume that

$$a_1 = 0.$$

Let F be the splitting field. In this field

$$f(x) = (x - x_1)(x - x_2)(x - x_3).$$

Let $G = \mathrm{Gal}(F/K) \subset S_3$. A cyclic filtration $\{e\} \subset A_3 \subset S_3$ gives a cyclic filtration

$$\{e\} \subset A_3 \cap G \subset G$$

and the corresponding tower

$$F \supset F^{A_3 \cap G} \supset K.$$

The extension $F/F^{A_3 \cap G}$ has Galois group $A_3 \cap G \subset \mathbb{Z}/3\mathbb{Z}$ which acts by cyclically permuting the roots $x_1 \to x_2 \to x_3 \to x_1$. Let's write down all Lagrange resolvents:

$$\begin{aligned} E_1 &= x_1 + x_2 + x_3 \\ E_\omega &= x_1 + \omega^2 x_2 + \omega x_3 \\ E_{\omega^2} &= x_1 + \omega x_2 + \omega^2 x_3 \end{aligned}$$

It suffices to derive formulas for the Lagrange resolvents, since then we can compute the roots x_1, x_2, x_3 by solving a system of linear equations. By Vieta formulas, we have

$$E_1 = -a_1 = 0$$

and so it suffices to compute

$$E_\omega^3,\ E_{\omega^2}^3 \in F^{A_3 \cap G}.$$

The extension $F^{A_3 \cap G}/K$ is cyclic with a Galois group contained in $S_3/A_3 \simeq \mathbb{Z}/2\mathbb{Z}$: this quotient group is generated by a transposition σ that exchanges $x_2 \leftrightarrow x_3$. By our general recipe, instead of computing E_ω^3 and $E_{\omega^2}^3$ directly, we want to compute their Lagrange resolvents

$$E_\omega^3 \pm \sigma(E_\omega^3) \quad \text{and} \quad E_{\omega^2}^3 \pm \sigma(E_{\omega^2}^3),$$

which have the property that their squares belong to K. Then we compute E_ω^3 and $E_{\omega^2}^3$ by solving a system of linear equation.

Here the calculation is simplified by the fact that

$$\sigma(E_\omega^3) = E_{\omega^2}^3.$$

So the Lagrange resolvents for the second step are simply

$$E_\omega^3 \pm E_{\omega^2}^3.$$

It remains to compute these resolvents and then to solve the system of two linear equations in two variables to find E_ω^3 and $E_{\omega^2}^3$. Note that $E_\omega^3 + E_{\omega^2}^3$ is invariant under σ, i.e. it is in fact a symmetric polynomial in x_1, x_2, x_3, i.e. it should be possible to express it in terms of coefficients of $f(x)$. A little calculation shows that

$$E_\omega^3 + E_{\omega^2}^3 = -27a_3.$$

A square of $E_\omega^3 - E_{\omega^2}^3$ should also be invariant, in fact we have

$$(E_\omega^3 - E_{\omega^2}^3)^2 = 27(4a_2^3 + 27a_3^2) = -27\Delta^2,$$

where D is the discriminant. Backtracking through this calculation gives formulas for roots of the cubic equation discovered by the Italian mathematician Niccolò Tartaglia.

§4.8. **Exercises.**

Homework 4

1. Compute $\Phi_5(x)$, $\Phi_8(x)$, $\Phi_{12}(x)$.

2. Let n and m be coprime integers. Show that $\Phi_n(x)$ (the n-th cyclotomic polynomial) is irreducible over $\mathbb{Q}(\zeta_m)$.

3. If $\cos\frac{2\pi m}{n} \in \mathbb{Q}$ then it is equal to 1, $\frac{1}{2}$, 0, $-\frac{1}{2}$, or -1.

4. Find all angles $\theta \in \mathbb{Q}\pi$ such that $\cos(\theta)$ can be written as $a + b\sqrt{D}$, where $a, b \in \mathbb{Q}$ and $D \in \mathbb{Z}$ is square-free. Find a and b for each θ.

5. Let

$$\alpha_r = \sqrt{2 + \sqrt{2 + \sqrt{2 + \ldots + \sqrt{2}}}} \qquad (r \text{ nested radicals}).$$

(a) Show that the minimal polynomial $f_r(x) \in \mathbb{Q}[x]$ of α_r can be computed recursively as follows: $f_r(x) = f_{r-1}(x^2-2)$, where $f_1(x) = x^2-2$. (b) Describe all roots of $f_r(x)$ in terms of cosines of various angles. (c) Show that $\mathbb{Q}(\alpha_r)/\mathbb{Q}$ is a Galois extension and compute its Galois group.

6. Let G be a finite Abelian group. (a) Show that there exists a positive square-free integer n and a subgroup $\Gamma \subset \mathbb{Z}_n^*$ such that $G \simeq \mathbb{Z}_n^*/\Gamma$. (b) Show that there exists a Galois extension $K/\mathbb{Q}$ with a Galois group G. (One of the most famous open problems, the inverse problem of Galois Theory, is to prove the same statement for any finite group G).

7. Let $f(x) \in \mathbb{Z}[x]$, $\deg(f) > 0$. Show that the reduction of $f(x)$ modulo p has a root in $\mathbb{F}_p$ for infinitely many primes p. [Hint: if $f(x) = x$, your argument should become the Euclid's argument for the infinitude of primes.]

8. Let $\Phi_n(x)$ be the n-th cyclotomic polynomial, a a non-zero integer, p a prime. Assume that p does not divide n. Prove that $\Phi_n(a) \equiv 0 \mod p$ if and only if a has order n in $(\mathbb{Z}/p\mathbb{Z})^*$.

9. Fix an integer $n > 1$. Use the previous two exercises to show[2] that there exist infinitely many primes p such that $p \equiv 1 \mod n$.

10. Let F/K be a Galois extension with a cyclic Galois group G of order p, where $\operatorname{char} K = p$. Let σ be a generator of G. (a) Show that there exists $\alpha \in F$ such that $\sigma(\alpha) = \alpha + 1$. (b) Show that $F = K(\alpha)$, where α is a root of $x^p - x - a$ for some $a \in K$.

11. Suppose that $\operatorname{char} K = p$ and let $a \in K$. Show that the polynomial $x^p - x - a$ either splits in K or is irreducible. Show that in the latter case its Galois group is cyclic of order p.

12. Let $\alpha = \sqrt{2 + \sqrt{7}}$. Compute the rational number $N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)$.

13. Let F/K be a Galois extension with a cyclic Galois group G. Let σ be a generator of G. Show that

$$\operatorname{Ker}[\operatorname{Tr}_{F/K}] = \operatorname{Im}[\operatorname{Id}_F - \sigma].$$

In other words, if $\beta \in F$ then $\operatorname{Tr}_{F/K}(\beta) = 0$ iff $\beta = \alpha - \sigma(\alpha)$ for some $\alpha \in F$.

14. Let F/K be a Galois extension with a cyclic Galois group G. Let σ be a generator of G. Let $\beta \in F$. (a) There exists $\theta \in F$ such that $\alpha \neq 0$, where

$$\alpha = \theta + \beta\sigma(\theta) + \beta\sigma(\beta)\sigma^2(\theta) + \beta\sigma(\beta)\sigma^2(\beta)\sigma^3(\theta) + \ldots + \beta\sigma(\beta)\ldots\sigma^{n-2}(\beta)\sigma^{n-1}(\theta).$$

[2] This proof is due to J. Sylvester. The result is a special case of the Dirichlet's theorem on primes in arithmetic progressions: for any coprime integers a and n, there exist infinitely many primes p such that $p \equiv a \mod n$. The proof uses complex analysis.

(b) Show that $N_{F/K}(\beta) = 1$ if and only if $\beta = \alpha/\sigma(\alpha)$ for some $\alpha \in F^*$.

15. Let $K = \mathbb{Q}(\zeta)$, where ζ is a primitive n-th root of unity. Show that if $n = p^r$ for some prime p then $N_{K/\mathbb{Q}}(1 - \zeta) = p$.

§5. Quadratic Extensions of $\mathbb{Q}$

§5.1. **Quadratic case of the Kronecker–Weber theorem.** The role of cyclotomic fields can only be fully appreciated because of the following theorem

THEOREM 5.1.1 (Kronecker–Weber). *Any Galois extension $K/\mathbb{Q}$ with an Abelian Galois group is contained in some cyclotomic field $\mathbb{Q}(\zeta_n)$.*

This remarkable theorem is very difficult, and attempts to generalize it to Abelian extensions of other fields of algebraic numbers led to the development of Class Field Theory (and then to the modern Langlands program). We will prove the easiest case, first observed by Gauss.

THEOREM 5.1.2. *Any quadratic extension $K/\mathbb{Q}$ is contained in some $\mathbb{Q}(\zeta_n)$.*

We will need the following definition:

DEFINITION 5.1.3. Let p be an odd prime. Since $\mathbb{F}_p^*$ is a cyclic group of even order, we have

$$\mathbb{F}_p^*/(\mathbb{F}_p^*)^2 \simeq \{\pm 1\}.$$

The induced homomorphism

$$\mathbb{F}_p^* \twoheadrightarrow \{\pm 1\}, \quad \nu \mapsto \left(\frac{\nu}{p}\right)$$

is called the *quadratic (or Legendre) symbol*. Concretely, $\left(\frac{\nu}{p}\right)$ is equal to 1 if ν is a square in $\mathbb{F}_p$ and -1 otherwise. The quadratic symbol is obviously multiplicative (being a homomorphism):

$$\left(\frac{\nu}{p}\right)\left(\frac{\nu'}{p}\right) = \left(\frac{\nu\nu'}{p}\right).$$

Proof of Theorem 5.1.2. Every quadratic extension of $\mathbb{Q}$ has the form $\mathbb{Q}(\sqrt{n})$, where n is a square-free integer. Let $n = \pm p_1 \dots p_r$ be the prime decomposition. It's clear that if $\sqrt{p_i} \in \mathbb{Q}(\zeta_{l_i})$ for every i then $\sqrt{n} \in \mathbb{Q}(\zeta_{4l_1\dots l_r})$. So it suffices to show that if p is prime then $\sqrt{p} \in \mathbb{Q}(\zeta_n)$ for some n.

The case $p = 2$ is easy:

$$\sqrt{2} = 2\cos \pi/4 = \zeta_8 + \zeta_8^{-1}.$$

Suppose now that p is odd. Let $\zeta = \zeta_p$ and consider the *Gauss sum*

$$S = \sum_{\nu \in \mathbb{F}_p^*} \left(\frac{\nu}{p}\right) \zeta^\nu \in \mathbb{Q}(\zeta).$$

CLAIM 5.1.4 (Gauss).

$$S^2 = \left(\frac{-1}{p}\right) p$$

Given the claim, $\sqrt{p} \in \mathbb{Q}(\zeta_p)$ if $(\frac{-1}{p}) = 1$ and $i\sqrt{p} \in \mathbb{Q}(\zeta_p)$ if $(\frac{-1}{p}) = -1$. In the latter case $\sqrt{p} \in \mathbb{Q}(\zeta_{4p})$ (because $i \in \mathbb{Q}(\zeta_4)$). The theorem is proved. $\square$

Proof of the Claim 5.1.4. This is one long ingenious calculation

$$S^2 = \sum_{\nu,\mu\in\mathbb{F}_p^*} \left(\frac{\nu}{p}\right)\left(\frac{\mu}{p}\right)\zeta^{\nu+\mu} = \sum_{\nu,\mu\in\mathbb{F}_p^*} \left(\frac{\nu\mu}{p}\right)\zeta^{\nu+\mu} =$$

(a neat trick to replace ν with $\nu\mu$ for any fixed $\mu \in \mathbb{F}_p^*$)

$$= \sum_{\nu,\mu\in\mathbb{F}_p^*} \left(\frac{\nu\mu^2}{p}\right)\zeta^{\nu\mu+\mu} =$$

(multiplicativity of the quadratic symbol)

$$= \sum_{\nu,\mu\in\mathbb{F}_p^*} \left(\frac{\nu}{p}\right)\zeta^{\mu(\nu+1)} =$$

(separate the cases $\nu = -1$ and $\nu \neq -1$)

$$= \sum_{\mu\in\mathbb{F}_p^*} \left(\frac{-1}{p}\right)\zeta^0 + \sum_{\nu\neq -1} \left(\frac{\nu}{p}\right) \sum_{\mu\in\mathbb{F}_p^*} \zeta^{\mu(\nu+1)} =$$

$$\left(\frac{-1}{p}\right)(p-1) - \sum_{\nu\neq -1} \left(\frac{\nu}{p}\right) + \sum_{\nu\neq -1} \left(\frac{\nu}{p}\right) \sum_{\mu\in\mathbb{F}_p} \zeta^{\mu(\nu+1)} =$$

(it is easy to see (why?) that $\sum\limits_{\mu\in\mathbb{F}_p} (\zeta^{\nu+1})^\mu = 0$)

$$= \left(\frac{-1}{p}\right)(p-1) - \sum_{\nu\neq -1} \left(\frac{\nu}{p}\right) =$$

$$= p\left(\frac{-1}{p}\right) - \sum_{\nu\in\mathbb{F}_p} \left(\frac{\nu}{p}\right) = p\left(\frac{-1}{p}\right).$$

Indeed, it is clear (why?) that $\sum\limits_{\nu\in\mathbb{F}_p} \left(\frac{\nu}{p}\right) = 0$. This proves the Claim. □

§5.2. **Integral extensions.** To go forward, we have to extend the notion of "algebraic extension" to commutative rings. All rings in this section are commutative, with 1.

DEFINITION 5.2.1. Let $R \subset S$ be rings.

- An element $\alpha \in S$ is called *integral over* R if there exists a monic polynomial $f \in R[x]$ such that $f(\alpha) = 0$.
- The ring S is called *integral over* R if every $\alpha \in S$ is integral over R.
- The *integral closure* of R in S is the set of all elements $\alpha \in S$ integral over R.
- The ring R is called *integrally closed in* S if R is equal to its integral closure in S.
- Let R be an integral domain. Its integral closure in the field of fractions K is called a *normalization* or an *integral closure* of R.
- An integral domain R is called *normal* or *integrally closed* if R is equal to its integral closure in the field of fractions K of R.

Most of the results in this section about integral extensions S/R of rings are proved analogously to the corresponding results about algebraic extensions F/K of fields with "finite-dimensional K-vector space" substituted for "finitely generated R-module".

Here is the main technical result:

THEOREM 5.2.2. *Let $R \subset S$ be rings. Let $\alpha \in S$. Then TFAE:*

(1) *α is integral over R.*
(2) *$R[\alpha] \subset S$ is a finitely generated R-module.*
(3) *$\alpha \in T$ for some subring $T \subset S$ that is a finitely generated R-submodule.*

Proof. $(1) \Rightarrow (2)$. There exists a monic polynomial $f(x) \in R[x]$ of degree n such that $f(\alpha) = 0$. It follows that $\alpha^n \in R + R\alpha + \ldots + R\alpha^{n-1}$. Arguing by induction on k, we see that $\alpha^k \in R + R\alpha + \ldots + R\alpha^{n-1}$ for all $k \geq n$. It follows that

$$R[\alpha] = R + R\alpha + \ldots + R\alpha^{n-1}$$

is finitely generated as an R-module.

$(2) \Rightarrow (3)$. Take $T = R[\alpha]$.

$(3) \Rightarrow (1)$. If R is Noetherian then we can repeat the argument we used for fields. Indeed, in this case T, being a finitely generated R-module, satisfies ACC for submodules. So if we denote $M_k \subset T$ to be an R-submodule generated by $1, \alpha, \ldots, \alpha_k$ then $M_{n-1} = M_n$ for some n, i.e. $\alpha^n \in M_{n-1}$. This shows that α is integral over R.

In general, one can use the following trick. Let $e_1, \ldots, e_m$ be generators of the R-module T. For every i we can write

$$\alpha e_i = \sum_j a_{ij} e_j \quad \text{for some } a_{ij} \in R.$$

This implies

$$Ae_j = 0 \quad \text{for any } j,$$

where A is the matrix $[\alpha\delta_{ij} - a_{ij}]$. Multiplying this identity by the adjoint matrix of A on the left gives

$$(\det A)e_j = 0 \quad \text{for any } j.$$

Since $1 \in T$, we can write 1 as an R-linear combination of $e_1, \ldots, e_m$. This implies $\det A = 0$. Therefore α is a root of the monic polynomial $f(x) = \det[x\delta_{ij} - a_{ij}]$, i.e. the characteristic polynomial of $[a_{ij}]$. □

LEMMA 5.2.3. *Consider rings $R \subset S \subset T$. If S is a finitely generated R-module and T is a finitely generated S-module then T is a finitely generated R-module.*

Proof. If $\{e_i\}$ generate S as an R-module and $\{f_j\}$ generate T as an S-module then and $\{e_i f_j\}$ generate T as an R-module. □

LEMMA 5.2.4. *Consider rings $R \subset S$ and suppose $\alpha_1, \ldots, a_s \in S$ are integral over R. Then $R[\alpha_1, \ldots, \alpha_s]$ is a finitely generated R-module.*

Proof. Let

$$R_0 = R, \quad R_i = R[\alpha_1, \ldots, \alpha_i] \quad \text{for } i = 1, \ldots, s.$$

Since α_i is integral over R, it is aposteriori integral over R_{i-1} as well for every $i = 1, \ldots, s$. It follows that R_i is a finitely-generated R_{i-1}-module

for every $i = 1, \ldots, s$. Applying Lemma 5.2.3 inductively shows that $R_s = R[\alpha_1, \ldots, \alpha_s]$ is a finitely generated R-module. $\square$

COROLLARY 5.2.5. *Suppose $R \subset T \subset S$, T is integral over R, and $\alpha \in S$ is integral over T. Then α is integral over R.*

Proof. There exists a monic polynomial $f(x) = x^n + a_1 x^{n-1} + \ldots + a_n \in T[x]$ such that $f(\alpha) = 0$. Therefore α is integral over $R[a_1, \ldots, a_n]$. Therefore $R[\alpha, a_1, \ldots, a_n]$ is a finitely generated $R[a_1, \ldots, a_n]$-module. On the other hand, since $a_1, \ldots, a_n$ are integral over R, Lemma 5.2.4 shows that $R[a_1, \ldots, a_n]$ is a finitely-generated R-module. Therefore $R[\alpha, a_1, \ldots, a_n]$ is a finitely generated R-module. So α is integral over R. $\square$

COROLLARY 5.2.6. *The integral closure of R in S is a ring. This ring is integrally closed in S.*

Proof. Let $\alpha, \beta \in S$ be integral over R. Then $R[\alpha, \beta]$ is a finitely generated R-module by Lemma 5.2.4. Since $\alpha + \beta, \alpha\beta \in R[\alpha, \beta]$, we can apply Theorem 5.2.2 (3) to conclude that $\alpha + \beta$, $\alpha\beta$ are integral over R. Therefore, the integral closure T of R in S is a ring.

It remains to show that T is integrally closed. Suppose $\alpha \in S$ is integral over T. By Corollary 5.2.5, α is integral over R. Therefore $\alpha \in T$. $\square$

An important example:

THEOREM 5.2.7. *Any UFD R is integrally closed in its field of fractions K.*

Proof. Take $\alpha = p/q \in K$, where $p, q \in R$ and we can assume that they are coprime. Suppose α is integral over R. Then $f(\alpha) = 0$ for some monic polynomial $f(x) = x^n + a_1 x^{n-1} + \ldots + a_n \in R[x]$. Therefore

$$p^n + a_1 p^{n-1} q + a_2 p^{n-2} q^2 + \ldots + a_n q^n = 0$$

and so $q | p^n$. Since p and q are coprime, it follows that q is a unit in R, i.e. $\alpha \in R$. So R is integrally closed in K. $\square$

REMARK 5.2.8. Applying this argument to $R = \mathbb{Z}$ gives the standard proof of the "rational roots" theorem: a rational root of a monic integral polynomial is in fact an integer.

COROLLARY 5.2.9. $\mathbb{Z}[\zeta_p] \cap \mathbb{Q} = \mathbb{Z}$.

Proof. Suppose $\alpha \in \mathbb{Z}[\zeta_p] \cap \mathbb{Q}$. Since ζ_p is a root of a monic polynomial $x^p - 1 \in \mathbb{Z}[x]$, it is integral over $\mathbb{Z}$. Therefore, $\mathbb{Z}[\zeta_p]$ is integral over $\mathbb{Z}$. Therefore α is integral over $\mathbb{Z}$. But $\mathbb{Z}$ is a UFD, so it is integrally closed in $\mathbb{Q}$. Since $\alpha \in \mathbb{Q}$ is integral over $\mathbb{Z}$, we see that in fact $\alpha \in \mathbb{Z}$. $\square$

We can also now prove Theorem 2.4.3:

COROLLARY 5.2.10 (Theorem on Symmetric Polynomials).

$$k[x_1, \ldots, x_n]^{S_n} = k[\sigma_1, \ldots, \sigma_n].$$

Proof. From Example 2.4.2 we already know that

$$k(x_1, \ldots, x_n)^{S_n} = k(\sigma_1, \ldots, \sigma_n).$$

So it suffices to show that

$$k[x_1, \ldots, x_n] \cap k(\sigma_1, \ldots, \sigma_n) = k[\sigma_1, \ldots, \sigma_n].$$

Suppose $\alpha \in k[x_1, \ldots, x_n] \cap k(\sigma_1, \ldots, \sigma_n)$. Since every x_i is a root of a monic polynomial $\prod(X - x_i) \in k[\sigma_1, \ldots, \sigma_n][X]$, every x_i is integral over $k[\sigma_1, \ldots, \sigma_n]$. Therefore, $k[x_1, \ldots, x_n]$ is integral over $k[\sigma_1, \ldots, \sigma_n]$. Therefore α is integral over $k[\sigma_1, \ldots, \sigma_n]$. But $k[\sigma_1, \ldots, \sigma_n]$ is a polynomial ring in n variables[3]. So it is a UFD by the Gauss lemma. Therefore it is integrally closed in $k(\sigma_1, \ldots, \sigma_n)$. Since $\alpha \in k(\sigma_1, \ldots, \sigma_n)$ is integral over $k[\sigma_1, \ldots, \sigma_n]$, we see that in fact $\alpha \in k[\sigma_1, \ldots, \sigma_n]$. □

REMARK 5.2.11. In practice, there exists a simple algorithm to write any symmetric polynomial $f \in k[x_1, \ldots, x_n]^{S_n}$ as a polynomial in $\sigma_1, \ldots, \sigma_n$. This algorithm also proves that $k[x_1, \ldots, x_n]^{S_n} = k[\sigma_1, \ldots, \sigma_n]$ by "lexicographic induction". Order the variables $x_1 > x_2 > \ldots > x_n$ and then order all monomials in $k[x_1, \ldots, x_n]$ lexicographically. This is a total order. This also gives a partial order on $k[x_1, \ldots, x_n]$: we can compare two polynomials by comparing their leading monomials. If $f \in k[x_1, \ldots, x_n]^{S_n}$ has a leading monomial $ax_1^{k_1} \ldots x_n^{k_n}$ then it is easy to see that $k_1 \geq k_2 \geq \ldots \geq k_n$. Moreover, $f - a\sigma_1^{k_1-k_2}\sigma_2^{k_2-k_3} \ldots \sigma_n^{k_n}$ is also S_n-invariant and its leading monomial is smaller than the leading monomial of f.

§5.3. **Quadratic reciprocity.** The famous fact about quadratic symbols is

THEOREM 5.3.1 (Quadratic Reciprocity, or Gauss' *Theorema Aureum*).

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

whenever p and q are odd primes.

Along with multiplicativity of the quadratic symbol and the formula

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

(proved in the exercises), the reciprocity law can be used to quickly decide when a given number is a square modulo p.

Proof of the Quadratic Reciprocity. It is easy to check (see the exercises) that

$$\left(\frac{p}{q}\right) \equiv p^{\frac{q-1}{2}} \mod q.$$

By (5.1.4), we have

$$S^2 = p\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}p,$$

where S is the Gauss sum. So we have

$$S^{q-1} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}p^{\frac{q-1}{2}} \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right) \mod q,$$

[3]This is actually not quite obvious. We will see how to prove this carefully when we discuss transcendence degree, see Example 7.3.7.

where from now on we work in the ring $\mathbb{Z}[\zeta_p]$. So "$a \equiv b \mod q$" is just a notation for "$a - b \in (q)$". Since q is a prime number we have

$$S^q \equiv \sum_{\nu \in \mathbb{F}_p^*} \left(\frac{\nu}{p}\right)^q \zeta^{\nu q} \mod q$$

$$\equiv \sum_{\nu \in \mathbb{F}_p^*} \left(\frac{\nu}{p}\right) \zeta^{\nu q} \equiv \sum_{\nu \in \mathbb{F}_p^*} \left(\frac{\nu q}{p}\right) \left(\frac{q}{p}\right) \zeta^{\nu q} \equiv \left(\frac{q}{p}\right) S \mod q.$$

We can combine two formulas for S^q to get the quadratic reciprocity law, but we have to be careful because we are doing calculations in $\mathbb{Z}[\zeta_p]$ rather than in $\mathbb{Z}$. So far we have proved that

$$(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right) S \equiv \left(\frac{q}{p}\right) S \mod q$$

This implies

$$(-1)^{\frac{p-1}{2}\frac{q-1}{2}} S^2 - \left(\frac{q}{p}\right)\left(\frac{p}{q}\right) S^2 \equiv 0 \mod q,$$

i.e.

$$(-1)^{\frac{p-1}{2}\frac{q-1}{2}} S^2 - \left(\frac{q}{p}\right)\left(\frac{p}{q}\right) S^2 = qz,$$

where $z \in \mathbb{Z}[\zeta_p]$. Since $S^2 = \pm p$, z is obviously a rational number.

By Corollary 5.2.9, $\mathbb{Z}[\zeta_p] \cap \mathbb{Q} = \mathbb{Z}$. It follows that

$$(-1)^{\frac{p-1}{2}\frac{q-1}{2}} S^2 - \left(\frac{q}{p}\right)\left(\frac{p}{q}\right) S^2 \equiv 0 \mod q \quad \text{in } \mathbb{Z}.$$

Since $S^2 = \pm p$ and $(p, q) = 1$, we can cancel S^2. This shows that

$$(-1)^{\frac{p-1}{2}\frac{q-1}{2}} - \left(\frac{p}{q}\right)\left(\frac{q}{p}\right)$$

is divisible by q in $\mathbb{Z}$. Since its absolute value is at most 2, it is equal to 0. □

§5.4. **Some Examples of the Integral Closure.** One of the main goals of algebraic geometry is to build a vocabulary that relates geometric properties of a "space X" and algebraic properties of its "ring of functions $\mathcal{O}(X)$". For example, let's fix a field k and consider an affine space

$$X = \mathbb{A}^n.$$

Its *points* are just n-tuples $(a_1, \ldots, a_n) \in k^n$. And *functions* in algebraic geometry are just polynomial functions, so we define

$$\mathcal{O}(\mathbb{A}^n) := k[x_1, \ldots, x_n].$$

Let $X \subset \mathbb{A}^2$ be a cuspidal curve $y^2 = x^3$. Functions on it should be restrictions of polynomial functions, i.e. we should have a surjection

$$\mathcal{O}(\mathbb{A}^2) \to \mathcal{O}(X).$$

Its kernel should consists of all functions that vanish along the curve. This motivates the following definition:

$$\mathcal{O}(X) := k[x, y]/(y^2 - x^3).$$

Much less trivially, the fact that X is singular at the origin is related to the fact that $\mathcal{O}(X)$ is not integrally closed.

EXAMPLE 5.4.1. Let $R = k[x,y]/(y^2 - x^3)$. We have a homomorphism

$$\psi : k[x,y] \to k[t], \quad x \mapsto t^2,\ y \mapsto t^3.$$

The image is a subring $k[t^2, t^3]$ (polynomials in t without a linear term). Let I be the kernel. Clearly $(y^2 - x^3) \subset I$. We claim that in fact they are equal. Let $f(x,y) \in I$. Modulo $(y^2 - x^3)$, we can write

$$f(x,y) = a(x) + b(x)y.$$

So we have $a(t^2) + b(t^2)t^3 = 0$. Coefficients in a (resp. b) contribute only to even (resp. odd) degree monomials in t. So $a(x) = b(x) = 0$ and therefore $f(x,y) = 0$. So $(y^2 - x^3) = I$. By the first isomorphism theorem we have

$$R \simeq k[t^2, t^3],$$

in particular R is a domain. Notice that $t = t^3/t^2$ belongs to the field of fractions K of R. In particular, $K = k(t)$. Since $t \notin R$ but t is a root of the polynomial $T^2 - t^2 \in R[T]$, R is not integrally closed. We claim that its integral closure is $k[t] \subset K$. Indeed, $k[t]$ is integral over R. Also, $k[t]$ is a UFD and therefore integrally closed. So $k[t]$ is an integral closure of R.

Geometrically, the embedding of R into its integral closure $k[t]$ corresponds to parametrization of the cusp

$$\mathbb{A}^1 \to X, \quad t \mapsto (t^2, t^3),$$

which is an example of desingularization in algebraic geometry.

Examples of a different sort can be found in number theory.

DEFINITION 5.4.2. Let K be an algebraic extension of $\mathbb{Q}$. The integral closure of $\mathbb{Z}$ in K is called the *ring of algebraic integers* in K. Notation: $\mathcal{O}_K$.

EXAMPLE 5.4.3. Recall that $\mathbb{Z}[\sqrt{2}]$ is a PID and therefore a UFD. Therefore $\mathbb{Z}[\sqrt{2}]$ is algebraically closed in its field of fractions, which is $\mathbb{Q}(\sqrt{2})$. Also, $\sqrt{2}$ is obviously integral over $\mathbb{Z}$: it is a root of a monic polynomial $x^2 - 2$. So $\mathbb{Z}[\sqrt{2}]$ is an integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{2})$.

EXAMPLE 5.4.4. We claim that $\mathbb{Z}[\sqrt{5}]$ is not integrally closed in $\mathbb{Q}(\sqrt{5})$, and therefore an integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{5})$ is strictly larger than $\mathbb{Z}[\sqrt{5}]$. Indeed, the golden ratio $\frac{1+\sqrt{5}}{2}$ belongs to $\mathbb{Q}(\sqrt{5})$ and is integral over $\mathbb{Z}$: it is a root of a monic polynomial $x^2 - x - 1$.

THEOREM 5.4.5. *Let $K = \mathbb{Q}(\sqrt{D})$, where D is a square-free integer. Then*

$$\mathcal{O}_K = \mathbb{Z}[\omega],$$

where

$$\omega = \begin{cases} \sqrt{D} & \text{if } D = 2,3 \mod 4 \\ \frac{1+\sqrt{D}}{2} & \text{if } D = 1 \mod 4 \end{cases}$$

Proof. Since $\sqrt{D}$ is a root of $x^2 - D = 0$ and $\frac{1+\sqrt{D}}{2}$ is a root of $x^2 - x + \frac{1-D}{4} = 0$ (if $D \equiv 1 \mod 4$), we see that $\mathbb{Z}[\omega]$ is integral over $\mathbb{Z}$. It remains to show that if $\alpha = a + b\sqrt{D} \in \mathbb{Q}(\sqrt{D})$ is integral over $\mathbb{Z}$ then $\alpha \in \mathbb{Z}[\omega]$. Let $f(x)$ be the minimal polynomial of α over $\mathbb{Q}$. Since α is a root of a monic polynomial in $\mathbb{Z}[x]$, it follows, by Gauss lemma, that $f(x) \in \mathbb{Z}[x]$. If $b = 0$ then $a \in \mathbb{Z}$ because $\mathbb{Z}$ is integrally closed. So let's assume that $b \neq 0$. Then $f(x)$ has degree 2. Write $f(x) = x^2 - px + q$. The Galois group $\mathrm{Gal}\, K/\mathbb{Q}$ sends α to $a - b\sqrt{D}$. Therefore this is also a root of $f(x)$, and we have

$$p = 2a, \quad q = a^2 - b^2 D.$$

If $a \in \mathbb{Z}$ then $b^2 D \in \mathbb{Z}$, and, since D is square-free, $b \in \mathbb{Z}$ as well. In this case $\alpha \in \mathbb{Z}[\sqrt{D}]$. Since $a = p/2$ another possibility is that $a = a'/2$, where a' is an odd integer. Since $(a')^2 - 4b^2 D \in 4\mathbb{Z}$, we see that $4b^2 D \in (a')^2 + 4\mathbb{Z}$ and therefore that $4b^2 D \equiv 1 \mod 4$. It follows that $b = b'/2$, where b' is an odd integer. Therefore $\alpha \in \mathbb{Z}[\omega]$. □

REMARK 5.4.6. In this analysis we allow D to be be negative. For example, since $-1 \equiv 3 \mod 4$, we see that $\mathbb{Z}[i]$ is an integral closure of $\mathbb{Z}$ in $\mathbb{Q}(i)$. This also follows from the fact that $\mathbb{Z}[i]$ is a UFD. Another interesting example if $\mathbb{Z}[\sqrt{-5}]$. By the theorem above, this ring is integrally closed. However, it is not a UFD. Indeed, 6 has two different factorizations into irreducible elements:

$$(1 + \sqrt{-5})(1 - \sqrt{-5}) = 2 \cdot 3.$$

We should mention here a famous theorem of Heegner–Stark:

THEOREM 5.4.7. *Let $K = \mathbb{Q}(\sqrt{d})$, where d is a negative integer. Then $\mathcal{O}_K$ is a UFD if and only if*

$$d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}.$$

This was first conjectured by Gauss. On the other hand, it is not known how to classify UFDs of this form with $d > 0$.

§5.5. **Exercises.**

Homework 5

1. Show that a finite field extension F/K is solvable if and only if $\mathrm{Gal}\, L/K$ is solvable, where L is the Galois closure of F in $\bar{K}$.

2. Let p be a prime number and let $\zeta_p \in \mathbb{C}$ be a primitive p-th root of unity. Show that $\mathrm{Gal}(\mathbb{Q}(\zeta_p, \sqrt[p]{2})/\mathbb{Q})$ is a semidirect product of $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{F}_p^*$.

3. Suppose D_4 acts on $F = \mathbb{C}(x_1, \ldots, x_4)$ by permutations of variables (here we identify variables with vertices of the square). Show that F^{D_4} is generated over $\mathbb{C}$ by 4 rational functions.

4. Let M be a module over a ring R. A sequence of submodules

$$M = M_1 \supset M_2 \supset \ldots \supset M_r = 0$$

is called a *filtration* of M (of length r). A module M is called *simple* if it does not contain any submodules other than 0 and itself. A filtration is called simple if each M_i/M_{i+1} is simple. A module M is said to be of *finite length* if it admits a simple finite filtration. Two filtrations of M are called equivalent if they have the same length and the same collection of subquotients $\{M_1/M_2, M_2/M_3, \ldots, M_{r-1}/M_r\}$ (up to isomorphism and renumbering). Prove that if M has finite length then any two simple filtrations of M are equivalent and any filtration of M can be refined to a simple filtration.

5. (a) Let $f(x) \in K[x]$ be an irreducible separable polynomial with roots

$$\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n \in \bar{K}.$$

Suppose that there exist rational functions $\theta_1(x), \ldots, \theta_n(x) \in K(x)$ such that $\alpha_i = \theta_i(\alpha)$ for any i. Suppose also that

$$\theta_i(\theta_j(\alpha)) = \theta_j(\theta_i(\alpha))$$

for any i, j. Show that the Galois group of the splitting field of $f(x)$ is Abelian[4]. (b) Give an example of the situation as in part (a) with $K = \mathbb{Q}$ and such that the Galois group of $f(x)$ is not cyclic. Give a specific polynomial $f(x)$, and compute its roots and functions θ_i.

6. (a) Let $\bar{K}$ be an algebraic closure of K. Show that there exists the unique maximal (by inclusion) subfield $K \subset K^{ab} \subset \bar{K}$ such that K^{ab}/K is Galois and the Galois group $\mathrm{Gal}(K^{ab}/K)$ is Abelian. (b) Deduce from the Kronecker–Weber Theorem that

$$\mathbb{Q}^{ab} = \bigcup_{n \geq 1} \mathbb{Q}(\zeta_n).$$

7. Let $K = \mathbb{C}[z^{-1}, z]]$ be the field of Laurent series (series in z, polynomials in z^{-1}). Let $K_m = \mathbb{C}[z^{\frac{-1}{m}}, z^{\frac{1}{m}}]] \supset K$. (a) Show that K_m/K is Galois with a Galois group $\mathbb{Z}/m\mathbb{Z}$. (b) Show that any Galois extension F/K with a Galois group $\mathbb{Z}/m\mathbb{Z}$ is isomorphic to K_m. (c) Show that

$$K^{ab} = \bigcup_{m \geq 1} K_m,$$

the field of so called *Puiseux series*[5]

---

[4] This was proved by Abel himself.

[5] Sir Isaac Newton proved that the field of Puiseux series in in fact algebraically closed.

§6. Sample Midterm on Galois Theory

1. Let L/K be a finite Galois extension with Galois group G. A map $f : G \to L^*$ is called a Galois 1-cocycle if it has the following property:

$$f(\sigma\tau) = f(\sigma)\sigma(f(\tau)) \quad \text{for any} \quad \sigma, \tau \in G.$$

Show that a map $f : G \to L^*$ is a Galois 1-cocycle if and only if there exists $\alpha \in L^*$ such that

$$\sigma(\alpha) = f(\sigma)\alpha \quad \text{for any} \quad \sigma \in G.$$

2. Let p be a prime number. Find the Galois group of $f(x) = x^4 + p \in \mathbb{Q}[x]$.

3. Let L/K be a Galois extension with Galois group $\mathrm{SL}_2(\mathbb{F}_7)$. Find the number of subfields $K \subset F \subset L$ such that $[F : K] = 48$.

4. Let p be a prime number. Let K be a field. Let $a \in K$. Suppose that one of the following two conditions holds:

(a) $\mathrm{char}\, K = p$.
(b) $\mathrm{char}\, K \neq p$ and K contains all p-th roots of 1.

Show that $f(x) = x^p - a \in K[x]$ is either irreducible or has a root in K.

5. Let L/K be a finite Galois extension with Galois group G. Show that the following properties are equivalent:

(a) L is a splitting field of an irreducible polynomial of degree n.
(b) G contains a subgroup H of index n such that $\bigcap\limits_{g \in G} gHg^{-1} = \{e\}$.

6. Let K be a field. Show that if $\mathrm{Gal}\, \bar{K}/K$ is Abelian then any finite separable extension of K is Galois.

Homework 6

1. For any $k \geq 0$, let $p_k = \sum_{i=1}^{n} \alpha_i^k$. Show that

$$\begin{vmatrix} 1 & \dots & 1 \\ \alpha_1 & \dots & \alpha_n \\ \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \dots & \alpha_n^{n-1} \end{vmatrix} = \prod_{i>j}(\alpha_i - \alpha_j); \quad \begin{vmatrix} p_0 & p_1 & \dots & p_{n-1} \\ p_1 & p_2 & \dots & p_n \\ p_2 & p_3 & \dots & p_{n+1} \\ \vdots & \vdots & \ddots & \vdots \\ p_{n-1} & p_n & \dots & p_{2n-2} \end{vmatrix} = \prod_{i>j}(\alpha_i - \alpha_j)^2.$$

2. (continuation of the previous problem). (a) Let p be an odd prime number. Show that the discriminant of the cyclotomic polynomial $\Phi_p(x)$ is equal to $(-1)^{\frac{p-1}{2}} p^{p-2}$. (b) Use (a) to give a different proof of the Kronecker–Weber theorem for quadratic extensions.

3. Let q be an odd prime and let a be an integer coprime to q. Then

$$\left(\frac{a}{q}\right) \equiv a^{\frac{q-1}{2}} \mod q.$$

4. Let p be a on odd prime. Let α be a primitive 8-th root of unity in $\overline{\mathbb{F}}_p$ and let $y = \alpha + \alpha^{-1}$. (a) Show that $y^p = (-1)^{\frac{p^2-1}{8}} y$. (b) Show that $y^2 = 2$. (c) Show that $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

5. Compute $(\frac{2013}{4567})$

6. Let R be a domain with the field of fractions K. Let F/K be an algebraic extension and let S be the integral closure of R in F. For any $\alpha \in F$, show that there exists $r \in R$ such that $r\alpha \in S$.

7. Suppose $n, m \geq 2$ are coprime positive integers. Show that $\mathbb{C}[x, y]/(x^n - y^m)$ is a domain and find its normalization.

8. Let A be an integrally closed domain with the field of fractions K. Let F/K be an algebraic extension of fields. Let $\alpha \in F$. Show that α is integral over A if and only if its minimal polynomial has coefficients in A.

9. Prove that the Gauss Lemma holds not only in a UFD but in any integrally closed domain R in the following form: suppose $f(x) \in R[x]$ is a monic polynomial and $f(x) = g(x)h(x)$, where $g(x), h(x) \in K[x]$ are monic polynomials (here K is the field of fractions of R). Then $g(x), h(x) \in R[x]$.

10. Let $A \subset B$ be domains and suppose that B is integral over A. Let $I \subset B$ be an ideal. Show that B/I is integral over $A/A \cap I$.

11. (a) Let $A \subset B$ be rings and suppose that B is integral over A. Show that A is a field if and only if B is a field. (b) Let $A \subset B$ be rings and suppose that B is integral over A. Let $\mathfrak{p} \subset B$ be a prime ideal. Show that $\mathfrak{p}$ is a maximal ideal of B if and only if $\mathfrak{p} \cap A$ is a maximal ideal of A.

12. Let A be an integrally closed domain with the field of fractions K. Let F/K be a Galois extension with the Galois group G. Let B be the integral closure of A in F. Show that G preserves B and that $B^G = A$.

§7. TRANSCENDENTAL NUMBERS AND EXTENSIONS

§7.1. **Transcendental numbers. Liouville's Theorem.** The field of algebraic numbers $\bar{\mathbb{Q}} \subset \mathbb{C}$ is countable but $\mathbb{C}$ is not. So "most" of complex numbers are transcendental (Cantor, 1874). But it could be difficult to prove that a given number is transcendental. The first transcendental number was constructed by Liouville (1844). An irrational number $\alpha \in \mathbb{R}$ is called a *Liouville number* if, for any positive integer n, there exist integers p and q with $q > 1$ and such that

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^n}.$$

In other words, a Liouville number is irrational but it admits an incredibly close approximation by rational numbers.

EXAMPLE 7.1.1 (Liouville). The number

$$\alpha = \sum_{j=1}^{\infty} 10^{-j!} = 0.11000100000000000000000001000\ldots$$

is a Liouville number. Indeed, for any n

$$\sum_{j=1}^{n} 10^{-j!} = \frac{p}{q} \quad \text{where} \quad q = 10^{n!}$$

and

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{10^{(n+1)!-1}} < \frac{1}{q^n}$$

LEMMA 7.1.2. *Liouville numbers are transcendental.*

Proof. Suppose that α is algebraic and let $f(x) \in \mathbb{Z}[x]$ be an integer multiple of its minimal polynomial. Let $m = \deg f(x)$. Let

$$M := \sup_{|x-\alpha|\leq 1} |f'(x)|.$$

Take $n > 0$ and let p/q be an approximation of α as in the definition of the Liouiville number. Since $f(p.q) \neq 0$, we obviously have

$$|f(p/q)| \geq 1/q^m.$$

But by the mean value theorem

$$\frac{1}{q^m} \leq |f(p/q)| = |f(p/q) - f(\alpha)| \leq M \left|\frac{p}{q} - \alpha\right| < \frac{M}{q^n}.$$

If n is large enough, this gives a contradiction. □

Liouville numbers are a bit artificial, but with some effort, one can show that "interesting" numbers, such as e (Hermite, 1873) or π (Lindemann, 1882), are also transcendental. In fact, Lindemann proved the following:

THEOREM 7.1.3. *If $\alpha_1, \ldots, \alpha_r$ are distinct algebraic numbers then $e^{\alpha_1}, \ldots, e^{\alpha_r}$ are linearly independent over $\bar{\mathbb{Q}}$.*

It follows that e^α is transcendental for any $\alpha \in \mathbb{Q}^*$, which again shows the transcendence of e. The transcendence of π follows by the following neat trick: the Euler identity

$$e^{\pi i} = -1$$

shows that $e^{\pi i}$ and e^0 are linearly dependent over $\bar{\mathbb{Q}}$. It follows that πi, and therefore π, can not be algebraic.

§7.2. **Bonus section: proof of Hermite's Theorem.** For every polynomial $f(x)$, we set

$$F(x) = f(x) + f'(x) + f''(x) + \dots$$

Hermite shows that

$$e^x \int_0^x e^{-t} f(t)\, dt = e^x F(0) - F(x). \tag{7.2.1}$$

Indeed, using integration by parts we get

$$e^x \int_0^x e^{-t} f(t)\, dt = e^x f(0) - f(x) + e^x \int_0^x e^{-t} f'(t)\, dt$$

and then we iterate the process.

We argue by contradiction and suppose that e is algebraic, i.e.

$$a_0 + a_1 e + \dots + a_n e^n = 0$$

for some integers a_i with $a_0 \neq 0$. Setting $x = k$ in (7.2.1), multiplying the equation by a_k, and adding these equations gives

$$\sum_{k=0}^n a_k e^k \int_0^k e^{-t} f(t)\, dt = F(0) \sum_{k=0}^n a_k e^k - \sum_{k=0}^n a_k F(k),$$

which gives

$$\sum_{k=0}^n a_k F(k) = -\sum_{k=0}^n a_k e^k \int_0^k e^{-t} f(t)\, dt \tag{7.2.2}$$

Now we choose $f(t)$ by setting

$$f(t) = \frac{1}{(p-1)!} t^{p-1} \prod_{k=1}^n (k-t)^p,$$

where p is a sufficiently large prime.

CLAIM 7.2.1. *The RHS of* (7.2.2) *tends to* 0 *as the prime* p *increases.*

Indeed,

$$\left| \sum_{k=0}^n a_k e^k \int_0^k e^{-t} f(t)\, dt \right| < C \int_0^n |f(t)|\, dt < \frac{C_1 (C_2)^p}{(p-1)!} \xrightarrow[p\to\infty]{} 0.$$

So it suffices to prove that

CLAIM 7.2.2. *The LHS of* (7.2.2) *is a non-zero integer.*

The trick is to show that the LHS is an integer that is not divisible by p. Since $f(t)$ has a zero of multiplicity $p-1$ at $t=0$, we have

$$f^{(k)}(0)=0, \quad k<p-1,$$

and by the (iterated) differentiation of a product formula

$$f^{(k)}(0)=\binom{k}{p-1}\left(\frac{d}{dt}\right)^{k-p+1}\left(\prod_{k=1}^{n}(k-t)^p\right)\Bigg|_{t=0} \quad \text{for} \quad k\geq p-1.$$

For example,

$$f^{(p-1)}(0)=(n!)^p.$$

We see that $f^{(k)}(0)$ is integral for any k and that $f^{(p-1)}(0)$ is not divisible by p (if $p>n$) but $f^{(k)}(0)$ is divisible by p for any $k\neq p-1$ because differentiating the product $\prod\limits_{k=1}^{n}(k-t)^p$ gives a factor of p. Therefore $a_0F(0)$ is integral but not divisible by p (if p is large enough).

Since $f(t)$ has a zero of multiplicity p at $t=m$, $1\leq m\leq n$, we have

$$f^{(k)}(m)=0, \quad 0\leq k\leq p-1$$

and

$$f^{(k)}(m)=-p\binom{k}{p}\left(\frac{d}{dt}\right)^{k-p}\left(t^{p-1}\prod_{\substack{i=1\dots n\\ i\neq m}}(s-t)^p)\right)\Bigg|_{t=m}, \quad k\geq p,$$

is integral and divisible by p. It follows that the LHS of (7.2.2) is an integer and is not divisible by p. In particular it is not zero.

§7.3. **Transcendence degree.** For simplicity, in this section we are going to assume that K/k is a finitely generated field extension. In particular, if K/k is algebraic then K/k is a finite extension.

DEFINITION 7.3.1. A subset S of K is called *algebraically dependent* over k if there exists a non-zero polynomial $f\in k[x_1,\dots,x_n]$ such that

$$f(\alpha_1,\dots,\alpha_n)=0$$

for some different $\alpha_1,\dots,\alpha_n\in S$. Otherwise, we say that S is *algebraically independent* over k.

For example, a one-element set $S=\{\alpha\}$ is algebraically dependent if and only if α is algebraic over k. This can be generalized as follows:

LEMMA 7.3.2. *TFAE:*

- $\alpha_1,\dots,\alpha_n\in K$ *are algebraically independent.*
- $k(\alpha_1,\dots,\alpha_n)$ *is isomorphic to the field of rational functions* $k(x_1,\dots,x_n)$ *in* n *variables via the map* $x_i\mapsto\alpha_i$.

Proof. The homomorphism $\psi: k[x_1,\dots,x_n]\to K$, $x_i\mapsto\alpha_i$ has a zero kernel if and only if $\alpha_1,\dots,\alpha_n\in K$ are algebraically independent. In this case this homomorphism induces a homomorphism from $k(x_1,\dots,x_n)$ to K by the universal property of the field of fractions. The image of $k(x_1,\dots,x_n)$ is obviously $k(\alpha_1,\dots,\alpha_n)$. □

DEFINITION 7.3.3. A maximal (by inclusion) algebraically independent subset $S \subset K$ is called a *transcendence basis*. The cardinality of any transcendence basis is called the *transcendence degree* of K/k (we will prove that it does not depend on S). Notation: $\mathrm{tr.deg.}(K/k)$.

LEMMA 7.3.4. *Let $S \subset K$ be an algebraically independent subset and let $k \in K$. Then $S \cup \{\alpha\}$ is algebraically dependent if and only if α is algebraic over $k(S)$.*

Proof. $\alpha \in K$ is transcendental over $k(S) \Leftrightarrow k(\alpha, S)$ is isomorphic to the field of rational functions in variables indexed by $\{\alpha\} \cup S \Leftrightarrow \{\alpha\} \cup S$ is algebraically independent by Lemma 7.3.2. □

THEOREM 7.3.5. *Suppose K/k is a finitely generated field extension. Then K admits a finite transcendence basis $\alpha_1, \ldots, \alpha_n$ (possibly $n = 0$), $K/k(\alpha_1, \ldots, \alpha_n)$ is a finite extension, and $\mathrm{tr.deg.}(K/k) = n$ is well-defined (i.e. any other transcendence basis has n elements).*

Proof. Since K is finitely generated, we can write $K = k(\alpha_1, \ldots, \alpha_r)$. We can rearrange generators so that $S := \{\alpha_1, \ldots, \alpha_n\}$ is a maximal algebraically independent subset among all subsets of $\{\alpha_1, \ldots, \alpha_r\}$. By Lemma 7.3.4, every α_i is algebraic over $k(S)$, and therefore $K/k(S)$ is a finite extension. Applying Lemma 7.3.4 again, we see that $S \cup \{\alpha\}$ is algebraically dependent for every $\alpha \in K$, i.e. S is a transcendence basis.

It remains to show that any two transcendence bases A and B have the same number of elements. In fact, it suffices to prove the following claim:

LEMMA 7.3.6. *Let A and B be two transcendence bases and let $\alpha \in A - B$. Then there exists $\beta \in B - A$ such that $B - \{\beta\} \cup \{\alpha\}$ is a transcendence basis.*

Indeed, given the Lemma, we can repeatedly exchange elements of B for elements of A to find a sequence of transcendence bases $B = B_1, B_2, \ldots, B_k$ of size $|B|$ such that $A \subset B_k$. It follows that $A = B_k$, and so $|A| = |B|$.

It remains to prove the Lemma. Let $B = \{\beta_1, \ldots, \beta_m\}$. Since $B \cup \{\alpha\}$ is algebraically dependent, there exists a polynomial $f \in k[x_0, \ldots, x_m]$ such that $f(\alpha, \beta_1, \ldots, \beta_m) = 0$. Since B and $\{\alpha\}$ are independent sets, f contains monomials with x_0 and monomials with x_i for some $i > 0$. Let $\beta = \beta_i$. Let $C = B - \{\beta\} \cup \{\alpha\}$. Then β is algebraic over $k(C)$.

It follows that C is algebraically independent. Indeed, otherwise α is algebraic over $B - \{\beta\}$ and therefore β is in fact algebraic over $k(B - \{\beta\})$, which contradicts algebraic independence of B.

Finally, we claim that C is a transcendence basis. Indeed, since β is algebraic over $k(C)$, $k(B)$ is algebraic over $k(C)$. Therefore K is algebraic over $k(C)$, i.e. C is a transcendence basis by Lemma 7.3.4. □

EXAMPLE 7.3.7. Let S_n act on $K = k(x_1, \ldots, x_n)$ by permutations of variables. Then $K^{S_n} = k(\sigma_1, \ldots, \sigma_n)$ (elementary symmetric functions). Since $x_1, \ldots, x_n$ is a transcendence basis of K (almost by definition), we have $\mathrm{tr.deg.}(K/k) = n$. Since K/K^{S_n} is algebraic, a maximal by inclusion algebraically independent subset of $\{\sigma_1, \ldots, \sigma_n\}$ is going to be another transcendence basis of K. It follows that $\{\sigma_1, \ldots, \sigma_n\}$ is a transcendence basis of K. In particular, these elements are algebraically independent and K^{S_n} is isomorphic to the field of rational functions in n variables.

§7.4. **Noether's Normalization Lemma.**

THEOREM 7.4.1 (Noether's Normalization Lemma). *Let A be a finitely generated k-algebra. Then A contains elements $x_1, \ldots, x_n$ (maybe $n = 0$) which are algebraically independent over k and such that A is integral over $k[x_1, \ldots, x_n]$.*

Proof. Suppose that k is an infinite field (see exercises for a finite field case). Let $y_1, \ldots, y_r$ be generators of A over k. We argue by induction on r. If $r = 0$ there $A = k$ and there is nothing to prove.

Let $r > 1$. If $y_1, \ldots, y_r$ are algebraically independent then again there is nothing to prove. Suppose we have a polynomial relation

$$f(y_1, \ldots, y_r) = 0$$

for some polynomial $f(Y_1, \ldots, Y_r) \in k[Y_1, \ldots, Y_r]$. We recall the following terminology. A *degree* of a monomial $Y_1^{n_1} \ldots Y_r^{n_r}$ is the sum $n_1 + \ldots + n_r$. A polynomial is called *homogeneous* if all its monomials have the same degree. Every polynomial is a sum of its homogeneous components obtained by grouping together monomials of the same degree. In particular, let $F(Y_1, \ldots, Y_r)$ be the homogeneous component of f of top total degree. Then $F(Y_1, \ldots, Y_{r-1}, 1)$ is a non-trivial polynomial. Since k is infinite, we can find $\lambda_1, \ldots, \lambda_{r-1} \in k$ such that

$$F(\lambda_1, \ldots, \lambda_{r-1}, 1) \neq 0.$$

We introduce a new polynomial $g(Y_1, \ldots, Y_r) \in k[Y_1, \ldots, Y_r]$ by formula

$$g(Y_1, \ldots, Y_{r-1}, Y_r) := \frac{1}{F(\lambda_1, \ldots, \lambda_{r-1}, 1)} f(Y_1 + \lambda_1 Y_r, \ldots, Y_{r-1} + \lambda_{r-1} Y_r, Y_r).$$

As a polynomial in Y_r, $g(Y_r)$ has leading coefficient 1 – it is monic.

Now we introduce new elements $y_1', \ldots, y_{r-1}' \in A$ by formulas

$$y_1' := y_1 - \lambda_1 y_r, \quad \ldots, \quad y_{r-1}' := y_{r-1} - \lambda_{r-1} y_r.$$

We notice that $y_1', \ldots, y_{r-1}', y_r$ generate A and we have

$$g(y_1', \ldots, y_{r-1}', y_r) = f(y_1' + \lambda_1 y_r, \ldots, y_{r-1}' + \lambda_{r-1} y_r, y_r) = 0.$$

It follows that y_r (and therefore A) is integral over a subalgebra A' generated by $y_1', \ldots, y_{r-1}'$. By induction, A' is integral over its subalgebra B generated by algebraically independent elements $x_1, \ldots, x_n$. By transitivity of integral dependence, A is integral over B as well. $\square$

Homework 7

1. Let R be an integrally closed Noetherian domain with field of fractions K. Let L/K be a finite extension (not necessarily Galois). Let T be the integral closure of R in L. Show that there exists $b_1, \ldots, b_n \in T$ which form a basis of L over K.

2. Let R be an integrally closed Noetherian domain with field of fractions K. Let L/K be a finite Galois extension with Galois group $G = \{\sigma_1, \ldots, \sigma_n\}$. Let T be the integral closure of R in L. Let $b_1, \ldots, b_n \in T$ be a basis of L over K. Consider the determinant $d = \det |\sigma_i(b_j)|$. (a) Show that $d \in T$. (b) Show that $d^2 \in R$.

3. (continuation of the previous problem). $d^2 T \subset Rb_1 + \ldots + Rb_n$.

4. Let R be an integrally closed Noetherian domain with field of fractions K. Let L/K be a finite extension (not necessarily Galois). Let T be the integral closure of R in L. Show that T is a finitely generated R-module.

5. Let $K/\mathbb{Q}$ be a finite extension (not necessarily Galois). Show that $\mathcal{O}_K$ is a finitely generated free abelian group.

6. Let k be a field. Let $F \subset k(x)$ be a subfield properly contaning k. Show that $k(x)/F$ is a finite extension.

7. Let K_1 and K_2 be algebraically closed extensions of $\mathbb{C}$ of transcendence degree 11. Show that any homomorphism $f : K_1 \to K_2$ is an isomorphism.

8. Let $k \subset K \subset E$ be finitely generated field extensions. Show that

$$\text{tr.deg. } E/k = \text{tr.deg. } K/k + \text{tr.deg. } E/K.$$

9. A *matroid* is a set E and a non-empty family of finite subsets of E called *independent sets* such that

- Every subset of an independent set is independent.
- If A and B are two independent sets and $|A| > |B|$ then there exists $a \in A - B$ such that $B \cup \{a\}$ is independent.

Show that the following are matroids: (a) E is a vector space; independent sets are linearly independent sets of vectors. (b) E is a field extension of k; independent sets are algebraically independent sets. (c) E is the set of edges of a graph; independent sets are subsets of edges without loops.

10. A *basis* of a matroid is a maximal (by inclusion) independent set. Show that if a matroid has a finite basis then all its bases have the same number of elements (called *dimension* of the matroid).

11. Let k be a field and let A be a finitely generated k-algebra. Let $B \subset A$ be a k-subalgebra such that A is integral over B. Show that A is a finitely generated B-module and B is a finitely generated k-algebra (Hint: consider a k-subalgebra $C \subset B$ generated by coefficients of monic equations satisfied by generators of A).

12. Prove Noether's normalization lemma when k is an arbitrary field by using a change of variables $y_i' = y_i - y_{r+1}^{n_i}$ instead of $y_i' = y_i - \lambda_i y_{r+1}$.

§8. Basic Algebraic Geometry – I

§8.1. **Weak Nullstellensatz.** Hilbert's Nullstellensatz (Theorem on Zeros), is a higher-dimensional analogue of the Fundamental Theorem of Algebra. For our purposes the latter can be stated as follows:

Claim 8.1.1. *There is a bijection between $\mathbb{C}$ and the set of maximal ideals in $\mathbb{C}[x]$,*

$$a \in \mathbb{C} \quad \mapsto \quad (x-a) \subset \mathbb{C}[x].$$

This maximal ideal consists of all polynomials that vanish at a.

Proof. Indeed, the traditional formulation of the fundamental theorem is that $\mathbb{C}$ is algebraically closed. This implies that only linear polynomials in $\mathbb{C}[x]$ are irreducible. On the other hand, for every field k, maximal ideals in $k[x]$ are principal ideals (f) generated by irreducible polynomials $f(x)$. □

Theorem 8.1.2 (Weak Nullstellensatz). *If k is any algebraically closed field, there is a bijection between k^n and the set of maximal ideals of $k[x_1, \ldots, x_n]$,*

$$(a_1, \ldots, a_n) \in k^n \quad \mapsto \quad (x-a_1, \ldots, x-a_n) \subset k[x_1, \ldots, x_n].$$

This maximal ideal consists of all polynomials that vanish at $(a_1, \ldots, a_n)$.

Proof. Given a point $(a_1, \ldots, a_n)$, consider an evaluation homomorphism

$$\psi : k[x_1, \ldots, x_n] \to k, \quad x_i \mapsto a_i. \tag{8.1.1}$$

It is surjective onto a field, and so its kernel is a maximal ideal. A Taylor expansion of a polynomial centered at $(a_1, \ldots, a_n)$ shows that this maximal ideal is generated by $x - a_1, \ldots, x - a_n$.

Now suppose that $\mathfrak{m} \subset k[x_1, \ldots, x_n]$ is a maximal ideal such that

$$k[x_1, \ldots, x_n]/\mathfrak{m} \simeq k.$$

It induces a projection homomorhism $\psi : k[x_1, \ldots, x_n] \to k$ with kernel $\mathfrak{m}$. Let $a_i := \psi(x_i)$. Then ψ is equal to the homomorphism (8.1.1). Therefore $\mathfrak{m}$ is the kernel of the evaluation map at the point $(a_1, \ldots, a_n)$ of $\mathbb{A}^n$.

If $\mathfrak{m} \subset k[x_1, \ldots, x_n]$ is *any* maximal ideal then

$$A := k[x_1, \ldots, x_n]/\mathfrak{m}$$

is a field that contains k, which is finitely generated over k by cosets $x_i + \mathfrak{m}$. Since k is algebraically closed, everything follows from a lemma below. □

Lemma 8.1.3. *If A is both a finitely generated k-algebra and a field then A/k is an algebraic field extension. In particular, if k is algebraically closed them $A = k$.*

Proof. By Noether's normalization lemma, A is integral over its subalgebra $B = k[x_1, \ldots, x_r]$, where $x_1, \ldots, x_r$ are algebraically independent over k. Let $\alpha \in B$. Since A is a field, $1/\alpha$ is in A. Since A in integral over B, $1/\alpha$ satisfies a monic equation

$$(1/\alpha)^n + b_1(1/\alpha)^{n-1} + \ldots + b_n, \quad b_i \in B.$$

Multiplying by α^{n-1}, this gives

$$1/\alpha = -b_1 - \ldots - b_n\alpha^{n-1} \in B.$$

It follows that B is a field as well. This is impossible unless $r = 0$, because B is isomorphic to the algebra of polynomials in r variables. So A is in fact integral (and hence algebraic) over k. □

§8.2. **Algebraic sets. Strong Nullstellensatz.** The weak Nullstellensatz establishes a bijection between algebra (the set of maximal ideals) and geometry (the set of points). We would like to extend this bijection, for example can we characterize the set of all ideals in similar terms? The fundamental theorem of algebra again provides an inspiration. Indeed, a proper ideal in $\mathbb{C}[x]$ is a principal ideal (f) generated by a polynomial of positive degree. This ideal is completely determined by the set of roots of the polynomial $\{\alpha_1, \ldots, \alpha_n\} \subset \mathbb{C}$ counted with positive multiplicities. A polynomial $f(x)$ has no multiple roots if and only if (f) is a radical ideal, i.e. $(f) = \sqrt{(f)}$. Recall that a *radical* of an ideal $I \subset R$ is the ideal

$$\sqrt{I} = \{r \mid r^l \in I \text{ for some } l > 0\}.$$

So we have a bijection

$$\text{proper radical ideals } (f) \subset \mathbb{C}[x] \ \leftrightarrow \ \text{non-empty finite sets } \{\alpha_1, \ldots, \alpha_n\} \subset \mathbb{C}.$$

To generalize this to higher dimensions, we have to define an analogue of the right hand side.

DEFINITION 8.2.1. A subset $X \subset k^n$ is called *a closed algebraic set* if there exist polynomials $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$ such that

$$X = \{(a_1, \ldots, a_n) \in k^n \quad | \quad f_i(a_1, \ldots, a_n) = 0 \text{ for any } i = 1, \ldots, m\}.$$

For example, closed algebraic subsets of $\mathbb{C}$ are finite sets (and $\mathbb{C}$ itself).

LEMMA 8.2.2. *We can characterize closed algebraic sets as subsets of the form*

$$V(I) := \{(a_1, \ldots, a_n) \in k^n \quad | \quad f(a_1, \ldots, a_n) = 0 \text{ for any } f \in I\}.$$

Here $I \subset k[x_1, \ldots, x_n]$ is an arbitrary ideal.

FIGURE 1. Here's looking at you, closed algebraic set.

Proof. Let X be a closed algebraic set as in the definition. Consider an ideal

$$I = (f_1, \ldots, f_m) \subset k[x_1, \ldots, x_n].$$

Take any $g = \sum h_i f_i \in I$. Then $g(x) = \sum h_i(x) f_i(x) = 0$ for any $x \in X$, so $X = V(I)$. By the Hilbert's basis theorem, any ideal $I \subset k[x_1, \ldots, x_n]$ has finitely many generators $f_1, \ldots, f_m$. Therefore, closed algebraic sets are precisely sets of the form $V(I)$. □

Let $X \subset k^n$ be any closed algebraic set. Consider all polynomial functions that vanish along it:

$$I(X) := \{f \in k[x_1, \ldots, x_n] \quad | \quad f(a_1, \ldots, a_n) = 0 \text{ for every } (a_1, \ldots, a_n) \in X\}.$$

This is clearly an ideal, in fact a radical ideal. We have two operations:

- Ideals $\to$ closed algebraic sets, $I \mapsto V(I)$.
- Closed algebraic sets $\to$ radical ideals, $X \mapsto I(X)$.

It is clear that $I \subset I(V(I))$. The precise relationship is given by

THEOREM 8.2.3 (Strong Nullstellensatz). *Suppose $k = \bar{k}$. Then*

$$V(I(X)) = X$$

for every closed algebraic set $X \subset k^n$ and

$$I(V(I)) = \sqrt{I}$$

for every ideal $I \subset k[x_1, \ldots, x_n]$.

In particular we have the following corollary:

COROLLARY 8.2.4. *Operations V and I set up an inclusion-reversing bijection*

$$\text{radical ideals } I \subset k[x_1, \ldots, x_n] \ \leftrightarrow \ \text{closed algebraic sets } X \subset k^n.$$

Proof. Let $X = V(I)$. It is clear that $\sqrt{I} \subset I(X)$. Indeed, if $g \in \sqrt{I}$ then $g^l \in I$ for some $l > 0$ and so $g^l(x) = 0$ for every $x \in X$. Thus $g \in I(X)$. Also, if we can show that $\sqrt{I} = I(X)$ then it will follow that

$$V(I(X)) = V(I(V(I))) = V(\sqrt{I}) = V(I) = X.$$

So it remains to show that $\sqrt{I} \supset I(X)$.

In concrete terms, we have to show the following. Let $I = (f_1, \ldots, f_m)$ and suppose that $g \in k[x_1, \ldots, x_n]$ vanishes at every point $(a_1, \ldots, a_n)$ where each f_i vanishes. Then we claim that there exists an integer l and polynomials $h_1, \ldots, h_m$ such that

$$g^l = h_1 f_1 + \ldots + h_m f_m.$$

We use an approach known as "Rabinowitch's trick": consider the ideal

$$B = (f_1, \ldots, f_m, 1 - g x_{n+1}) \subset k[x_1, \ldots, x_{n+1}].$$

CLAIM 8.2.5. $B = k[x_1, \ldots, x_{n+1}]$.

Proof. Indeed, if B is a proper ideal then it is contained in some maximal ideal, which, by the weak Nullstellensatz, consists of all polynomials that vanish at some point $(a_1, \ldots, a_{n+1})$. But then $f_i(a_1, \ldots, a_n) = 0$ for any i but $g(a_1, \ldots, a_n) a_{n+1} = 1$. This is a contradiction because we should have $g(a_1, \ldots, a_n) = 0$. □

It follows that we can find polynomials $h_1^*, \ldots, h_{m+1}^* \in k[x_1, \ldots, x_{n+1}]$ such that

$$h_1^* f_1 + \ldots + h_m^* f_m + h_{m+1}^*(1 - g x_{n+1}) = 1.$$

The trick is to substitute $1/g$ for x_{n+1} in this formula. This gives

$$\sum h_i^* \left(x_1, \ldots, x_n, \frac{1}{g(x_1, \ldots, x_n)} \right) f_i(x_1, \ldots, x_n) = 1. \tag{8.2.1}$$

For purists: we are applying a homomorphism

$$k[x_1, \ldots, x_{n+1}] \to k(x_1, \ldots, x_n), \quad x_i \mapsto x_i \quad (i \le n), \quad x_{n+1} \mapsto \frac{1}{g(x_1, \ldots, x_n)}.$$

To clear denominators in (8.2.1), multiply by a sufficiently large power of g, which gives

$$\sum h_i(x_1, \ldots, x_n) f_i(x_1, \ldots, x_n) = g^l(x_1, \ldots, x_n)$$

for some polynomials $h_1, \ldots, h_m$. QED. □

REMARK 8.2.6. In Algebraic Geometry a notion of a scheme is introduced to make strong Nullstellensatz even stronger: there is a bijection

$$\text{ideals } I \subset k[x_1, \ldots, x_n] \ \leftrightarrow \ \text{closed algebraic subschemes } X \subset k^n.$$

For example, a closed algebraic subscheme of $\mathbb{C}$ is a finite set of points with assigned multiplicities (or $\mathbb{C}$ itself).

§8.3. **Zariski topology on $\mathbb{A}^n$.** We use notation $\mathbb{A}^n$ and k^n interchangeably, but we are going to gradually add more and more structure to the former.

THEOREM 8.3.1. *$\mathbb{A}^n$ has a topology, called Zariski topology, such that closed algebraic sets are precisely closed sets in Zariski topology.*

Proof. Recalling axioms of topology, we have to show that any intersection or finite union of closed sets is a closed set. But

$$\bigcap_{i \in I} V(I_i) = V\left(\sum I_i \right)$$

and

$$V(I_1) \cup \ldots \cup V(I_n) = V(I_1 \cdot \ldots \cdot I_n)$$

(the product of ideals). □

For example, Zariski closed subsets of $\mathbb{A}^1$ are finite unions of points (and the whole $\mathbb{A}^1$).

§8.4. **Irreducible algebraic sets.** Zariski topology has very strange properties compared to the usual Euclidean topology. For example, any two non-empty open sets intersect or, alternatively, the union of two proper closed sets is proper. Indeed, $V(f_1, \ldots, f_n) \cup V(g_1, \ldots, g_m) \subset V(f_1) \cup V(g_1)$ and this union does not contain any point where neither f_1 nor g_1 vanishes. To generalize this observation, we introduce the following definition:

DEFINITION 8.4.1. A closed subset of a topological space is called *irreducible* if it is not a union of two proper closed subsets.

Only points of $\mathbb{C}^n$ are irreducible subsets in the Euclidean topology but we just saw that in Zariski topology $\mathbb{C}^n$ itself is irreducible!

DEFINITION 8.4.2. The *spectrum* (or *prime spectrum*) $\operatorname{Spec} R$ of the ring R is the set of prime ideals of R.

LEMMA 8.4.3. *The usual correspondence $Y \to I(Y)$ from Nullstellensatz induces a bijection between the set of irreducible subsets of $\mathbb{A}^n$ and* $\operatorname{Spec} k[x_1, \ldots, x_n]$.

Proof. Suppose $Y \subset \mathbb{A}^n$ is a reducible subset, $Y = Y_1 \cup Y_2$. Let I (resp. I_1 and I_2) be the ideals of all polynomials vanishing along Y (resp. Y_1 and Y_2). Since Y_1 and Y_2 are proper subsets of Y, we have $I \neq I_1$ and $I \neq I_2$ by the Nullstellensatz. So there exist $f \in I_1 \setminus I$ and $g \in I_2 \setminus I$. However, clearly $fg \in I(Y)$. This shows that I is not prime.

If $I = I(Y)$ is not prime then we can find $f, g \in k[x_1, \ldots, x_n] \setminus I$ such that $fg \in I$. This means that, for any $y \in Y$, either $f(y) = 0$ or $g(y) = 0$. It follows that Y can be decomposed as $(Y \cap V(f)) \cup (Y \cap V(g))$. □

So maximal ideals of $k[x_1, \ldots, x_n]$ correspond to points of $\mathbb{A}^n$ and other prime ideals correspond to other irreducible subsets.

EXAMPLE 8.4.4. The only prime ideal in $k[x]$ that is not maximal is (0), i.e.

$$\operatorname{Spec} k[x] = \mathbb{A}^1_k \cup \{\eta\}, \text{ where } \eta = (0).$$

One can visualize η as a sort of a fuzzy point.

EXAMPLE 8.4.5. According to the homework, the prime ideals of $k[x, y]$ are

- maximal ideals $(x - a, y - b)$;
- ideals (f), where $f \in k[x, y]$ is an irreducible polynomial;
- (0).

The corresponding closed algebraic sets are

- points $(a, b) \in \mathbb{A}^2$;
- algebraic curves $(f = 0)$, where $f \in k[x, y]$ is irreducible;
- $\mathbb{A}^2$.

See Figure 2.

REMARK 8.4.6. One can endow $\operatorname{Spec} R$ with Zariski topology for any ring R. Namely, for any subset $I \subset R$, we declare

$$V(I) := \{\mathfrak{p} \in \operatorname{Spec} R \mid \mathfrak{p} \supset I\}$$

to be a closed subset in Zariski topology (see the homework for details). If $R = k[x_1, \ldots, x_n]$ then $\mathbb{A}^n$ with Zariski topology can be identified with the set of maximal ideals $\operatorname{MaxSpec} R \subset \operatorname{Spec} R$ with induced topology. "Fuzzy" points discussed above then have a remarkable property, rare in traditional topological contexts: they are not closed! For example, consider $(0) \in \operatorname{Spec} k[x]$. This point belongs to only one Zariski closed subset, namely $V((0))$. It follows that $\overline{(0)} = \operatorname{Spec} k[x]$.

§8.5. **Irreducible components.**

DEFINITION 8.5.1. Let $Y \subset \mathbb{A}^n$ be a closed algebraic set. Maximal (by inclusion) irreducible subsets of Y are called *irreducible components* of Y.

THEOREM 8.5.2. *A closed algebraic set Y has finitely many irreducible components $Y_1, \ldots, Y_r$ and we have*

$$Y = Y_1 \cup \ldots \cup Y_r.$$

FIGURE 2. $\operatorname{Spec} k[x, y]$ (From Mumford's *Red Book*).

Proof. It suffices to prove that Y can be written as a finite union of irreducible subsets $Z_1, \ldots, Z_r$. Indeed, by throwing away subsets contained in other subsets we can also assume that $Z_i \not\subset Z_j$ for $i \neq j$. If $Z \subset Y$ is any subset then $Z = (Z \cap Z_1) \cup \ldots \cup (Z \cap Z_r)$, and so if Z is irreducible then it must be contained in one of the Z_i's. It follows that Z_i's are exactly irreducible components of Y.

Let's prove the claim. If Y is irreducible then there is nothing to do. If $Y = Y_1 \cup Y_2$ then we can start breaking Y_1 and Y_2 further into unions of proper closed subsets. We claim that this process eventually stops and produces the decomposition of Y as a finite union of irreducible subsets. Indeed, if the process doesn't terminate then we will produce a nested chain of closed subsets

$$Y = Y^1 \supset Y^2 \supset Y^3 \supset \ldots$$

where $Y^i \neq Y^{i+1}$. But this produces an infinite increasing chain of ideals

$$I(Y^1) \subset I(Y^2) \subset I(Y^3) \subset \ldots$$

such that $I(Y^i) \neq I(Y^{i+1})$ (by Nullstellensatz). But $k[x_1, \ldots, x_n]$ is a Noetherian ring (Hilbert's basis theorem). □

REMARK 8.5.3. What does this theorem tell us on the algebraic side? By Nullstellensatz, a closed algebraic set $Y \subset \mathbb{A}^n$ corresponds to a radical ideal $I \subset k[x_1, \ldots, x_n]$. Irreducible subsets contained in Y correspond to prime ideals $\mathfrak{p} \supset I$. Irreducible components $Y_1, \ldots, Y_r$ of Y correspond

to minimal (by inclusion) prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ containing I. We claim that in fact

$$I = \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_r.$$

Indeed, if $f \in \mathfrak{p}_i$ for any i then f vanishes along each Y_i, and so $f \in I$.

In other words, every radical ideal in $k[x_1, \ldots, x_n]$ is the intersection of minimal (by inclusion) prime ideals which contain it. The same statement in fact holds in any Noetherian ring. Moreover, every ideal in a Noetherian ring can be expressed (although not uniquely) as the intersection of so-called *primary ideals* (generalization of prime ideals). This statement is known as *primary decomposition*.

§8.6. **Affine algebraic sets. Regular functions.**

DEFINITION 8.6.1. Let $Y \subset \mathbb{A}^n$ be a closed algebraic set. The algebra of *regular functions* on Y is the algebra of "restrictions of polynomial functions"

$$\mathcal{O}(Y) = k[x_1, \ldots, x_n]/I(Y).$$

$\mathcal{O}(Y)$ is also called the *coordinate algebra* of Y. Another notation: $k[Y]$.

Notice that Y is irreducible if and only if $\mathcal{O}(Y)$ is a domain.

DEFINITION 8.6.2. A ring R is called *reduced* if its nilradical $\sqrt{0}$ is equal to 0.

LEMMA 8.6.3. *$\mathcal{O}(Y)$ is a finitely generated reduced k-algebra. Moreover, any finitely generated reduced k-algebra is isomorphic to the algebra of the form $\mathcal{O}(Y)$.*

Proof. Since $I(Y)$ is a radical ideal, the nilradical of $\mathcal{O}(Y)$ is the zero ideal. Now let A be any finitely generated reduced k-algebra. Then we can write $A \simeq k[x_1, \ldots, x_n]/I$. We claim that $I = \sqrt{I}$. Indeed, if $x \in \sqrt{I}$ then $x + I$ is a nilpotent in A, hence zero. It follows that $A \simeq \mathcal{O}(X)$, where $X = V(I)$. □

DEFINITION 8.6.4. A pair $(X, \mathcal{O}(X))$ of a closed algebraic set $X \subset \mathbb{A}^n$ and its coordinate algebra is called an *affine algebraic set*. An irreducible affine algebraic set is called an *affine algebraic variety*.

One example is the affine space $\mathbb{A}^n = (k^n, k[x_1, \ldots, n])$. We can extend Nullstellensatz and other previously discussed results from $\mathbb{A}^n$ to any affine algebraic set Y as follows:

COROLLARY 8.6.5. *Let $(Y, \mathcal{O}(Y))$ be an affine algebraic set. We have several versions of Nullstellensatz:*

(a) *There is a bijection between the set of closed algebraic subsets of Y and the set of radical ideals of $\mathcal{O}(Y)$ which sends $Z \subset Y$ to $\{f \in \mathcal{O}(Y) \mid f|_Z = 0\}$.*
(b) *This bijection induces a bijection between the set of irreducible algebraic subsets of Y and the set of prime ideals,* $\operatorname{Spec} \mathcal{O}(Y)$.
(c) *This bijection induces a bijection between the set of points of Y and the set of maximal ideals of $\mathcal{O}(Y)$.*

Closed algebraic subsets of Y are closed subsets of topology, called Zariski topology. This topology is induced by Zariski topology of $\mathbb{A}^n$ via inclusion $Y \subset \mathbb{A}^n$.

Proof. This follows from analogous results about $\mathbb{A}^n$ using correspondence between ideals of $\mathcal{O}(Y)$ and ideals of $k[x_1, \ldots, x_n]$ containing $I = I(Y)$. For example, points of Y (viewed as a subset of $\mathbb{A}^n$) correspond to maximal ideals of $k[x_1, \ldots, x_n]$ containing I. By the first isomorphism theorem these ideals correspond to maximal ideals of $\mathcal{O}(Y) = k[x_1, \ldots, x_n]/I$. □

§8.7. **Morphisms of affine algebraic sets.** Given closed algebraic sets

$$Y_1 \subset \mathbb{A}^n_{x_1,\dots,x_n} \quad \text{and} \quad Y_2 \subset \mathbb{A}^m_{y_1,\dots,y_m}$$

(subscripts indicate variables), how should we define maps from Y_1 to Y_2?

DEFINITION 8.7.1. A map $\alpha : Y_1 \to Y_2$ is called a *regular morphism* if α is the restriction of a polynomial map

$$\mathbb{A}^n_{x_1,\dots,x_n} \to \mathbb{A}^m_{y_1,\dots,y_m}, \quad y_i = f_i(x_1,\dots,x_n),$$

i.e. if there exists m polynomials $f_1,\dots,f_m$ in variables $x_1,\dots,x_n$ such that

$$\alpha(a_1,\dots,a_n) = (f_1(a_1,\dots,a_n),\dots,f_m(a_1,\dots,a_n))$$

for any point $(a_1,\dots,a_n) \in Y_1$.

EXAMPLE 8.7.2. The map

$$t \mapsto (t^2, t^3)$$

is a morphism from $\mathbb{A}^1$ to the cusp $V(y^2 - x^3) \subset \mathbb{A}^2$.

EXAMPLE 8.7.3. A morphism from $\mathbb{A}^1_t$ to the parabola $X = V(y - x^2) \subset \mathbb{A}^2$, $t \mapsto (t, t^2)$, and a morphism $X \to \mathbb{A}^1$, $(x, y) \mapsto x$, are inverses of each other.

DEFINITION 8.7.4. For any regular morphism $\alpha : Y_1 \to Y_2$, a *pull-back homomorphism* $\alpha^* : \mathcal{O}(Y_2) \to \mathcal{O}(Y_1)$ is defined as follows. If $f \in \mathcal{O}(Y_2)$ and $a \in Y_1$ then we simply define

$$(\alpha^* f)(a) = f(\alpha(a)).$$

To show that $\alpha^* f \in \mathcal{O}(Y_1)$, we have to check that it is the restriction of a polynomial function on $\mathbb{A}^n$. But f itself is the restriction of a polynomial function $\bar{f} \in k[y_1,\dots,y_m]$. Then $\alpha^*(f)$ is the restriction of the function

$$\bar{f}(f_1(x_1,\dots,x_n),\dots,f_m(x_1,\dots,x_n)),$$

which is obviously a polynomial in n variables.

EXAMPLE 8.7.5. For the map

$$\alpha : \mathbb{A}^1 \to X = V(y^2 - x^3) \subset \mathbb{A}^2, \quad t \mapsto (t^2, t^3),$$

we have $\mathcal{O}(X) = k[x,y]/(x^3 - y^2)$, and

$$\alpha^* : k[x,y]/(x^3 - y^2) \to k[t], \quad x \mapsto t^2,\ y \mapsto t^3.$$

The image of α^* is $k[t^2, t^3] \subset k[t]$. The field of fractions of $k[t^2, t^3]$ is equal to $k(t)$ and $k[t]$ is the integral closure of $k[t^2, t^3]$. Geometrically, we say that $\mathbb{A}^1$ is the normalization of the cuspidal curve X.

EXAMPLE 8.7.6. Regular morphisms between $\mathbb{A}^1$ and $X = V(y - x^2) \subset \mathbb{A}^2$ from Example 8.7.3 induce isomorphisms

$$\mathcal{O}(X) = k[x,y]/(y - x^2) \simeq k[t] = \mathcal{O}(\mathbb{A}^1), \quad (x \mapsto t,\ y \mapsto t^2), \quad (t \mapsto x).$$

LEMMA 8.7.7. *Let* $\mathbf{Mor}(Y_1, Y_2)$ *be the set of regular morphisms* $Y_1 \to Y_2$*. Then*

$$\mathbf{Mor}(Y_1, Y_2) \simeq \mathrm{Hom}_{\mathbf{Rings}}(\mathcal{O}(Y_2), \mathcal{O}(Y_1)), \quad \alpha \mapsto \alpha^*.$$

In other words, a regular morphism of affine algebraic sets is completely determined by its pull-back homomorphism, and any homomorphism of algebras of regular functions arises as the pull-back for some regular morphism.

REMARK 8.7.8. In the language of category theory, the category of affine algebraic sets and regular morphisms is equivalent to the category of finitely generated reduced k-algebras and homomorphisms.

Proof. If $\alpha : Y_1 \to Y_2$ is a morphism and

$$\alpha(a_1, \ldots, a_n) = (b_1, \ldots, b_m)$$

for some $(a_1, \ldots, a_n) \in Y_1$ then $b_i = \alpha^*(y_i)(a_1, \ldots, a_n)$. So α^* determines α.

Let $F : \mathcal{O}(Y_2) \to \mathcal{O}(Y_1)$ be any homomorphism. We have to realize it as a pull-back homomorphism for some morphism of algebraic sets. We can construct a homomorphism $\tilde{F}$ that fits into the commutative diagram of homomorphisms

$$\begin{array}{ccc} \mathcal{O}(Y_2) & \xrightarrow{\quad F \quad} & \mathcal{O}(Y_1) \\ f \mapsto \bar{f} \uparrow & & \uparrow \\ k[y_1, \ldots, y_m] & \xrightarrow[y_i \mapsto \bar{f}_i]{\tilde{F}} & k[x_1, \ldots, x_n] \end{array}$$

by choosing, for each $i = 1, \ldots, m$, a representative $f_i \in k[x_1, \ldots, x_n]$ of a coset $F(\bar{y}_i)$. Consider a regular morphism

$$\alpha : \mathbb{A}^n \to \mathbb{A}^m, \quad (a_1, \ldots, a_n) \mapsto (f_1(a_1, \ldots, a_n), \ldots, f_m(a_1, \ldots, a_n)).$$

We claim that $\alpha(Y_1) \subset Y_2$. It suffices to check that any polynomial $f \in I(Y_2)$ vanishes on $\alpha(Y_1)$, i.e. that $f(f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n) \in I(Y_1)$. But modulo $I(Y_1)$ this polynomial is equal to $F(\bar{f})$=0. □

For example, we can think about the embedding of a closed algebraic set $X \subset \mathbb{A}^n$ as a regular morphism $X \hookrightarrow \mathbb{A}^n$. The corresponding pull-back homomorphism is just the canonical projection

$$\mathcal{O}(\mathbb{A}^n) = k[x_1, \ldots, x_n] \to k[x_1, \ldots, x_n]/I(X) = \mathcal{O}(X).$$

And vice versa, the following proposition shows that any realization of an affine algebraic set X as a closed algebraic subset of the affine space $\mathbb{A}^m$ is equivalent to a choice of generators of the algebra $\mathcal{O}(X)$.

PROPOSITION 8.7.9. *Given a choice of generators $\bar{y}_1, \ldots, \bar{y}_m$ of $\mathcal{O}(X)$, consider a homomorphism $k[y_1, \ldots, y_m] \xrightarrow{\alpha^*} \mathcal{O}(X)$ which sends y_i to $\bar{y}_i$. Let $\alpha : X \to \mathbb{A}^m$ be the corresponding map. Then $\alpha(X) \subset \mathbb{A}_m$ is a closed algebraic set and $\alpha : X \to \alpha(X)$ is an isomorphism of affine algebraic sets.*

Proof. By definition, X is a closed algebraic subset in some affine space $\mathbb{A}^n$. Let $Y = V(\operatorname{Ker} \alpha^*) \subset \mathbb{A}^m$. By the first isomorphism theorem, we have $\mathcal{O}(X) \simeq \mathcal{O}(Y)$. By Lemma 8.7.7, this shows that X and Y are isomorphic. Since the map $X \to Y$ is our map α, we see that $\alpha(X) = Y$ is closed. □

§8.8. **Dominant morphisms.** Let's translate some geometry into algebra.

DEFINITION 8.8.1. A regular morphism $\alpha : Y_1 \to Y_2$ of affine algebraic sets is called *dominant* if its image is Zariski dense in Y_2.

EXAMPLE 8.8.2. Consider projection from the hyperbola $V(xy-1) \subset \mathbb{A}^2$ to the x-axis $\mathbb{A}^1_x$. The image misses only $0 \in \mathbb{A}^1$, so this map is dominant. The pull-back homomorphism is

$$k[x] \to k[x,y]/(xy-1) \simeq k\left[x, \frac{1}{x}\right], \quad x \mapsto x.$$

Notice that this homomorphism is injective. This is not a coincidence.

PROPOSITION 8.8.3. *$\alpha : Y_1 \to Y_2$ is dominant if and only if α^* is injective.*

Proof. Assume α is dominant. If $f \in \operatorname{Ker} \alpha^*$ then $f(\alpha(a)) = 0$ for any $a \in Y_1$. It follows that α maps Y_1 to a closed subset $V(f) \cap Y_2$. Since $\overline{\alpha(Y_1)} = Y_2$, we have $V(f) \cap Y_2 = Y_2$, i.e. f vanishes along Y_2. So $f = 0$.

Suppose α is not dominant. Then $\overline{\alpha(Y_1)}$ is a proper closed subset of Y_2, and therefore there exists $f \in \mathcal{O}(Y_2)$, $f \neq 0$, such that $\overline{\alpha(Y_1)} \subset V(f)$. But then $\alpha^*(f) = 0$, i.e. $\operatorname{Ker} \alpha^* \neq 0$. $\square$

Homework 8

In this worksheet, we fix an algebraically closed field k. We also fix a commutative ring R (with 1).

1. Let $f, g \in \mathbb{C}[x, y]$. Suppose that f is irreducible and does not divide g in $\mathbb{C}[x, y]$. (a) Show that f is irreducible and does not divide g in $\mathbb{C}(x)[y]$. (b) Show that $V(f, g)$ is a union of finitely many points.

2. Let $\mathfrak{p} \in \operatorname{Spec} k[x, y]$. Show that there are exactly three possibilities:

- $\mathfrak{p} = \{0\}$;
- $\mathfrak{p} = (f)$, where $f \in k[x, y]$ is an irreducible polynomial;
- $\mathfrak{p} = (x - a, y - b)$ for some $(a, b) \in k^2$.

3. Let $F \in k[x_1, \ldots, x_n]$ be an irreducible polynomial. Let G be a polynomial such that $G|_{V(F)} = 0$. Show that G is divisible by F.

4. (a) Show that Zariski topology of $\mathbb{A}^n$ has a basis of open sets of the form

$$D(f) = \{(a_1, \ldots, a_n) \in \mathbb{A}^n \mid f(a_1, \ldots, a_n) \neq 0\} \quad \text{for} \quad f \in k[x_1, \ldots, x_n].$$

(b) Show that any Zariski open cover of $\mathbb{A}^n$ has a finite subcover.

5. Let $X \subset \mathbb{A}^2$ be defined by the ideal $I = (x^2 + y^2 - 1, x - 1)$. Is it true that $I(X) = I$?

6. Let X be an affine algebraic set. Consider an ideal $I \subset \mathcal{O}(X)$ and suppose that $V(I) = \emptyset$. Show that $I = \mathcal{O}(X)$.

7. For any ideal I of R, let

$$V(I) = \{\mathfrak{p} \in \operatorname{Spec} R \mid I \subset \mathfrak{p}\}.$$

(a) Show that $\operatorname{Spec} R$ satisfies axioms of a topological space with closed subsets $V(I)$. This topology is called *Zariski topology*. (b) Given a homomorphism of rings $f : A \to B$, show that the map $\alpha : \operatorname{Spec} B \to \operatorname{Spec} A$, $\alpha(\mathfrak{p}) = f^{-1}(\mathfrak{p})$ is continuous in Zariski topology. (c) For any $f \in R$, let $D(f) \subset \operatorname{Spec} R$ be the complement of the closed set $V(f)$. Show that sets $D(f)$ form a base of Zariski topology, i.e. any Zariski open subset of $\operatorname{Spec} R$ can be expressed as a union of open sets of the form $D(f)$.

8. Let $x, y \in \operatorname{Spec} R$. Show that there exists either a neighborhood of x that does not contain y or a neighborhood of y that does not contain x.

9. Let $f : A \to B$ be a homomorphism of rings. (a) Show that in general the map $\alpha : \operatorname{MaxSpec} B \to \operatorname{MaxSpec} A$ is not always well-defined. (b) If A and B are finitely generated k-algebras then α is well-defined.

10. Let R be a direct product of rings $R_1 \times \ldots \times R_k$. Show that $\operatorname{Spec} R$ is homeomorphic to the disjoint union of spectra $\operatorname{Spec} R_1 \coprod \ldots \coprod \operatorname{Spec} R_k$.

11. (a) Show that the intersection of Zariski closed subsets $\cap_\alpha V(I_\alpha)$ of $\operatorname{Spec} R$ is empty if and only if $\sum_\alpha I_\alpha = R$. (b) Show that $\operatorname{Spec} R$ is quasi-compact, i.e. any open covering of $\operatorname{Spec} R$ has a finite sub-covering.

12. Let $\mathfrak{p} \subset R$ be a prime ideal. Let $I_1, \ldots, I_r \subset R$ be arbitrary ideals. (a) If $I_1 \cap \ldots \cap I_r \subset \mathfrak{p}$ then $I_j \subset \mathfrak{p}$ for some $j = 1, \ldots, r$. (b) If $I_1 \cap \ldots \cap I_r = \mathfrak{p}$ then $I_j = \mathfrak{p}$ for some $j = 1, \ldots, r$.

13. Let $J, I_1, \ldots, I_r$ be ideals of R such that $J \subset I_1 \cup \ldots \cup I_r$. Show that $J \subset I_k$ for some k if (a) $r = 2$; (b) all ideals $I_1, \ldots, I_r$ are prime. (c) at most two of the ideals $I_1, \ldots, I_r$ are not prime.

§9. LOCALIZATION AND LOCAL RINGS

§9.1. **Examples from number theory and geometry.**

EXAMPLE 9.1.1 (Number Theory). A typical example of localization is a formation of rational numbers as fractions of integers: $\mathbb{Z} \subset \mathbb{Q}$. But there are many other intermediate subrings between $\mathbb{Z}$ and $\mathbb{Q}$ formed by fractions with some condition on denominators. For example, we can invert only 2:

$$\mathbb{Z}[1/2] = \left\{ \frac{a}{2^n} \mid a \in \mathbb{Z}, \quad n \geq 0 \right\}.$$

A principal ideal (2) is maximal in $\mathbb{Z}$ but in $\mathbb{Z}[1/2]$ it gives the whole ring. Or we can invert everything *coprime* to 2 (i.e. odd):

$$\mathbb{Z}_{(2)} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}, \quad b \notin (2) \right\}.$$

This ring has only one maximal ideal, namely a principal ideal (2). Indeed, any element not in this ideal is invertible. This an example of a local ring:

DEFINITION 9.1.2. A ring is called *local* if it has only one maximal ideal.

In general, localization of the ring gives a ring with a simplified ideal structure: any ideal containing one of the denominators disappears.

EXAMPLE 9.1.3 (Geometry). In geometry we often study spaces *locally* in a neighborhood of a point. What are these neighborhoods in algebraic geometry? Consider the affine line $\mathbb{A}^1$ with ring of functions $k[x]$. Zariski neighborhoods of the origin $0 \in \mathbb{A}^1$ have form

$$U = \mathbb{A}^1 \setminus \{\alpha_1, \ldots, \alpha_r\}, \quad \alpha_i \neq 0 \quad \text{for any } i.$$

What are the functions on this neighborhood? We are algebraists, so we are interested in polynomial or rational functions defined in U, and so we take

$$\mathcal{O}(U) := \left\{ \frac{p(x)}{(x-\alpha_1)^{n_1} \ldots (x-\alpha_r)^{n_r}} \quad \middle| \quad p(x) \in k[x] \right\} \subset k(x)$$

$$= k\left[x, \frac{1}{x-\alpha_1}, \ldots, \frac{1}{x-\alpha_r}\right],$$

the ring obtained from $k[x]$ by inverting $x - \alpha_1, \ldots, x - \alpha_r$.

We can go further and invert all polynomials that don't vanish at 0:

$$k[x]_{(x)} = \left\{ \frac{f(x)}{g(x)} \quad \middle| \quad g \notin (x) \right\} \subset k(x).$$

This gives functions defined in *some* Zariski neighborhood of 0. The neighborhood depends on function: we have to throw away all roots of the denominator $g(x)$. The ring $k[x]_{(x)}$ is local: the only maximal ideal left is the principal ideal of x. A useful intuition in algebraic geometry is to think about $k[x]_{(x)}$ as functions on a small "local" neighborhood of $0 \in \mathbb{A}^1$, even though there is no Zariski neighborhood that can be used for that purpose.

§9.2. **Localization of rings.**

DEFINITION 9.2.1. A subset $S \subset R$ is called a *multiplicative system* if

- If $s, t \in S$ then $st \in S$.
- $1 \in S$, $0 \notin S$.

A localization $S^{-1}R$ is the set of equivalence classes of fractions

$$\left\{ \frac{r}{s} \quad \middle| \quad r \in R,\ s \in S \right\}.$$

Two fractions r/s and r'/s' are equivalent if there exists $t \in S$ such that

$$t(s'r - sr') = 0. \tag{9.2.1}$$

The ring structure on $S^{-1}R$ is defined using usual addition and multiplication of fractions. One has to check that these operations are well-defined. We have a homomorphism

$$R \to S^{-1}R, \quad r \mapsto \frac{r}{1}.$$

If R is not a domain then this homomorphism is not necessarily injective.

REMARK 9.2.2. If R is a domain then without loss of generality we can take $t = 1$ in (9.2.1), but in general we have to modify the usual cross-multiplication formula. This is because we want any $t \in S$ to become invertible in $S^{-1}R$. Suppose that $ta = 0$ in R for some $a \in R$. Then we should have $\frac{ta}{1} = 0$ in $S^{-1}R$. Since $\frac{t}{1}$ is invertible, we should be able to conclude that $\frac{a}{1} = 0$, i.e. that fractions $\frac{a}{1}$ and $\frac{0}{1}$ are equivalent. And according to our definition they are because $t(1 \cdot a - 0 \cdot 1) = 0$. We also see that it is possible that $a \neq 0$ in R but $\frac{a}{1} = 0$ in $S^{-1}R$.

LEMMA 9.2.3. *The ring $S^{-1}R$ is well-defined.*

Proof. A tedious calculation. □

EXAMPLE 9.2.4. If R is a domain then $S = R \setminus \{0\}$ is a multiplicative system. The localization $S^{-1}R$ is the quotient field of R. More generally, for any ring R, we can take S to be the set of all non-zerodivisors. The localization $S^{-1}R$ is called a *total ring of fractions*.

EXAMPLE 9.2.5. Suppose $x \in R$ is not a nilpotent element. Then

$$S = \{1, x, x^2, x^3, \ldots\}$$

is a multiplicative system. The localization $S^{-1}R$ is often denoted by $R\left[\frac{1}{x}\right]$.

Here is perhaps the most important example of localization:

DEFINITION 9.2.6. Let $\mathfrak{p} \subset R$ be a prime ideal, i.e.

$$\text{if } xy \in \mathfrak{p} \text{ then either } x \in \mathfrak{p} \text{ or } y \in \mathfrak{p}.$$

A contrapositive of this statement shows that $S = R \setminus \mathfrak{p}$ is a multiplicative system. The corresponding localization $S^{-1}R$ is denoted by $R_{\mathfrak{p}}$ and called *the localization of R at $\mathfrak{p}$*.

EXAMPLE 9.2.7. Take a prime ideal $(x) \subset k[x]$, the ideal of polynomial functions that vanish at $0 \in \mathbb{A}^1$. Then $k[x]_{(x)}$ is the ring of all rational functions of the form $\frac{f(x)}{g(x)}$ such that $g(x) \notin (x)$, i.e. such that $g(0) \neq 0$.

§9.3. **Extension and contraction of ideals in R and $S^{-1}R$.** .

DEFINITION 9.3.1. Let $f : A \to B$ be a homomorphism of rings. For any ideal $J \subset B$, the ideal $f^{-1}(J)$ of A is called a *contraction* of J. For any ideal $I \subset A$, the ideal $Bf(I)$ of B is called an *extension* of I (notice that $f(I)$ itself is almost never an ideal unless f is surjective).

Applying this construction for the localization gives

DEFINITION 9.3.2. For any ideal $I \subset R$, its extension $S^{-1}I \subset S^{-1}R$ is the subset of fractions of the form $\frac{x}{s}$ with $x \in I$, $s \in S$. Let $f : R \to S^{-1}R$ be the canonical map. If $J \subset S^{-1}R$ is an ideal then its contraction $f^{-1}(J) \subset R$, abusing notation, it is often denoted by $J \cap R$.

PROPOSITION 9.3.3. *We have the following properties:*

- *The mapping $I \mapsto S^{-1}I$ is a $1:1$ mapping of the set of all contracted ideals of R (i.e. ideals of the form $R \cap J$) to the set of all ideals of $S^{-1}R$.*
- *Prime ideals of $S^{-1}R$ are in $1:1$ correspondence ($\mathfrak{p} \leftrightarrow S^{-1}\mathfrak{p}$) with prime ideals of R that don't intersect S.*

Proof. Let $J \subset S^{-1}R$ be an ideal and let $r/s \in J$. Then $r = s(r/s) \in J$, and therefore $r \in R \cap J$. It follows that $J \subset S^{-1}(R \cap J)$. The other inclusion is obvious, and so we have

$$J = S^{-1}(R \cap J).$$

This proves the first part.

For the second part, if $I \subset R$ is any ideal that intersects S then of course $S^{-1}I = R^{-1}S$. We claim that if $\mathfrak{p} \subset R$ is a prime ideal that does not intersect S then $S^{-1}\mathfrak{p}$ is also prime. Indeed, suppose we have

$$\frac{r}{s}\frac{r'}{s'} = \frac{x}{t},$$

where $x \in \mathfrak{p}$. Then $u(trr' - xss') = 0$ for some $u \in S$. It follows that $trr' - xss' \in \mathfrak{p}$, and therefore $trr' \in \mathfrak{p}$. This implies that r or r' is in $\mathfrak{p}$, i.e. $\frac{r}{s}$ or $\frac{r'}{s'}$ is in $S^{-1}\mathfrak{p}$. In the other direction, if $J \subset S^{-1}R$ is a prime ideal then $R \cap J$ is also a prime ideal. This is true for any homomorphism $f : A \to B$: if $J \subset B$ is a prime ideal then $f^{-1}(J) \subset A$ is also a prime ideal. □

In the language of spectra, the homomorphism $R \to S^{-1}R$ induces an injective map of spectra $\operatorname{Spec} S^{-1}R \hookrightarrow \operatorname{Spec} R$. The image consists of prime ideals which do not intersect S.

LEMMA 9.3.4. *$R_{\mathfrak{p}}$ is a local ring with a maximal ideal $\mathfrak{p}_{\mathfrak{p}}$ (extension of $\mathfrak{p}$).*

Proof. We will use the following simple observation: If A is a local ring with a maximal ideal $\mathfrak{m}$ then any $x \notin \mathfrak{m}$ is not contained in a proper ideal and therefore is invertible. Elements in $\mathfrak{m}$ are of course not invertible. And the other way around, if $A^* \subset A$ is the set of invertible elements (units) and $\mathfrak{m} = A \setminus A^*$ happens to be an ideal of A then A is a local ring with a maximal ideal $\mathfrak{m}$, because any proper ideal does not intersect A^*.

Returning to $R_{\mathfrak{p}}$, let $\mathfrak{m}$ be the extension of the ideal $\mathfrak{p}$. This is a proper ideal by the previous proposition. But any element not in $\mathfrak{m}$ has form r/s with $r, s \notin \mathfrak{p}$, which is obviously invertible in $R_{\mathfrak{p}}$. So $R_{\mathfrak{p}}$ is a local ring. □

Localization is used when we want to focus on ideals disjoint from S. We give two examples of using this idea in arguments.

§9.4. **Nilradical.**

PROPOSITION 9.4.1. *Let R be a commutative ring. The intersection of all its prime ideals is equal to the set of nilpotent elements (called the nilradical) of R:*

$$\bigcap_{\mathfrak{p}\in\operatorname{Spec} R} \mathfrak{p} = \{x \in R \,|\, x^n = 0 \text{ for some } n > 0\}.$$

Proof. If $\mathfrak{p}$ is a prime ideal and $x^n = 0$ for some n then $x^n \in \mathfrak{p}$ and therefore $x \in \mathfrak{p}$. Now suppose that x is not nilpotent. Then

$$S = \{1, x, x^2, \dots\}$$

is a multiplicative system. Consider the localization $S^{-1}R$ and any maximal (and hence prime) ideal I of it. Then $\mathfrak{p} = R \cap I$ is a prime ideal of R that does not intersect S, and therefore does not contain x. □

§9.5. **Going-up Theorem.**

THEOREM 9.5.1 (Going-up Theorem). *Let $A \subset B$ be rings and suppose that B is integral over A. Then the pull-back map* $\operatorname{Spec} B \to \operatorname{Spec} A$ *is surjective.*

Proof. We have to show that for any prime ideal $\mathfrak{p} \subset A$, there exists a prime ideal $\mathfrak{q} \subset B$ such that

$$\mathfrak{p} = \mathfrak{q} \cap A.$$

Let $S \subset A$ be a complement of $\mathfrak{p}$. We can view S as a multiplicative system not only in A but also in B. Localizing at S gives a commutative diagram

$$\begin{array}{ccc} B & \xrightarrow{\alpha} & S^{-1}B \\ \uparrow & & \uparrow \\ A & \xrightarrow{\beta} & A_{\mathfrak{p}} \end{array} \tag{9.5.1}$$

where the vertical arrows are inclusions. Notice that $S^{-1}B$ is integral over $A_{\mathfrak{p}}$: if $b \in B$ is a root of a monic polynomial

$$b^n + a_1 b^{n-1} + \ldots + a_n = 0$$

then b/s for $s \in S$ is a root of a monic polynomial

$$(b/s)^n + (a_1/s)(b/s)^{n-1} + \ldots + (a_n/s^n) = 0.$$

Suppose we can prove the theorem for $A_{\mathfrak{p}} \subset S^{-1}B$. Then there exists a prime ideal J of $S^{-1}B$ such that $J \cap A_{\mathfrak{p}} = S^{-1}\mathfrak{p}$. Let $\mathfrak{q} = \alpha^{-1}(J)$. We claim that $\mathfrak{q} \cap A = \mathfrak{p}$. This follows from commutativity of the diagram (9.5.1) and because $\beta^{-1}(S^{-1}\mathfrak{p}) = \mathfrak{p}$ by Prop. 9.3.3.

It remains to consider the case when A is a local ring with a maximal ideal $\mathfrak{m}$. Let $\mathfrak{m}' \subset B$ be any maximal ideal. We claim that $\mathfrak{m}' \cap A = \mathfrak{m}$. In

any case, $\mathfrak{m}' \cap A \subset \mathfrak{m}$ because $\mathfrak{m}' \cap A$ is a proper ideal of A and $\mathfrak{m}$ is its only maximal ideal. We have a commutative diagram

$$\begin{array}{ccc} B & \longrightarrow & B/\mathfrak{m}' \\ \uparrow & & \uparrow \\ A & \longrightarrow & A/(\mathfrak{m}' \cap A) \end{array}$$

where the vertical arrows are inclusions. Notice that $B/\mathfrak{m}'$ is a field integral over $A/(\mathfrak{m}' \cap A)$. But then $A/(\mathfrak{m}' \cap A)$ is a field (see the proof of Lemma 8.1.3). So $\mathfrak{m}' \cap A$ is a maximal ideal, and therefore $\mathfrak{m}' \cap A = \mathfrak{m}$. $\square$

EXAMPLE 9.5.2. Consider the embedding $f : \mathbb{Z} \hookrightarrow \mathbb{Z}[i]$. Since i is a root of a monic polynomial $T^2 + 1 = 0$, this is an integral extension. These rings are PIDs, and non-zero prime ideals correspond to primes (irreducible elements) in $\mathbb{Z}$ and in $\mathbb{Z}[i]$, respectively (up-to association).

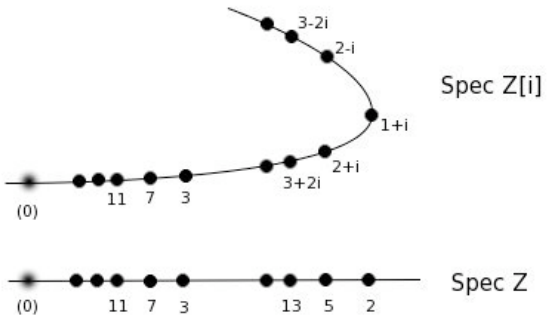
Suppose $\gamma \in \mathbb{Z}[i]$ is prime and let $p \in \mathbb{Z}$ be a prime such that $(p) = (\gamma) \cap \mathbb{Z}$. We have a commutative diagram

$$\begin{array}{ccc} \mathbb{Z}/(p) & \hookrightarrow & \mathbb{Z}[i]/(p) \\ & \searrow & \downarrow \\ & & \mathbb{Z}[i]/(\gamma) \end{array}$$

The field extension $\mathbb{Z}/(p) \subset \mathbb{Z}[i]/(\gamma)$ is generated by the image of i in $\mathbb{Z}[i]/(\gamma)$, and consequently has degree 1 or 2 depending on whether -1 is a square in $\mathbb{Z}/(p)$ or not. If -1 is not a square then the map $\mathbb{Z}[i]/(p) \to \mathbb{Z}[i]/(\gamma)$ is an isomorphism (as both sets have p^2 elements and this map is surjective). Therefore, in this case $(p) = (\gamma)$ and $p = \gamma$ up to association. If -1 is a square modulo p then $\mathbb{Z}[i]/(\gamma)$ has p elements. The number of elements in $\mathbb{Z}[i]/(\gamma)$ is the area of the square with sides γ and $i\gamma$, therefore, $|\gamma| = \sqrt{p}$. It follows that $\gamma\overline{\gamma} = p$. Since $\mathbb{Z}[i]$ is a PID, it follows that there are exactly two possibilities for γ, unless γ and $\overline{\gamma}$ are associate, i.e. if $\gamma/\overline{\gamma}$ is a unit in $\mathbb{Z}[i]$. There are just 4 units, ± 1 and $\pm i$, and it is easy to see that γ and $\overline{\gamma}$ are associate if and only if $\gamma = 1 + i$ (up to association).

Finally, it is very easy to see (using the fact that $\mathbb{F}_p^*$ is cyclic) that -1 is not a square modulo p if and only if $p \equiv 3 \mod 4$.

So the full picture of the pull-back map of spectra is as follows:



§9.6. **Finite morphisms.** Now let's translate some algebra into geometry.

DEFINITION 9.6.1. A morphism of affine algebraic sets $X \to Y$ is called *finite* if $\mathcal{O}(X)$ is integral over $\mathcal{O}(Y)$ via the pull-back $\mathcal{O}(Y) \to \mathcal{O}(X)$.

EXAMPLE 9.6.2. This gives a geometric way to reformulate Noether's normalization lemma: any closed algebraic set X admits a dominant finite morphism to $\mathbb{A}^n$ for some n. Moreover, the proof in §7.4 gives the following more accurate statement: if $X \subset \mathbb{A}^m$ is a closed algebraic subset then we can choose a direct sum decomposition of vector spaces $\mathbb{A}^m = \mathbb{A}^n \oplus \mathbb{A}^r$ such that the projection of X onto $\mathbb{A}^n$ along $\mathbb{A}^r$ is a finite morphism.

THEOREM 9.6.3. *Any dominant finite morphism is surjective and has finite fibers.*

Proof. Let $\alpha : X \to Y$ be a dominant finite morphism. Let $A = \mathcal{O}(X)$ and let $B = \mathcal{O}(Y)$. By Lemma 8.8.3, we can identify B with a subring of A via the pull-back homomorphism. By definition of a finite morphism, A is integral over B. Let $y \in Y$. It corresponds to a maximal ideal $\mathfrak{m} \subset B$. To show that α is surjective, we have to check that there exists a maximal ideal $\mathfrak{n} \subset A$ such that $\mathfrak{n} \cap B = \mathfrak{m}$ and to show that α has finite fibers, we have to check that there are only finitely many possible $\mathfrak{n}$'s. By the going-up theorem, we can find a prime ideal $\mathfrak{p} \subset A$ such that $\mathfrak{p} \cap B = \mathfrak{m}$. But then $A/\mathfrak{p}$ is a domain integral over a field $k = B/\mathfrak{m}$, and so $A/\mathfrak{p}$ is also a field, and so $\mathfrak{p}$ is in fact a maximal ideal.

There is a natural bijection between the set of maximal ideals $\mathfrak{n} \subset A$ such that $\mathfrak{n} \cap B = \mathfrak{m}$ and $\operatorname{MaxSpec} A/A\mathfrak{m}$. The algebra $A/A\mathfrak{m}$ is finitely generated and integral over $B/\mathfrak{m} = k$, and so is a finitely generated k-module, i.e. a finite-dimensional vector space. Since any ideal of $A/A\mathfrak{m}$ is a vector subspace, we see that $A/A\mathfrak{m}$ satisfies a descending chain condition for ideals. So it is enough to prove Lemma 9.6.5 below. □

DEFINITION 9.6.4. A ring R is called *Artinian* if it satisfies d.c.c. for ideals.

LEMMA 9.6.5. *Any Artinian ring R has the following properties:*

- *Any prime ideal of R is maximal.*
- *R has only finitely many maximal ideals.*

Proof. For the first statement, if $\mathfrak{p} \subset R$ is a prime ideal then $R/\mathfrak{p}$ is an Artinian domain. For any $x \in R/\mathfrak{p}$, the sequence

$$(x) \supset (x^2) \supset (x^3) \supset \dots$$

stabilizes, and therefore $x^n = x^{n+1}y$ for some n and for some $y \in R/\mathfrak{p}$, but this implies that $1 = xy$. So $R/\mathfrak{p}$ is a field and $\mathfrak{p}$ is maximal.

For the second statement, consider the set of finite intersections of maximal ideals. By d.c.c, this set has the minimal element, i.e. there exist maximal ideals $\mathfrak{m}_1, \dots, \mathfrak{m}_r \subset R$ such that

$$\mathfrak{m} \cap \mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_r = \mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_r$$

for any maximal ideal $\mathfrak{m}$, or equivalently

$$\mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_r \subset \mathfrak{m}.$$

We claim that this implies that $\mathfrak{m} = \mathfrak{m}_i$ for some i. If not, then each $\mathfrak{m}_i$ contains x_i such that $x_i \notin \mathfrak{m}$. But then

$$x_1 \dots x_r \in \mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_r \subset \mathfrak{m},$$

and since $\mathfrak{m}$ is prime, one of the x_i's is contained in $\mathfrak{m}$, contradiction. □

EXAMPLE 9.6.6. Consider projection α of the parabola $X = V(y - x^2) \subset \mathbb{A}^2$ onto the y-axis $Y = \mathbb{A}^1_y$. The pull-back homomorphism α^* is

$$k[y] = \mathcal{O}(Y) \to \mathcal{O}(X) = k[x, y]/(x^2 - y) \simeq k[x], \quad y \mapsto x^2.$$

Since x is a root of a monic polynomial $T^2 - y$, $\mathcal{O}(X)$ is integral over $\mathcal{O}(Y)$, and so α is a finite morphism. The preimage of any point $a \in \mathbb{A}^1_y$ is obviously $\pm\sqrt{a}$, i.e. either one (if $a = 0$) or two (if $a \neq 0$) points. Analysis used in the proof of Theorem 9.6.3 gives us a bit more: points in the preimage of $a \in \mathbb{A}^1_y$ correspond to maximal ideals of the Artinian k-algebra

$$k[x]/(x^2 - a) \simeq \begin{cases} \frac{k[x]}{(x-\sqrt{a})} \oplus \frac{k[x]}{(x+\sqrt{a})} \simeq k \oplus k & \text{if } a \neq 0 \\ k[x]/(x^2) = \{a + b\epsilon \mid a, b \in k,\ \epsilon^2 = 0\} & \text{if } a = 0 \end{cases}$$

The algebra $k[x]/(x^2)$ is known as the *algebra of dual numbers*. It has only one maximal ideal (ϵ). However, this algebra is 2-dimensional as a vector space over k, just like the algebra $k \oplus k$. This reflects our intuition that the preimage of 0 should be one point but counted with multiplicity 2.

§9.7. **Localization of modules.** Localization of rings $R \mapsto S^{-1}R$ can be generalized to localization of modules.

DEFINITION 9.7.1. Let M be an R-module and let $S \subset R$ be a multiplicative system. We define $S^{-1}M$ as the set of equivalence classes of fractions m/s, where $m \in M$, $s \in S$. Two fractions m/s and m'/s' are called equivalent if there exists $t \in S$ such that

$$t(s'm - sm') = 0.$$

We make $S^{-1}M$ into an $S^{-1}R$-module by declaring that $r/s \in S^{-1}R$ acts on $m/t \in S^{-1}M$ by sending it to $(rm)/(st)$.

REMARK 9.7.2. Even when R is a domain, it can of course happen that $tm = 0$ for some $t \in S$, $m \in M \setminus \{0\}$. Then $m/1$ should be equal to 0 in $S^{-1}M$ because t is invertible in $S^{-1}R$. This explains appearance of t in the definition of equivalent fractions.

NOTATION 9.7.3. If $\mathfrak{p} \in \operatorname{Spec} R$ and $S = R \setminus \mathfrak{p}$ then $S^{-1}M$ is denoted by $M_{\mathfrak{p}}$.

LEMMA 9.7.4. *Localization of modules is well-defined.*

Proof. A tedious calculation. □

LEMMA 9.7.5. *Localization is a special case of extension of scalars:*

$$S^{-1}M \simeq S^{-1}R \otimes_R M.$$

Proof. Consider a bilinear map of R modules

$$S^{-1}R \times M \to S^{-1}M, \quad \left(\frac{r}{s}, m\right) \mapsto \frac{rm}{s}.$$

It induces a surjective map of R-modules

$$\psi : S^{-1}R \otimes_R M \to S^{-1}M.$$

Why is it injective? Any element of $S^{-1}R \otimes_R M$ can be written as

$$\sum_i \frac{r_i}{s_i} \otimes m_i = \sum_i \frac{t_i r_i}{s} \otimes m_i \qquad (\text{where } s = \prod_j s_j \text{ and } t_i = \prod_{j \neq i} s_j)$$

$$= \sum_i \frac{1}{s} \otimes t_i r_i m_i = \frac{1}{s} \otimes m \qquad (\text{where } m = \sum_i t_i r_i m_i).$$

If $0 = \psi(\frac{1}{s} \otimes m) = \frac{m}{s}$ then $tm = 0$ for some $t \in S$. But then

$$\sum_i \frac{r_i}{s_i} \otimes m_i = \frac{1}{s} \otimes m = \frac{t}{ts} \otimes m = \frac{1}{ts} \otimes tm = 0.$$

So ψ is injective. □

§9.8. **Localization is exact.**

LEMMA 9.8.1. *If*

$$0 \to M \to N \to K \to 0$$

is an exact sequence of R-modules then

$$0 \to S^{-1}M \to S^{-1}N \to S^{-1}K \to 0$$

is an exact sequence of $S^{-1}R$-modules. In particular, if $M \subset N$ then we can view $S^{-1}M$ as a submodule of $S^{-1}N$.

Proof. Any extension of scalars, and more generally tensoring with any R-module, is right-exact. So

$$S^{-1}M \to S^{-1}N \to S^{-1}K \to 0$$

is exact. It remains to show that if $M \xrightarrow{\phi} N$ is injective then $S^{-1}M \xrightarrow{\psi} S^{-1}N$ is also injective. If $\psi(\frac{m}{s}) = \frac{\phi(m)}{s} = 0$ in $S^{-1}N$ then $t\phi(m) = \phi(tm) = 0$ for some $t \in S$. But then $tm = 0$ in M and therefore $\frac{m}{s} = 0$ in $S^{-1}M$. □

REMARK 9.8.2. We can view the second sequence of the lemma as the first sequence tensored with $S^{-1}R$. In the language of flat modules, the lemma says that $S^{-1}R$ is a flat R-module.

§9.9. **Nakayama's Lemma.** Nakayama's Lemma is usually used in the following form:

LEMMA 9.9.1 (Nakayama's Lemma - I). *Let R be a local ring with a maximal ideal $\mathfrak{m}$ and let M be a finitely generated R-module. Let $s_1, \ldots, s_n \in M$. If these elements generate M modulo $\mathfrak{m}M$ then in fact they generate M.*

This follows from

LEMMA 9.9.2 (Nakayama's Lemma - II). *Let R be a local ring with a maximal ideal $\mathfrak{m}$ and let M be a finitely generated R-module. If $\mathfrak{m}M = M$ then $M = 0$.*

Indeed, let N be a submodule of M generated by $s_1, \ldots, s_n$. Then we are given that $M = N + \mathfrak{m}M$, i.e. that $M/N = \mathfrak{m}(M/N)$. We deduce that $M/N = 0$, i.e. that $M = N$.

To prove version II, we are going to use the "adjoint matrix/determinant" trick we used to show that $x \in B$ is integral over a subring $A \subset B$ if and only if x is contained in a finitely generated A-submodule of B.

We will prove a slightly more general result. Let R be any ring and let M be a finitely generated R-module. Claim: if I is an ideal contained in all maximal ideals and $IM = M$ then $M = 0$.

Let $m_1, \ldots, m_k$ be generators of M. We have

$$m_i = \sum a_{ij} m_j, \quad \text{where } a_{ij} \in I.$$

Then

$$\sum_j (\delta_{ij} - a_{ij}) m_j = 0$$

for any i. Multiplying by the adjoint matrix, we see that

$$a m_j = 0 \quad \text{for any } j,$$

where $a = \det(\delta_{ij} - a_{ij})$ can be written as $1 + x$, where $x \in I$. We claim that a is invertible, and therefore

$$m_j = a^{-1}(a m_j) = 0 \quad \text{for any } j,$$

and therefore $M = 0$. If a is not invertible then it belongs to some maximal ideal $\mathfrak{m} \subset R$. But $x \in I \subset \mathfrak{m}$, and so $1 = a - x \in \mathfrak{m}$, a contradiction.

Homework 9

Let R be a commutative ring (with 1).

1. (a) Show that the nilradical of R is a prime ideal if and only if $\operatorname{Spec} R$ contains a "generic point" η, i.e. a point such that $\bar{\eta} = \operatorname{Spec} R$. (b) Let $I \subset R$ be an ideal. Show that

$$\sqrt{I} = \bigcap_{\substack{\mathfrak{p} \in \operatorname{Spec} R \\ I \subset \mathfrak{p}}} \mathfrak{p}.$$

2. Let $\phi : A \to B$ be a homomorphism of rings. Construct a bijection

$$\{\text{contracted ideals in } A\} \quad \leftrightarrow \quad \{\text{extended ideals in } B\}.$$

3. Let R be a ring and let Σ be the set of its multiplicative systems. Show that Σ contains maximal (by inclusion) subsets and that $S \in \Sigma$ is maximal if and only if $R \setminus S$ is a minimal (by inclusion) prime ideal.

4. Let $A \subset B$ be domains. Suppose $B \setminus A$ is multiplicatively closed in B. Show that A is integrally closed in B.

5. Let R be a ring and let $\mathfrak{p} \subset R$ be a prime ideal. (a) Show that the localization $R_{\mathfrak{p}}$ is a field if and only if for any element $x \in \mathfrak{p}$ there exists $y \notin \mathfrak{p}$ such that $xy = 0$. (b) Find an example of a commutative ring R and a prime ideal $\mathfrak{p} \neq 0$ such that $R_{\mathfrak{p}}$ is a field.

6. Let R be a ring with only finitely many maximal ideals. Suppose that for each maximal ideal $\mathfrak{m} \subset R$, $R_{\mathfrak{m}}$ is Noetherian. Prove that (a) the product of localization maps $R \mapsto \prod_{\mathfrak{m}} R_{\mathfrak{m}}$ is an embedding; (b) R is Noetherian.

7. Consider the following ideal

$$P = (2, 1 + \sqrt{-5}) \subset R = \mathbb{Z}[\sqrt{-5}].$$

(a) Show that P is maximal but not principal. (b) Show that the extended ideal $P_P \subset R_P$ is principal.

8. Let $A \subset B$ be rings, B is integral over A. Let $\mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_n$ be a chain of prime ideals of A and let $\mathfrak{q}_1 \subset \ldots \subset \mathfrak{q}_m$ $(m < n)$ be a chain of prime ideals of B such that $\mathfrak{q}_i \cap B = \mathfrak{p}_i$ for $i \leq m$. Then the $\mathfrak{q}$-chain can be extended to a chain $\mathfrak{q}_1 \subset \ldots \subset \mathfrak{q}_n$ such that $\mathfrak{q}_i \cap B = \mathfrak{p}_i$ for all i.

9. Show that the ring R is reduced if and only if $R_{\mathfrak{p}}$ s reduced for any prime ideal $\mathfrak{p} \subset R$.

10. Let R be a domain and let $I \subset R$ be an ideal. An element $x \in R$ is called integral over I if it satisfies an equation of the form $x^n + a_1 x_{n-1} + \ldots + a_n = 0$ with $a_k \in I^k$, the k-th power of the ideal I, for each $k \geq 1$. Show that x is integral over I if and only if there exists a finitely generated R-module M, not annihilated by any element of R, such that $xM \subset IM$.

11. Let R be a ring. Let M_1 and M_2 be submodules of an R-module N.

$$(a) \qquad (S^{-1}M_1) + (S^{-1}M_2) = S^{-1}(M_1 + M_2);$$

$$(b) \qquad (S^{-1}M_1) \cap (S^{-1}M_2) = S^{-1}(M_1 \cap M_2);$$

$$(c) \qquad \text{if } M_1 \supset M_2 \text{ then} \quad S^{-1}(M_1/M_2) \simeq (S^{-1}M_1)/(S^{-1}M_2).$$

12. Let R be a ring. Let M be a finitely generated R-module. Show that

$$S^{-1}(\operatorname{Ann} M) \simeq \operatorname{Ann}(S^{-1}M).$$

§10. BONUS SECTION: A BIT MORE ALGEBRAIC GEOMETRY

§10.1. **Rational functions.**

DEFINITION 10.1.1. Let X be an affine variety. The field of fractions $k(X)$ of the domain $\mathcal{O}(X)$ is called the field of rational functions on X. For example,

$$k(\mathbb{A}^n) = k(x_1, \ldots, x_n).$$

Any rational function $f \in k(X)$ can be written as a ratio of 2 regular functions $p, q \in \mathcal{O}(X)$. It can be thought of as a function $X \setminus V(q) \to k$.

DEFINITION 10.1.2. A rational function $f \in k(X)$ is called *regular* at $x \in X$ if it can be written as p/q such that $q(x) \neq 0$. In terms of the the corresponding maximal ideal $\mathfrak{m} \subset \mathcal{O}(X)$, functions regular at x form a local ring $\mathcal{O}(X)_{\mathfrak{m}}$.

REMARK 10.1.3. If $\mathcal{O}(X)$ is not a UFD then fractions cannot be written in lowest terms, and it is not always obvious if $f \in k(X)$ is regular at $x \in X$. For example, consider the quadric cone

$$X = V(xy - z^2) \subset \mathbb{A}^3.$$

We claim that $x/z \in k(X)$ is regular at $p = (0, 1, 0) \in X$ even though $z(p) = 0$. Indeed, in $k(X)$ we have $x/z = z/y$ and $y(p) \neq 0$.

PROPOSITION 10.1.4. *Let X be an affine algebraic variety. Let $f \in k(X)$. Then f is regular at any point $x \in X$ if and only if $f \in \mathcal{O}(X)$.*

Proof. One direction is obvious. Suppose f is regular at any point $x \in X$, i.e. we can write $f = \frac{p_x}{q_x}$, where $q_x(x) \neq 0$. Consider an ideal $I \subset \mathcal{O}(X)$ generated by q_x for $x \in X$. Since $V(I) = \emptyset$, $\sqrt{I} = \mathcal{O}(X)$ by Nullstellensatz[6]. It follows that $1 \in I$, i.e. we can write

$$1 = a_1 q_{x_1} + \ldots + a_r q_{x_r} \quad \text{for some } x_1, \ldots, x_r \in X.$$

It follows that

$$f = f a_1 q_{x_1} + \ldots + f a_r q_{x_r} = \frac{p_{x_1}}{q_{x_1}} a_1 q_{x_1} + \ldots + \frac{p_{x_r}}{q_{x_r}} a_r q_{x_r} =$$
$$= p_{x_1} a_1 + \ldots + p_{x_r} a_r \in \mathcal{O}(X).$$

This idea is known as "algebraic partition of unity" trick. □

§10.2. **Dimension.**

There are two ways to think about dimension:

- Dimension is the number of independent parameters needed to specify a point. For example, our space is three-dimensional because we need three coordinates, x, y, and z.
- Dimension of space is 1 plus maximal dimension of its subspace. For example, our space is three-dimensinal because it contains flags

$$\{\text{point}\} \subset \{\text{curve}\} \subset \{\text{surface}\} \subset \{\text{space}\}$$

In Algebraic Geometry, these ideas can be made rigorous:

DEFINITION 10.2.1. Let X be an affine variety. We define

$$\dim X := \text{tr.deg.}_k k(X).$$

[6] We proved Nullstellensatz for $\mathcal{O}(\mathbb{A}^n)$. The general case is treated in the homework.

DEFINITION 10.2.2. Let R be any ring. We define its *Krull dimension* $\dim R$ as the maximal number r (possibly ∞) such that R contains a chain of prime ideals of length $r+1$:

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_r. \tag{10.2.1}$$

THEOREM 10.2.3. *Let X be an affine variety. Then*

$$\dim X = \dim \mathcal{O}(X).$$

Proof. Since $\mathcal{O}(X)$ is a finitely generated k-algebra, it is integral over a polynomial subalgebra $k[y_1, \ldots, y_n]$, by Noether's Normalization Lemma. Then $k(X)/k(y_1, \ldots, y_n)$ is an algebraic field extension, and we have

$$\dim X = \mathrm{tr.deg.}_k\, k(X) = \mathrm{tr.deg.}_k\, k(y_1, \ldots, y_n) = n.$$

Next we would like to show that

$$\dim \mathcal{O}(X) = \dim k[x_1, \ldots, x_n]. \tag{10.2.2}$$

Let (10.2.1) be any chain of prime ideals in $\mathcal{O}(X)$. Then $\mathfrak{q}_i := \mathfrak{p}_i \cap k[x_1, \ldots, x_n]$ are prime ideals in $k[x_1, \ldots, x_n]$. We claim that $\mathfrak{q}_i \neq \mathfrak{q}_{i+1}$ for any i. Indeed, suppose $q_i = q_{i+1}$. Then $B := \mathcal{O}(X)/\mathfrak{p}_i$ is integral over $A := k[x_1, \ldots, x_n]/\mathfrak{q}_i$. Let $S = A \setminus \{0\}$. Then $S^{-1}B$ is integral over $S^{-1}A$, which is the field of fractions of A. By the standard lemma, it follows that $S^{-1}B$ is also a field. However, $S^{-1}\mathfrak{p}_{i+1}$ is its proper ideal, contradiction. Next take any chain

$$\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \ldots \subsetneq \mathfrak{q}_s$$

of prime ideals in $k[x_1, \ldots, x_n]$. By the Going-up Theorem[7], we can lift this chain to the chain

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_s$$

of prime ideals in $\mathcal{O}(X)$. The formula (10.2.2) follows. At this point everything is reduced to showing that

$$\dim k[x_1, \ldots, x_n] = n.$$

Existence of the chain of prime ideals

$$0 \subsetneq (x_1) \subsetneq (x_1, x_2) \subsetneq \ldots \subsetneq (x_1, \ldots, x_n)$$

shows that $\dim k[x_1, \ldots, x_n] \geq n$. For an opposite inequality, consider a chain of prime ideals

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_s \subset k[x_1, \ldots, x_n].$$

It gives a chain of affine varieties

$$V(\mathfrak{p}_s) \subsetneq V(\mathfrak{p}_{s-1}) \subsetneq \ldots \subsetneq V(\mathfrak{p}_0) \subset \mathbb{A}^n.$$

Since $\dim \mathbb{A}^n = n$, it suffices to prove the following Lemma 10.2.4. □

LEMMA 10.2.4. *Let $X \subset Y$ be affine varieties. Then $\dim X \leq \dim Y$. Moreover, if $X \neq Y$ then $\dim X < \dim Y$.*

[7] In our version of the Going-up Theorem, we showed how to lift one prime ideal. For this slightly more general version, see the homework.

Proof. The affine variety Y is a closed algebraic subset of $\mathbb{A}^N_{t_1,\ldots,t_N}$. Let $n = \dim Y$. Since $\mathcal{O}(Y)$, and therefore $k(Y)$, is generated by restrictions of $t_1, \ldots, t_N$, any $n+1$ of these restrictions are algebraically dependent. The same is true for their restrictions on X, and therefore $\dim X \leq n$.

Now let's suppose that $\dim X = n$. Then some n of the coordinates are algebraically independent in $k(X)$, and therefore also in $k(Y)$. Without loss of generality we can assume that restrictions of $t_1, \ldots, t_n$ are these algebraically independent coordinates. If $X \neq Y$ then we can find a non-zero $u \in \mathcal{O}(Y)$ such that $u|_X = 0$. Since u is algebraic over $k(t_1, \ldots, t_n)$, we have the following identity along Y:

$$a_0 u^m + \ldots + a_m = 0, \quad \text{where } a_i \in k[t_1, \ldots, t_n] \text{ for } i = 0, \ldots, m.$$

We can assume that $a_m(t_1, \ldots, t_n)$ is a non-vanishing polynomial (otherwise divide this identity by u). But since $u|_X = 0$, we have $a_m|_X = 0$. But $t_1, \ldots t_n$ are algebraically independent in $\mathcal{O}(X)$, a contradiction. $\square$

§10.3. **Discrete Valuation Rings.** Domains of Krull dimension 0 are fields. How to characterize domains R with $\dim R = 1$? In these domains every non-zero prime ideal is maximal, for example any PID such as $\mathbb{Z}$ or $k[x]$. More generally, Noetherian integrally closed domains of Krull dimension 1 are called *Dedekind domains*. For example, any ring of algebraic integers and any coordinate ring of an affine algebraic curve are Dedekind domains. A satisfactory structure theory of these rings is available, but we are only going to focus on the local case.

DEFINITION 10.3.1. A *discrete valuation* of a field K is a function $v : K^* \to \mathbb{Z}$ such that

- $v(xy) = v(x) + v(y)$;
- $v(x+y) \geq \min(v(x), v(y))$;
- $v(K^*) = \mathbb{Z}$.

The subring $R = \{x \in K \,|\, v(x) \geq 0$ is called the *valuation ring of* v.

A domain R is called a DVR (Discrete Valuation Ring) if its field of fractions has a discrete valuation such that R is its valuation ring.

EXAMPLE 10.3.2. The localization $Z_{(p)}$ is a DVR. Indeed, let's define a function $v : \mathbb{Q}^* \to \mathbb{Z}$ as follows: $v(x) = n$ if $x = p^n \frac{a}{b}$, where $a, b \in \mathbb{Z}$ are coprime to p. All properties of a discrete valuation can be immediately checked. Notice that $v(x) \geq 0$ if and only if x can be written as $\frac{a}{b}$ where $a, b \in \mathbb{Z}$ and b is coprime to p, i.e. if and only if $x \in \mathbb{Z}_{(p)}$. More generally, this construction shows that $R_{(f)}$ is a DVR for any irreducible element f of a UFD R. Example: $k[x]_{(x-a)}$ for any $a \in k$.

LEMMA 10.3.3. *Let v be any discrete valuation of a field K. Its valuation ring R is a local ring with maximal ideal $\mathfrak{m} = \{x \in R \,|\, v(x) > 0\}$ and field of fractions K.*

Proof. R is a ring. Indeed, if $v(x), v(y) \geq 0$ then $v(xy) = v(x) + v(y) \geq 0$ and $v(x+y) \geq \min(v(x), v(y)) \geq 0$. Since $v(1) = v(1 \cdot 1) = v(1) + v(1)$, we have $v(1) = 0$. So R is a ring with unity.

Let $x \in K$. If $v(x) \geq 0$ then $x \in R$. If $v(x) < 0$ then $x^{-1} \in R$ because $v(x^{-1}) = v(1) - v(x) > 0$. It follows that K is the field of fractions of R.

To show that $\mathfrak{m}$ is an ideal of R, suppose that $r \in R$ and $x, y \in \mathfrak{m}$. Then $v(rx) = v(r) + v(x) > 0$ and $v(x+y) \geq \min(v(x), v(y)) > 0$. Therefore, $rx \in \mathfrak{m}$ and $x + y \in \mathfrak{m}$.

If $x \in R$ and $v(x) = 0$ then $v(x^{-1}) = -v(x) = 0$, and therefore x is a unit in R. If $v(x) > 0$ then $x \in \mathfrak{m}$. So R is a local ring with maximal ideal $\mathfrak{m}$ (see the proof of Lemma 9.3.4). $\square$

The following theorem gives a nice characterization of DVRs. In the course of the proof we will discover other interesting things about DVRs.

THEOREM 10.3.4. *Let R be a ring. TFAE:*

(1) *R is a DVR.*
(2) *R is a Noetherian, integrally closed, local domain of Krull dimension 1.*

Proof. Let R be a DVR. We already know that R is a local domain with maximal ideal $\mathfrak{m}$.

Let $t \in \mathfrak{m}$ be any element such that $v(t) = 1$. We claim that $\mathfrak{m} = (t)$. More generally, we claim that any ideal I of R has form (t^n), where n is the minimal integer such that I contains an element x such that $v(x) = n$. Indeed, since $v(t^n/x) = 0$, t^n/x is a unit in R, and therefore t^n and x are associate, and in particular $t^n \in I$. If $y \in I$ then $v(y) \geq n$, and therefore $v(y/t^n) \geq 0$ and so $y/t^n \in R$. It follows that $I = (t^n)$.

Calculations of the previous paragraph show, in particular, that R is a PID and therefore is integrally closed and has Krull dimension 1.

Now let's fix a Noetherian, integrally closed, local domain R of Krull dimension 1. Let $\mathfrak{m} \in R$ be its only maximal ideal. Let

$$I = \bigcap_{n \geq 1} \mathfrak{m}^n.$$

Since R is Noetherian, I is a finitely generated R-module. Since $I = \mathfrak{m}I$, in fact $I = 0$ by Nakayama's lemma.

CLAIM 10.3.5. *The maximal ideal $\mathfrak{m}$ is principal, $\mathfrak{m} = (t)$.*

Given the claim, let's show that R is a DVR. Let $x \in R$. Since $I = 0$, we can find an integer n such that $x \in \mathfrak{m}^n = (t^n)$ but $x \notin \mathfrak{m}^{n+1} = (t^{n+1})$. It follows that $x = t^n u$, where $u \notin \mathfrak{m}$, i.e. u is a unit of R. It follows that any $x \in K^*$ can be written as $t^n u$, where $n \in \mathbb{Z}$ and $u \in R$ is a unit. This expression is unique, and therefore we can define a function $v : K^* \to \mathbb{Z}$, $v(x) = n$. It is straightforward to check all axioms of the valuation.

Let's prove the claim. By Nakayama's lemma, $\mathfrak{m} \neq \mathfrak{m}^2$. Let $t \in \mathfrak{m} \setminus \mathfrak{m}^2$. Since $\dim R = 1$, $\mathfrak{m}$ is the only non-zero prime ideal of R. It follows that

$$\mathfrak{m} = \sqrt{(t)}.$$

This implies that $\mathfrak{m}^n \subset (t)$ for some n. Indeed, since R is Noetherian, $\mathfrak{m}$ has finitely many generators $x_1, \ldots, x_r$ and we can choose $N > 0$ such that $x_i^N \in (t)$ for any i. Then $y_1 \ldots y_m \in (t)$ for any $y_1, \ldots, y_m \in \mathfrak{m}$ as long as $m > r(N-1)$. Let n be the integer such that $\mathfrak{m}^n \subset (t)$ but $\mathfrak{m}^{n-1} \not\subset (t)$. Let $b \in \mathfrak{m}^{n-1} \setminus (t)$. Let $x = t/b \in K$. Then $x^{-1} \notin R$ (since $b \notin (t)$). Since R is integrally closed, x^{-1} is not integral over R. It follows that $x^{-1}\mathfrak{m} \not\subset \mathfrak{m}$ (since $\mathfrak{m}$ is a finitely generated R-module). But $x^{-1}\mathfrak{m} \subset R$ (since if $z \in \mathfrak{m}$

then $bz \in \mathfrak{m}^n \subset (t)$ and therefore $x^{-1}z \in R$). It follows that $x^{-1}\mathfrak{m} = R$, i.e. that $\mathfrak{m} = (x)$. $\square$

Homework 10

Let R be a commutative ring (with 1). Let k be an algebraically closed field.

1. Let R be a ring. Let M_1 and M_2 be R-modules. Show that

$$S^{-1}(M_1 \otimes_R M_2) \simeq (S^{-1}M_1) \otimes_{S^{-1}R} (S^{-1}M_2).$$

2. Let R be a ring. Let M be an R-module. Show that $M = 0$ if and only if $M_{\mathfrak{m}} = 0$ for any maximal ideal $\mathfrak{m} \subset R$.

3. Show that Nakayama's Lemma fails if the module M is not assumed to be finitely generated.

4. Let M and N be finitely generated modules over a local ring R. Show that if $M \otimes_R N = 0$ then either $M = 0$ or $N = 0$.

5. Let M and N be finitely generated modules over a local ring R. Show that if $M \otimes_R N \simeq R$ then $M \simeq R$ and $N \simeq R$.

6. Let $\alpha : \mathbb{A}^2 \to \mathbb{A}^2$ be a morphism given by polynomials $f, g \in k[x, y]$. (a) Show that if α is an isomorphism then the polynomial

$$\det \begin{bmatrix} \frac{\partial f(x,y)}{\partial x} & \frac{\partial g(x,y)}{\partial x} \\ \frac{\partial f(x,y)}{\partial y} & \frac{\partial g(x,y)}{\partial y} \end{bmatrix}$$

is a nonzero constant (the converse of this is a famous open problem called the Jacobian Conjecture). (b) Give an example when α is an isomorphism but polynomials f, g are not both linear polynomials.

7. Is a hyperbola $V(xy - 1) \subset \mathbb{A}^2$ isomorphic to $\mathbb{A}^1$?

8. Consider the morphism $\mathbb{A}^2 \to \mathbb{A}^2$ defined by formulas $(x, y) \mapsto (x, xy)$. Is the image Zariski closed? Zariski open? Zariski dense?

9. Consider the morphism $\alpha : \mathbb{A}^1 \to \mathbb{A}^n$ given by $t \mapsto (t, t^2, \ldots, t^n)$. Show that α induces an isomorphism between $\mathbb{A}^1$ and $V(I)$, where I is generated by 2×2 minors of the following matrix

$$\begin{bmatrix} 1 & x_1 & x_2 & \ldots x_{n-1} \\ x_1 & x_2 & x_3 & \ldots x_n \end{bmatrix}$$

10. Compute the dimension of $V(x^2 + y^2 + z^2) \subset \mathbb{A}^3$.

11. Compute the Krull dimension of (a) an Artinian ring; (b) a ring of algebraic integers; (c) $\mathbb{Z}[x]$.

§11. SAMPLE MIDTERM

All rings are commutative, with 1. $\mathbb{C}$ is the field of complex numbers.

1. Let $A \subset B$ be rings such that B is integral over A. Let $f : A \to \mathbb{C}$ be any homomorphism. Show that there exists a homomorphism $g : B \to \mathbb{C}$ such that $g|_A = f$.

2. Let $R = \mathbb{C}[x,y]/(y^2 - x^3 - 2x)$. Let $f : \mathbb{C}[x] \to R$ be the natural map (the inclusion $\mathbb{C}[x] \to \mathbb{C}[x,y]$ followed by the projection $\mathbb{C}[x,y] \to R$). Show that

(a) R is a domain and f is injective.
(b) R is the integral closure of $\mathbb{C}[x]$ in the field of fractions of R.

3. Let $I_1, \ldots, I_k \subset \mathbb{C}[x_1, \ldots, x_n]$ be arbitrary ideals. Show that

(a) $V(I_1 \ldots I_k) = V(I_1 \cap \ldots \cap I_k) = V(I_1) \cup \ldots \cup V(I_k)$.
(b) $V(I_1 + \ldots + I_k) = V(I_1) \cap \ldots \cap V(I_k)$.

Here $V(I)$ is understood as a closed algebraic subset of $\mathbb{A}^n$.

4. Let R be a ring with a maximal ideal $\mathfrak{m}$. Let $f : M \to N$ be a homomorphism of R-modules. Suppose that the induced homomorphism $M \otimes_R (R/\mathfrak{m}) \to N \otimes_R (R/\mathfrak{m})$ is surjective. Prove the following:

(a) If R is local and N is finitely generated then f is surjective.
(b) Show that surjectivity of f can fail if R is not local.

5. Let $\mathfrak{p}$ be a prime ideal of a ring R. Its *height* $\mathrm{ht}(\mathfrak{p})$, by definition, is the maximal number r such that there exists a chain of prime ideals

$$\mathfrak{p}_0 \subsetneq \ldots \subsetneq \mathfrak{p}_r = \mathfrak{p}.$$

Let $f \in \mathbb{C}[x_1, \ldots, x_n]$ be a non-constant irreducible polynomial. Let $\mathfrak{p} = (f)$. Show that $\mathfrak{p}$ is prime and that $\mathrm{ht}\, \mathfrak{p} = 1$.

6. Let R be a ring and let $f : M \to N$ be a homomorphism of R-modules. Show that f is injective if and only if the induced homomorphism of localizations $M_\mathfrak{m} \to N_\mathfrak{m}$ is injective for any maximal ideal $\mathfrak{m} \subset R$.

§12. REPRESENTATIONS OF FINITE GROUPS

§12.1. **Definition and Examples.** Let G be a group and let k be a field. The goal of representation theory is to study various matrix realizations of G.

DEFINITION 12.1.1. A *representation* of G is a homomorphism

$$\rho : G \to \mathrm{GL}(V),$$

where V is a k-vector space. The dimension of V is called the *dimension of the representation*. A representation ρ is called *faithful* if ρ is injective. It is called *trivial* if $\rho(G) = \{e\}$.

REMARK 12.1.2. There are many ways to rephrase this definition. For example, a group G will act on the set of vectors in V by the formula

$$g \cdot v = \rho(g)v, \quad g \in G,\ v \in V,$$

and this action is linear, i.e. any $g \in G$ acts on V as a linear operator. It is clear that any linear action of G on V is given by some representation.

EXAMPLE 12.1.3. The symmetric group S_n acts linearly on k^n by permuting basis vectors $e_1, \dots, e_n$. This representation $\rho : S_n \to \mathrm{GL}_n(k)$ is faithful and any $\sigma \in S_n$ is represented by a *permutation matrix* $\rho(\sigma)$, i.e. a matrix which has exactly one 1 in each row and in each column, all other entries are zero. It can be used to rigorously define the sign of a permutation:

$$\mathrm{sgn}(\sigma) := \det \rho(\sigma).$$

Since ρ is a homomorphism $S_n \to \mathrm{GL}_n(k)$, and $\det$ is a homomorphism $\mathrm{GL}_n(k) \to k^*$, we see that sgn is a homomorphism $S_n \to k^*$. One can quickly check that sgn is equal to $(-1)^a$, where a is a number of transpositions needed to write σ. This of course gives us back the usual definition of the sign, but now we don't have to worry that it is well-defined.

EXAMPLE 12.1.4. Suppose G is a group which acts on a set X. Then G acts linearly on the k-vector space of functions $X \to k$ by the formula

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

For example, if $G = S_n$ and $X = \{1, \dots, n\}$ (with a natural action) then $V = k^n$ and we get the same action as in the previous example. If X is infinite then of course V will be infinite-dimensional. In this case we typically impose more structure, for example we can require that X is a topological space (or a manifold, or an affine algebraic variety) and that for any $g \in G$, the map $X \to X$, $x \mapsto g \cdot x$, is continuous (or smooth, or a regular morphism). Then we can take V to be the space of all continuous (or smooth, or regular algebraic) functions. V is still infinite-dimensional, but can often be approximated by finite-dimensional representations.

EXAMPLE 12.1.5. Many groups are defined as groups of symmetries of geometric objects, in which case one often has a corresponding representation. For example, the dihedral group D_n is the group of symmetries of a regular n-gon. Choosing a cartesian coordinate system with the origin in the center of the n-gon allows us to write any $g \in D_n$ as an orthogonal transformation $\rho(g) : \mathbb{R}^2 \to \mathbb{R}^2$. More precisely, we have a faithful representation

$$\rho : D_n \to \mathrm{O}_2(\mathbb{R}) \subset \mathrm{GL}_2(\mathbb{R}).$$

Analogously, we can consider symmetries of polytopes in $\mathbb{R}^3$. For example, the group of rotations of an icosahedron is isomorphic to A_5. So we have a faithful representation

$$\rho : A_5 \to \mathrm{O}_3(\mathbb{R}) \subset \mathrm{GL}_3(\mathbb{R}).$$

EXAMPLE 12.1.6 (Linear groups). Some groups are defined as groups of matrices. For example, $\mathrm{SL}_n(k)$, $\mathrm{O}_n(\mathbb{R})$ (the group of $n \times n$ orthogonal matrices), etc. So all these groups have a "standard" representation. Another example: the group of complex n-th roots of unity, μ_n, is a subgroup of $\mathbb{C}^* = \mathrm{GL}_1(\mathbb{C})$. So μ_n has a standard 1-dimensional representation. Abstractly, μ_n is a cyclic group generated by any primitive n-th root of unity.

EXAMPLE 12.1.7 (Finite groups of Lie type). The group $\mathrm{GL}_2(\mathbb{F}_q)$ by definition has a 2-dimensional representation over $\mathbb{F}_q$. Representations in characteristic p, especially over finite fields, are known as *modular* representations. Of course $\mathrm{GL}_2(\mathbb{F}_q)$ also has representations in characteristic 0. For

example, it is easy to see that $\mathrm{GL}_2(\mathbb{F}_2)$ has 6 elements and permutes three non-zero vectors of $(\mathbb{F}_2)^2$. Therefore, it is isomorphic to S_3 and has a 3-dimensional representation in k^3 by permuting basis vectors described in Example 12.1.4.

EXAMPLE 12.1.8. The quaternionic group Q_8 has a 2-dimensional complex representation by Pauli matrices.

EXAMPLE 12.1.9 (Regular representation). Let G be a finite group. Let $k[G]$ be a vector space with a basis $[g]$ indexed by elements $g \in G$:

$$k[G] = \left\{ \sum_{g \in G} a_g[g] \quad | \quad a_g \in k \right\}.$$

The action of G on itself by left multiplication extends to representation of G in $k[G]$ called *regular representation*:

$$g_0 \cdot \left(\sum_{g \in G} a_g[g] \right) = \sum_{g \in G} a_g[g_0 g]$$

EXAMPLE 12.1.10. Let F/K be a finite Galois extension with Galois group G. Then G acts on F and this action is K-linear:

$$\sigma(k\alpha) = \sigma(k)\sigma(\alpha) = k\sigma(\alpha) \quad \text{if } k \in K,\ \alpha \in F.$$

If we consider F as an n-dimensional K-vector space (where $n = |G|$), we get a faithful representation

$$G \to \mathrm{GL}_n(K).$$

According to the Normal Basis Theorem of Galois Theory, this representation is isomorphic to the regular representation of G, i.e. F has a basis over K indexed by elements of the Galois group, and such that the Galois group permutes them accordingly.

§12.2. **G-modules.** Given a representation

$$\rho : G \to \mathrm{GL}(V),$$

V is often called a *G-module*. To explain this, let's relate representations to modules of the group algebra.

DEFINITION 12.2.1. As in Example 12.1.9, let $k[G]$ be a k-vector space with a basis $[g]$ indexed by elements $g \in G$:

$$k[G] = \left\{ \sum_{g \in G} a_g[g] \quad | \quad a_g \in k \right\}.$$

This vector space is a k-algebra with multiplication defined as follows:

$$\left(\sum_{g \in G} a_g[g] \right) \left(\sum_{g \in G} b_g[g] \right) = \sum_{g,h \in G} a_g b_h [gh].$$

Associativity of multiplication in G implies that $k[G]$ is an associative (but not commutative!) algebra. It has a unit, namely $[e]$, where $e \in G$ is a unit.

LEMMA 12.2.2. *There exists an explicit bijection (constructed in the proof) between representations of G and $k[G]$-modules.*

Proof. Given a representation $\rho : G \to \mathrm{GL}(V)$, we define the action of $k[G]$ on V as follows:

$$\left(\sum_{g\in G} a_g[g]\right)\cdot v = \sum_{g\in G} a_g\rho(g)(v).$$

In the other direction, given a $k[G]$-module V, notice first of all that V is a k-module by restriction of scalars, i.e. a k-vector space. We can define a homomoprhism $\rho : G \to \mathrm{GL}(V)$ as follows:

$$\rho(g)(v) = [g]\cdot v.$$

It is straightforward to check that this gives a correspondence between representations and $k[G]$-modules. □

We can use this correspondence to transfer various module-theoretic definitions to representations. For example,

DEFINITION 12.2.3. Representations $\rho : G \to \mathrm{GL}(V)$ and $\rho' : G \to \mathrm{GL}(V')$ are called *isomorphic* or *equivalent* if the corresponding $k[G]$-modules are isomorphic. Explicitly, this means that there exists an invertible k-linear transformation $L : V \to V'$ such that

$$L(\rho(g)v) = \rho'(g)L(v)$$

for any $g \in G$, $v \in V$.

§12.3. **Mashke's Theorem.**

DEFINITION 12.3.1. Given a representation $\rho : G \to \mathrm{GL}(V)$, we define a *sub-representation* $U \subset V$ as any $k[G]$-submodule. Explicitly, U is a vector subspace of V such that $\rho(g)U = U$ for any $g \in G$[8]. Another terminology: U is called a G-invariant subspace of V.

DEFINITION 12.3.2. A representation of G in V is called *irreducible* if V has no proper G-invariant subspaces, i.e. no sub-representations.

DEFINITION 12.3.3. A direct sum of representations $\rho : G \to \mathrm{GL}(V)$ and $\rho' : G \to \mathrm{GL}(V')$ is a direct sum of vector spaces $V \oplus V'$ equipped with a component-wise linear action of G:

$$\rho(g)(v, v') = (\rho(g)v, \rho'(g)v').$$

Given bases in V and V' construct a basis of $V \oplus V'$ by concatenating them. In this basis, the matrix of $\rho(g)$ is block-diagonal with blocks $\rho(g)$ and $\rho'(g)$.

A basic question is whether any representation is isomorphic to a direct sum of irreducible representations. Here are two standard examples.

[8]This is equivalent to requiring that $\rho(g)U \subset U$ for any $g \in G$ since then $\rho(g^{-1})U \subset U$, which implies $U \subset \rho(g)U$.

EXAMPLE 12.3.4. The standard representation of S_n in k^n has two S_n-invariant subspaces:

$$V_1 = k(e_1 + \ldots + e_n) \quad \text{and} \quad V_2 = \left\{ \sum a_i e_i \mid \sum a_i = 0 \right\}.$$

It is clear that $k^n = V_1 \oplus V_2$. Since $\dim V_1 = 1$, V_1 is obviously irreducible. We will later see that V_2 is also irreducible.

EXAMPLE 12.3.5. Consider a subgroup

$$G = \left\{ \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \quad \middle| \quad x \in \mathbb{F}_q \right\} \subset \mathrm{GL}_2(\mathbb{F}_q)$$

and its natural representation in $\mathbb{F}_q^2$. We claim that $\langle e_1 \rangle$ is the only proper G-invariant subspace, and in particular that $\mathbb{F}_q^2$ is not a direct sum of irreducible subrepresentations. Indeed, since $\dim \mathbb{F}_q^2 = 2$, a proper G-invariant subspace would be spanned by a common eigenvector of all elements of G. But G contains a matrix $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, which has only one eigenspace, $\langle e_1 \rangle$.

Now the main result:

THEOREM 12.3.6 (Maschke). *Let G be a finite group. Suppose that $\mathrm{char}\, k$ does not divide $|G|$. Then any finite-dimensional representation V of G is a direct sum of irreducible sub-representations*[9].

Proof. Arguing by induction on $\dim V$, it suffices to prove the following: if $U \subset V$ is a G-invariant subspace then there exists a G-invariant subspace U' such that $V = U \oplus U'$. We will give two different proofs of that.

Proof A. Let's choose a complementary *vector subspace* W and let $\pi : V \to V$ be a projector onto U along W, i.e. $\mathrm{Ker}\, \pi = W$, $\pi(V) \subset U$, and $\pi|_U = \mathrm{Id}\,|_U$.
We will average π over G. Consider a linear operator $\pi_0 : V \to V$,

$$\pi_0(v) = \frac{1}{|G|} \sum_{g \in G} g\pi(g^{-1}v)$$

(here we use that $|G|$ is coprime to characteristic). Then

$$\pi_0(hv) = \frac{1}{|G|} \sum_{g \in G} g\pi(g^{-1}hv) = \frac{1}{|G|} \sum_{g \in G} h(h^{-1}g)\pi((h^{-1}g)^{-1}v) =$$

$$h\frac{1}{|G|} \sum_{g \in G} (h^{-1}g)\pi((h^{-1}g)^{-1}v) = h\frac{1}{|G|} \sum_{g \in G} g\pi(g^{-1}v) = h\pi_0,$$

i.e. π_0 commutes with action of G. It follows that

$$U' = \mathrm{Ker}\, \pi_0$$

is G-invariant. Since $\pi(V) \subset U$ and U is G-invariant, $\pi_0(V) \subset U$ as well. Since $\pi|_U = \mathrm{Id}\,|_U$, we also have $\pi_0|_U = \mathrm{Id}\,|_U$, which gives $V = U \oplus U'$, a direct sum of G-invariant subspaces.

[9] One can also say that V is *completely reducible*.

Proof B. This argument only works if $k = \mathbb{R}$ or $\mathbb{C}$. In this case let $(\cdot, \cdot)$ be a non-degenerate symmetric (if $k = \mathbb{R}$) or Hermitian (if $k = \mathbb{C}$) product on V and let's define another product by formula

$$(v, v')_0 = \frac{1}{|G|} \sum_{g \in G} (gv, gv').$$

Any positive linear combination of inner products is an inner product, and it is easy to check that $(\cdot, \cdot)_0$ is G-invariant, i.e. $(gv, gv')_0 = (v, v')_0$ for any $g \in G$. An advantage of having this invariant inner product is that if $U \subset V$ is a G-invariant subspace then we can just take U' to be an orthogonal complement of U: invariance of $(v, v')_0$ implies that U' is G-invariant. $\square$

§12.4. **Schur's Lemma.**

DEFINITION 12.4.1. Let $\rho : G \to \mathrm{GL}(V)$ be a representation. We define its endomorphism algebra as

$$\mathrm{End}_G(V) = \{L \in \mathrm{Hom}_k(V, V) \mid L(\rho(g)v) = \rho(g)L(v) \text{ for any } g \in G,\ v \in V\}.$$

This is clearly a subalgebra in the matrix algebra $\mathrm{Hom}_k(V, V)$. Notice that $\mathrm{End}_G(V)$ contains $\mathrm{Aut}_G(V)$, a group of all isomorphisms of V with itself.

LEMMA 12.4.2 (Schur). *Suppose ρ is an irreducible representation. Then $\mathrm{End}_G(V)$ is a division algebra, i.e. any non-zero element of it is invertible. If $k = \bar{k}$ and ρ is finite-dimensional then $\mathrm{End}_G(V) = k$, the algebra of scalar operators.*

Proof. Let $L \in \mathrm{End}_G(V)$. Then it is easy to check that $\mathrm{Ker}\, L$ and $\mathrm{Im}\, L$ are G-invariant subspaces of V. Since V is irreducible, we conclude that either $L = 0$ or L is invertible. So $\mathrm{End}_G(V)$ is a division algebra.

Now suppose that $k = \bar{k}$ and $\dim \rho < \infty$. We will give two proofs that $\mathrm{End}_G(V) = k$.

Proof A. Let λ be an eigenvalue of L and let

$$V_\lambda = \{v \in V \mid Lv = \lambda v\}$$

be the corresponding eigenspace. We claim that V_λ is G-invariant: indeed if $v \in V_\lambda$ then

$$L(gv) = gL(v) = g(\lambda v) = \lambda(gv),$$

and so $gv \in V_\lambda$. Since V is irreducible and $V_\lambda \neq 0$, it follows that $V_\lambda = V$, i.e. that L acts on V by multiplication by λ.

Proof B. Notice that $\mathrm{End}_G(V)$ obviously contains k as a subalgebra of scalar operators. Moreover, these scalar operators commute with any operator in $\mathrm{End}_G(V)$, i.e. k belongs to the center of $\mathrm{End}_G(V)$. Also, $\mathrm{End}_G(V)$ is a subalgebra of $\mathrm{Hom}_k(V, V)$, and so is a finite-dimensional k-algebra. We can try to argue that in fact if $k = \bar{k}$ then k is the only division algebra finite-dimensional over k and such that k is contained in its center. Indeed, let D be such an algebra and let $\alpha \in D$. Let $k(\alpha)$ be the minimal division subalgebra containing k and α. Since k and α commute, $k(\alpha)$ is in fact a field. This field is finite-dimensional and hence algebraic over k. Since k is algebraically closed, in fact $\alpha \in k$. $\square$

We see that if k is not algebraically closed then irreducible representations can be classified by a type of a division algebra that appears as its algebra of endomorphisms. For example, suppose $k = \mathbb{R}$. By a Theorem of Frobenius, finite-dimensional division algebras over $\mathbb{R}$ are $\mathbb{R}$, $\mathbb{C}$, and the algebra of quaternions $\mathbb{H}$. All these cases occur.

EXAMPLE 12.4.3. The trivial representation $G \to \mathrm{GL}_1(\mathbb{R})$ is irreducible for any G, and $\mathrm{End}_G = \mathbb{R}$.

EXAMPLE 12.4.4. Let C_n be a cyclic group with n elements ($n \geq 3$) and consider its representation in $\mathbb{R}^2$ as the group of rotations of a regular n-gon. No lines in $\mathbb{R}^2$ are invariant under this action, so this representation is irreducible. It is easy to check that the algebra of G-endomorphisms is $\mathbb{C}$. In fact, identifying $\mathbb{R}^2$ with $\mathbb{C}$ in the standard way, C_n acts by multiplication by n-th roots on unity. $\mathbb{C}$ acts on itself by left multiplication, and these two actions obviously commute.

EXAMPLE 12.4.5. Let $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ be the group of 8 quaternions. Its representation in $\mathbb{C}^2$ by Pauli matrices is equivalent to its linear action on all quaternions $\mathbb{H}$ by left multiplication. This gives an irreducible 4-dimensional real representation of Q_8. Its algebra of G-endomorphisms can be identified with $\mathbb{H}$, which acts on itself by *right* multiplication (notice that left multiplications by Q_8 and H do not commute!).

Our goal is to gather more specific information about irreducible representations. For example, we can ask how many of them are there, what are their dimensions, etc. This is going to depend on the field. To simplify matters, we are going to assume that k is algebraically closed.

From now on we are going to assume that k is algebraically closed.

We are also going to assume that G is a finite group, although sometimes we will state results in a more general setting.

From now on we are going to assume that G is finite.

It is worth mentioning that if $|G| < \infty$ then any irreducible representation V of G is finite-dimensional. Indeed, take any $v \in V$. Then $\mathrm{Span}\langle gv\rangle_{g\in G}$ is a finite-dimensional G-invariant subspace of V. Therefore $\dim V < \infty$.

§12.5. **One-dimensional representations.** One-dimensional representations are automatically irreducible. We are going to classify them completely.

DEFINITION 12.5.1. Let G be a group. For any $g, h \in G$, the element

$$[g, h] := ghg^{-1}h^{-1}$$

is called a commutator of g and h. Let $[G, G]$ be the subgroup of G generated by all commutators. It is called a *commutant* of G.

LEMMA 12.5.2.

(1) *The commutant $[G, G]$ is a normal subgroup of G and $G/[G, G]$ is Abelian*[10].
(2) *If H is normal in G and G/H is Abelian then $H \supset [G, G]$.*

[10]This group is called *an abelianization* of G.

(3) *Let $\pi : G \to [G,G]$ be the canonical projection. There is a natural bijection between the sets of 1-dimensional representations of G and $G/[G,G]$, which sends any homomorphism $f : G/[G,G] \to \mathrm{GL}_1(k)$ to $f \circ \pi$.*

Proof. The basic calculation is

$$a(ghg^{-1}h^{-1})a^{-1} = (aga^{-1})(aha^{-1})(aga^{-1})^{-1}(aha^{-1})^{-1},$$

which shows that the set of all commutators is preserved by conjugation. It follows that $[G,G]$ is preserved by conjugation, i.e. $[G,G]$ is a normal subgroup. For any cosets $g[G,G]$, $h[G,G]$, their commutator is

$$ghg^{-1}h^{-1}[G,G] = [G,G],$$

i.e. $G/[G,G]$ s Abelian.

If $f : G \to G'$ is any homomorphism then $f([G,G]) \subset [G',G']$. It follows that if G' is Abelian then $[G,G] \subset \mathrm{Ker}\, f$. This shows (2). It also shows (3) because $\mathrm{GL}_1(k) = k^*$ is Abelian. □

EXAMPLE 12.5.3. Let $G = S_n$. It is not hard to check that $[S_n, S_n] = A_n$. So 1-dimensional representations of S_n are in bijection with 1-dimensional representations of $S_n/A_n = \mathbb{Z}_2$. A homomorphism $f : \mathbb{Z}_2 \to k^*$ is completely determined by $f(1)$, which should satisfy $f(1)^2 = 1$, i.e. $f(1) = \pm 1$. We see that if $\mathrm{char}\, k \neq 2$ then $\mathbb{Z}_2$ has two 1-dimensional representations. It follows that the same is true for S_n: one representation is trivial and another (if $\mathrm{char}\, k \neq 2$) is the sign representation,

$$S_n \to k^*, \quad g \mapsto \mathrm{sgn}(g).$$

Now we are going to completely work out the case of Abelian groups.

LEMMA 12.5.4. *Let G be an Abelian group and let $k = \bar{k}$. Any finite-dimensional irreducible representation of G is 1-dimensional.*

Proof A. Let $\rho : G \to \mathrm{GL}(V)$ be an irreducible representation. For any $g_0 \in G$, $\rho(g_0)$ belongs to $\mathrm{End}_G(V)$. Indeed,

$$\rho(g_0)(gv) = \rho(g_0 g)(v) = \rho(g g_0)(v) = g\rho(g_0)v.$$

By Schur's Lemma, $\rho(g_0)$ must be a scalar linear operator. So G acts by scalar operators, and therefore any vector subspace is G-invariant. It follows that $\dim V = 1$. □

Proof B. Instead of using Schur's lemma directly, we can use an argument from its proof. The set $\{\rho(g)\}_{g \in G}$ is a set of commuting linear operators of a finite-dimensional vector space over an algebraically closed field. By linear algebra, these operators have a common eigenvector, which spans a one-dimensional G-invariant subspace. Since V is irreducible, $\dim V = 1$. □

DEFINITION 12.5.5. Let G be an Abelian group. Its *Pontryagin dual group* $\hat{G}$ is the group of all homomorphisms $\phi : G \to k^*$. The multiplication in $\hat{G}$ is given by the formula

$$(\phi\psi)(g) = \phi(g)\psi(g).$$

The unit element in $\hat{G}$ is the trivial homomorphism $G \to \{1\} \in k^*$.

One-dimensional representations of G are classified by elements of $\hat{G}$.

LEMMA 12.5.6. *Let G be a finite Abelian group. Suppose* $\operatorname{char} k$ *is coprime to $|G|$. Then $\hat{G}$ is non-canonically isomorphic to G, in particular $|G| = |\hat{G}|$ and so G has $|G|$ irreducible 1-dimensional representations. The map*

$$g \to [\phi \mapsto \phi(g)]$$

is a canonical isomorphism between G and $\hat{\hat{G}}$.

Proof. Notice that $\widehat{G_1 \times G_2} \simeq \hat{G}_1 \times \hat{G}_2$. Indeed, a homomorphism $\phi : G_1 \times G_2 \to k^*$ is uniquely determined by its restrictions $\phi|_{G_1}$ and ϕ_{G_2}. And given any homomorphisms $\phi_1 : G_1 \to k^*$ and $\phi_2 : G_2 \to k^*$, we can define a homomorphism $\phi : G_1 \times G_2 \to k^*$ by formula $\phi(g_1, g_2) = \phi_1(g_1)\phi_2(g_2)$.

By the fundamental theorem on Abelian groups, we therefore can assume that $G \simeq \mathbb{Z}/n\mathbb{Z}$ is cyclic. A homomorphism $\mathbb{Z}/n\mathbb{Z} \to k^*$ must send $1 + n\mathbb{Z}$ to an n-th root of unity in k. So $\widehat{\mathbb{Z}/n\mathbb{Z}} = \mu_n$. Since $\operatorname{char} k$ is coprime to $|G|$, it is coprime to n. Since k is algebraically closed, μ_n is a cyclic group of order n. This proves the first statement.

Finally, we claim that G is canonically isomorphic to its double dual. Since they have the same number of elements, it suffices to show that the map $g \to [\phi \mapsto \phi(g)]$ is injective. If it is not injective then any homomorphism $\phi : G \to k^*$ vanishes on some $g \in G$. But then $\hat{G}$ can be identified with $\widehat{G/\langle g \rangle}$, and in particular $|\hat{G}| < |G|$, which is a contradiction. □

EXAMPLE 12.5.7. Let's classify complex irreducible representations of $\mathbb{Z}/7\mathbb{Z}$. We have $\widehat{\mathbb{Z}/7\mathbb{Z}} = \mu_7 \subset \mathbb{C}$. For each root $\eta = e^{\frac{2pi}{7}k}$, the corresponding one-dimensional representation is

$$\mathbb{Z}/7\mathbb{Z} \to \mathbb{C}^*, \quad i \mapsto \eta^i.$$

COROLLARY 12.5.8. *Let G be a finite group. If $k = \bar{k}$ and* $\operatorname{char} k$ *is coprime to $|G|$ then the number of one-dimensional representations of G is equal to $[G : [G, G]]$.*

§12.6. **Exercises.**

1. Describe explicitly (i.e. how each element of the group acts) all irreducible complex representations of $(\mathbb{Z}/2\mathbb{Z})^r$.

2. Describe explicitly (i.e. how each element of the group acts) all one-dimensional complex representations of D_n.

3. Describe explicitly (i.e. how each element of the group acts) all one-dimensional complex representations of $\mathrm{GL}_2(\mathbb{F}_{11})$.

4. Let V be an irreducible complex representation of a finite group G. Show that there exists a unique (up to a positive scalar) G-invariant Hermitian inner product on V.

5. Let $k = \mathbb{F}_q$ be a finite field with $q = p^n$ elements. Let G be a p-group. Show that any irreducible representation of G over k is trivial.

6. Let G be a group (not necessarily finite) and let $V = \mathbb{C}[G]$ be its regular representation. Let $U \subset V$ be a vector subspace spanned by vectors

$$[gh] - [hg] \quad \text{for any } g, h \in G.$$

Suppose that $\dim V/U < \infty$. Show that G has only finitely many conjugacy classes and that their number is equal to $\dim V/U$.

7. Let G be a group and let V be a G-module over a field k. Let K/k be a field extension. Let $V_K := V \otimes_k K$. Show that V_K has a natural G-module structure over K compatible with extension of scalars: $V_K \simeq V \otimes_{k[G]} K[G]$.

8. Let V be an irreducible representation of a finite group G over $\mathbb{R}$.

(a) Show that $V_{\mathbb{C}}$ is either irreducible or a direct sum of two irreducible representations.
(b) Show on examples that both possibilities in (a) occur.

9. Let V denote the two-dimensional real representation of D_n given by the natural embedding $D_n \subset \mathrm{O}_2(\mathbb{R})$.

(a) Choose a system of generators of D_n and write down matrices of these elements in some basis of V.
(b) Show that $V_{\mathbb{C}}$ is irreducible.

10. Let G be the group of all rotations of $\mathbb{R}^3$ which preserve a regular tetrahedron centered at the origin. Let V denote the three-dimensional representation of G over $\mathbb{R}$ given by the natural embedding $G \subset \mathrm{O}_3(\mathbb{R})$.

(a) Choose a system of generators of G and write down matrices of these elements in some basis of V.
(b) Show that $V_{\mathbb{C}}$ is irreducible.

11. Let G be the group of all rotations of $\mathbb{R}^3$ which preserve a regular icosahedron centered at the origin. Let V denote the three-dimensional representation of G over $\mathbb{R}$ given by the natural embedding $G \subset \mathrm{O}_3(\mathbb{R})$.

(a) Choose a system of generators of G and write down matrices of these elements in some basis of V.
(b) Show that $V_{\mathbb{C}}$ is irreducible.

12. Let V be an irreducible complex representation of a finite group G.

(a) Let $x \in V$, $x \neq 0$. Prove that $\dim V \leq [G : G_x]$.
(b) Let $H \subset G$ be an Abelian subgroup. Prove that

$$\dim V \leq [G : H].$$

13. Let G be a finite Abelian group and let $\hat{G}$ be its Pontryagin dual group (over $\mathbb{C}$). For any function $f : G \to \mathbb{C}$, its Fourier transform $\hat{f} : \hat{G} \to \mathbb{C}$ is by definition the following function:

$$\hat{f}(\rho) = \frac{1}{\sqrt{|G|}} \sum_{g \in G} f(g)\overline{\rho(g)}.$$

Compute $\hat{\hat{f}}$ (here we identify $\hat{\hat{G}}$ with G).

§13. Irreducible representations of finite groups

§13.1. **Characters.** From now on we are going to work over $\mathbb{C}$. Our main tool will be orthogonality of characters, and we need complex numbers to make sense of it. However, most of the results about irreducible representations proved using characters can be proved using different methods over arbitrary algebraically closed fields of characteristic not dividing $|G|$.

DEFINITION 13.1.1. Let $\rho : G \to \mathrm{GL}(V)$ be a finite-dimensional complex representation of a group G. Its character χ_V is a function $G \to \mathbb{C}$ defined as follows:

$$\chi_V(x) = \operatorname{Tr} \rho(x) \quad \text{for any } x \in G.$$

EXAMPLE 13.1.2. Consider the standard action of S_n on $\mathbb{C}^n$ by permuting basis vectors. For any $\sigma \in S_n$, $\chi_{\mathbb{C}^n}(\sigma)$ is equal to the number of elements of $\{1, \dots, n\}$ fixed by σ.

EXAMPLE 13.1.3. For any representation $\rho : G \to \mathrm{GL}(V)$,

$$\chi_V(e) = \operatorname{Tr}(\mathrm{Id}_V) = \dim V.$$

EXAMPLE 13.1.4. G acts in the regular representation $\mathbb{C}[G]$ by formula

$$h\left(\sum_{g \in G} a_g[g]\right) = \sum_{g \in G} a_g[hg].$$

If $h \neq e$ then the matrix of h has no diagonal entries ($g \neq hg$ for any $g \in G$), and so we have

$$\chi_{reg}(x) = \begin{cases} |G| & \text{if } x = e \\ 0 & \text{if } x \neq e \end{cases}$$

§13.2. **Basic operations on representations and their characters.** Characters behave naturally with respect to various basic operations with representations. We are going to define these operations along with studying their characters in the proof of the following theorem.

THEOREM 13.2.1. *We have*

$$\chi_{V \oplus W} = \chi_V + \chi_W,$$

$$\chi_{V \otimes W} = \chi_V \chi_W,$$

$$\chi_{V^*} = \overline{\chi_V},$$

$$\chi_{\mathrm{Hom}(V,W)} = \overline{\chi_V} \chi_W.$$

Proof. We are going to use the following basic facts: the trace is the sum of eigenvalues; $\rho(g)$ is diagonalizable for any $g \in G$ (as any linear operator of finite order); all eigenvalues of $\rho(g)$ are roots of unity.

Direct sum: G acts on $V \oplus W$ by the formula $g(v, w) = (gv, gw)$. The matrix of this representation is a block-diagonal matrix of representations in V and W, and the trace is obviously additive.

Tensor product: G acts on $V \otimes W$ by the formula $g(v \otimes w) = gv \otimes gw$. Let's show that this is well-defined. Indeed, this linear map is induced by a bilinear map $G : V \times W \to V \otimes W$, defined as follows: $G(v, w) = (gv) \otimes (gw)$. Notice that if $v_1, \dots, v_n$ (resp. $w_1, \dots, w_m$) are eigenvectors for $\rho(g)$ in V (resp. in W) with eigenvalues $\lambda_1, \dots, \lambda_n$ (resp. $\mu_1, \dots, \mu_m$) then $\{v_i \otimes w_j\}$ are eigenvectors for $\rho(g)$ in $V \otimes W$ with eigenvalues $\lambda_i \mu_j$. We have

$$\chi_{V \otimes W}(g) = \sum_{i,j} \lambda_i \mu_j = \left(\sum_i \lambda_i\right)\left(\sum_j \mu_j\right) = \chi_V(g) \chi_W(g).$$

Dual representation: G acts on V^* as follows: if $f \in V^*$ then $\rho_{V^*}(g)f$ is a linear map

$$v \mapsto f(\rho(g^{-1})v).$$

The matrix of $\rho_{V^*}(g)$ can be obtained from the matrix of $\rho_V(g)$ by transposing and inverting. Since every eigenvalue λ of $\rho(g)$ is a root of unity, $\lambda^{-1} = \bar{\lambda}$. So

$$\chi_{V^*}(g) = \sum \lambda_i^{-1} = \sum \bar{\lambda}_i = \overline{\chi_V(g)}.$$

Hom representation: G acts on $\mathrm{Hom}(V, W)$ as follows: if $F \in \mathrm{Hom}(V, W)$ then $\rho_{\mathrm{Hom}(V,W)}(g)F$ is a linear transformation

$$v \mapsto \rho_W(g)F(\rho_V(g^{-1})v).$$

Notice that this action is compatible with a canonical isomorphism

$$\mathrm{Hom}(V, W) \simeq V^* \otimes W$$

of finite-dimensional vector spaces. So

$$\chi_{\mathrm{Hom}(V,W)} = \chi_{V^*}\chi_W = \overline{\chi_V}\chi_W.$$

The theorem is proved. □

§13.3. **Schur's orthogonality relations.** If G is a finite group then we can identify $\mathbb{C}[G]$ with the space of functions $G \to \mathbb{C}$, namely

$$\sum_{g\in G} a_g[g] \mapsto f, \quad f(g) = a_g.$$

This identification is compatible with the action of G: any $h \in G$ sends a linear combination above to $\sum\limits_{g\in G} a_g[hg] = \sum\limits_{g\in G} a_{h^{-1}g}[g]$, which corresponds to a function

$$\tilde{f}(g) = a_{h^{-1}g} = f(h^{-1}g).$$

DEFINITION 13.3.1. Let G be a finite group. We introduce a positive definite Hermitian product on $\mathbb{C}[G]$ (viewed as the set of functions $G \to C$):

$$(\phi, \psi) := \frac{1}{|G|} \sum_{g\in G} \phi(g)\overline{\psi(g)}. \tag{13.3.1}$$

THEOREM 13.3.2. *Let V, V' be irreducible G-modules. Then*

$$(\chi_V, \chi_{V'}) = \begin{cases} 1 & \text{if } V \text{ is isomorphic to } V' \\ 0 & \text{if } V \text{ is not isomorphic to } V' \end{cases}$$

Proof. Let χ be the character of the representation $\mathrm{Hom}(V', V)$. By Theorem 13.2.1, we have

$$\chi = \chi_V\overline{\chi_{V'}},$$

and so

$$(\chi_V, \chi_{V'}) = \frac{1}{|G|} \sum_{g\in G} \chi(g).$$

CLAIM 13.3.3. *For any G-module W, $\frac{1}{|G|} \sum\limits_{g\in G} \chi_W(g) = \dim_{\mathbb{C}} W^G$.*

Given the Claim, $(\chi_V, \chi_{V'}) = \dim \mathrm{Hom}(V', V)^G$. This space is identified with the space $\mathrm{Hom}_G(V', V)$ of G-module homomorphisms $V' \to V$. The kernel and the image of any homomorphism are G-invariant subspaces. Since V and V' are both irreducible, this shows that

$$\mathrm{Hom}(V', V)^G = 0$$

if V and V' are not isomorphic. If they are isomorphic then

$$\mathrm{Hom}(V', V)^G \simeq \mathrm{End}_G(V) = \mathbb{C}$$

by Schur's Lemma. The Theorem follows.

It remains to prove the Claim. Consider the following *Reynolds operator*:

$$R = \frac{1}{|G|} \sum_{g \in G} \rho(g), \quad R: W \to W.$$

It is easy to see that this linear operator has the following properties:

(1) $R(W) \subset W^G$;
(2) $R|_{W^G} = \mathrm{Id}\,|_{W_G}$.

By linear algebra, it follows that R is a projector onto W^G, and in particular

$$\frac{1}{|G|} \sum_{g \in G} \chi_W(g) = \frac{1}{|G|} \sum_{g \in G} \mathrm{Tr}\, \rho(g) = \mathrm{Tr}\, R = \dim_{\mathbb{C}} W^G.$$

Q.E.D. □

DEFINITION 13.3.4. Let V be a finite-dimensional complex representation of a finite group G. By Maschke's Theorem, we have a decomposition

$$V = V_1^{m_1} \oplus \ldots \oplus V_r^{m_r},$$

where $V_1, \ldots, V_r$ are pair-wise non-isomorphic irreducible subrepresentations and $V_i^{m_i}$ denotes a direct sum $V_i \oplus \ldots \oplus V_i$ (m_i times). The number m_i is called a *multiplicity* of V_i in V.

COROLLARY 13.3.5. *Multiplicities can be computed as follows:*

$$m_i = (\chi_V, \chi_{V_i}).$$

We also have

$$m_1^2 + \ldots + m_r^2 = (\chi_V, \chi_V).$$

Proof.

$$(\chi_V, \chi_{V_i}) = \left(\sum_j m_j \chi_{V_j}, \chi_{V_i} \right) = \sum_j m_j (\chi_{V_j}, \chi_{V_i}) = m_i$$

by orthogonality relations. The second formula is similar. □

COROLLARY 13.3.6. *A complex representation of a finite group is determined by its character up to an isomorphism.*

Proof. Indeed, Corollary 13.3.5 expresses multiplicities in terms of the character and multiplicities determine an isomorphism class. □

EXAMPLE 13.3.7. Consider the standard n-dimensional representation V of the symmetric group S_n. Then $\chi_V(\sigma)$ is the number of indices fixed by σ. Call this number $\mathrm{Fix}(\sigma)$. We have

$$(\chi_V, \chi_V) = \frac{1}{n!} \sum_{\sigma \in S_n} \mathrm{Fix}(\sigma)^2.$$

The symmetric group S_n acts naturally on the set of pairs

$$X = \{1, \ldots, n\} \times \{1, \ldots, n\}$$

and $\mathrm{Fix}(\sigma)^2 = \mathrm{Fix}_X(\sigma)$, where $\mathrm{Fix}_X(\sigma)$ is the number of elements of X fixed by σ. Recall that we have the Burnside's counting theorem: if a finite group G acts on a finite set X then $\frac{1}{|G|} \sum\limits_{g \in G} \mathrm{Fix}(g)$ is equal to the number of G-orbits in X. In our case there are two orbits: the diagonal $\{(i,i)\}_{i=1,\ldots,n}$ and its complement. It follows that

$$(\chi_V, \chi_V) = 2,$$

and therefore V is a direct sum of two non-isomorphic irreducible representations (there is only one way to write 2 as sum of squares: $1^2 + 1^2$). By Example 12.3.4, these subrepresentations must be the trivial one

$$V_1 = \mathbb{C}(e_1 + \ldots + e_n)$$

and the non-trivial one

$$V_2 = \left\{ \sum a_i e_i \mid \sum a_i = 0 \right\}.$$

In particular, V_2 is irreducible.

§13.4. **Decomposition of the regular representation.**

THEOREM 13.4.1. *Let G be a finite group. We have*

$$\mathbb{C}[G] \simeq V_1^{\dim V_1} \oplus \ldots \oplus V_r^{\dim V_r}, \tag{13.4.1}$$

the direct sum over all pair-wise non-isomorphic irreducible representations of G. In particular,

$$|G| = (\dim V_1)^2 + \ldots + (\dim V_r)^2.$$

Proof. By Example 13.1.4, the character of the regular representation is

$$\chi_{reg}(x) = \begin{cases} |G| & \text{if } x = e \\ 0 & \text{if } x \neq e \end{cases}$$

It follows that

$$(\chi_{reg}, \chi_{V_i}) = \chi_{V_i}(e) = \mathrm{Tr}\, \rho_{V_i}(e) = \dim V_i.$$

The formula (13.4.1) follows from Corollary 13.3.5. The second formula also follows from it because

$$(\chi_{reg}, \chi_{reg}) = \frac{1}{|G|} |G| \cdot |G| = |G|.$$

Alternatively, we can just compute dimensions of both sides of (13.4.1). □

EXAMPLE 13.4.2. We already know three irreducible complex representations of S_3: the trivial one, the sign representation, and the 2-dimensional representation of Example 13.3.7. Since

$$6 = 1^2 + 1^2 + 2^2,$$

this is a complete list of irreducible representations (up to an isomorphism).

§13.5. **The number of irreducible representations.**

DEFINITION 13.5.1. A function $G \to \mathbb{C}$ is called a *class function* if it is constant on conjugacy classes. Let $C(G)$ be a vector space of all class functions.

LEMMA 13.5.2. *Each character is a class function.*

Proof. Indeed,

$$\chi(hgh^{-1}) = \operatorname{Tr} \rho(hgh^{-1}) = \operatorname{Tr} \rho(h)\rho(g)\rho(h)^{-1} = \operatorname{Tr} \rho(g) = \chi(g).$$

So χ is constant on conjugacy classes. □

THEOREM 13.5.3. *Let $V_1, \dots, V_r$ be the list of all pair-wise non-isomorphic irreducible complex representations of a finite group G. Their characters $\chi_1, \dots, \chi_r$ form a basis of $C(G)$. In particular, the number r of irreducible representations of G is equal to the number of conjugacy classes of G.*

Proof. The positive-definite Hermitian pairing (13.3.1) on $\mathbb{C}[G]$ restricts to a positive-definite Hermitian pairing on $C(G)$. Since characters are orthonormal by Schur's relations, they are linearly independent (a linear relation $\sum_{i=1}^r a_i\chi_i = 0$ gives $0 = (\sum_{i=1}^r a_i\chi_i, \chi_j) = a_j$ for any $j = 1, \dots, r$).

Next we claim that $C(G)$ is a linear span of $\chi_1, \dots, \chi_r$. If not then we can find a non-zero class function $f \in C(G)$ orthogonal to all characters $\chi_1, \dots, \chi_r$. Any representation $\rho : G \to \mathrm{GL}(V)$ can be extended to a homomorphism $\mathbb{C}[G] \to \mathrm{End}(V)$, which we will also denote by ρ. Writing $f = \sum a_g[g] \in \mathbb{C}[G]$, notice that $hfh^{-1} = f$ for any $h \in G$ because f is a class function, and therefore $hf = fh$. So $\rho(f) \in \mathrm{End}_G(V)$ for any G-module V. In particular, $\rho_i(f) \in \mathrm{End}_G(V_i)$ is a scalar operator for any $i = 1, \dots, r$ by Schur's lemma. The same is true for $\rho_i(\bar{f})$ (complex conjugation) because $\bar{f}$ is also a class function. But we have

$$0 = (\chi_i, f) = \frac{1}{|G|} \sum_{g \in G} \operatorname{Tr}(\rho_i(g))\bar{a}_g = \frac{1}{|G|} \operatorname{Tr}(\sum_{g \in G} \bar{a}_g[g]) = \frac{1}{|G|} \operatorname{Tr}(\bar{f}).$$

If a scalar operator has zero trace then it is a zero operator. Therefore, f acts trivially in any irreducible representation of G and therefore in any finite-dimensional representation of G by Maschke's Theorem, for example in $\mathbb{C}[G]$. But this is nonsense: $f \cdot 1 = f \neq 0$.

It remains to show that $\dim_{\mathbb{C}} C(G)$ is equal to the number of conjugacy classes in G, but this is clear: $C(G)$ has an obvious basis given by characteristic functions $\sum_{g \in \mathcal{O}} [g]$ for each conjugacy class $\mathcal{O} \subset G$. □

EXAMPLE 13.5.4. The quaternionic group Q_8 has 5 conjugacy classes:

$$\{1\}, \{-1\}, \{\pm i\}, \{\pm j\}, \{\pm k\}.$$

There is only one way to write 8 as a sum of five squares:

$$8 = 1^2 + 1^2 + 1^2 + 1^2 + 2^2.$$

So Q_8 has four 1-dimensional and one 2-dimensional irreducible representations. More concretely, the abelianization $Q_8/[Q_8, Q_8]] = Q_8/\{\pm 1\}$ is the Klein's four-group. Its four irreducible representations give 1-dimensional representations of Q_8. The 2-dimensional irreducible representation is given by Pauli matrices

$$I = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \quad J = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad K = \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}.$$

It is irreducible because I, J, and K have no common 1-dimensional eigenspaces. Indeed, $\mathbb{C}e_1$ and $\mathbb{C}e_2$ are the only eigenspaces for I, but these subspaces are not J-invariant.

§13.6. **Character table of the dihedral group.** Let D_n be the dihedral group (the group of symmetries of the regular n-gon). We have $|D_n| = 2n$ and

$$D_n = \{R, S\} \subset \mathrm{O}_2(\mathbb{R}),$$

where

$$R = \begin{bmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{bmatrix}$$

is a rotation by $\frac{2\pi}{n}$ and

$$S = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

is a reflection in the x-axis. In terms of generators and relations,

$$D_n = \{r, s \mid r^n = s^2 = 1,\ srs = r^{-1}\}.$$

The complexification of the standard 2-dimensional representation is a complex 2-dimensional representation where R and S act by the same matrices as above. This representation is irreducible: the only 1-dimensional eigenspaces of S are $\mathbb{C}e_1$ and $\mathbb{C}e_2$ (because the eigenvalues are different), however these subspaces are not R-invariant. Let

$$l = \begin{cases} \frac{n-1}{2} & \text{if } n \text{ is odd} \\ \frac{n-2}{2} & \text{if } n \text{ is even.} \end{cases}$$

We can write down l two-dimensional irreducible representations $T_1, \ldots, T_l$ of D_n by keeping the same matrix S and "deforming" the matrix of R:

$$R = \begin{bmatrix} \cos(2\pi k/n) & -\sin(2\pi k/n) \\ \sin(2\pi k/n) & \cos(2\pi k/n) \end{bmatrix}, \qquad k = 1, \ldots, l.$$

The relations $R^n = S^2 = \mathrm{Id}$, $SRS = R^{-1}$ still hold, and the representation is still irreducible because $\sin(2\pi k/n) \neq 0$. These representations are pairwise non-isomorphic. This can be seen by computing their characters at r:

$$2\cos(2\pi k/n) \neq 2\cos(2\pi k'/n) \quad \text{for} \quad 1 \leq k < k' \leq l.$$

Now let's use the fact that $|D_n|$ is the sum of squares of dimensions of its irreducible representations. We have

$$|D_n| - 2^2 l = \begin{cases} 2 & \text{if } n \text{ is odd} \\ 4 & \text{if } n \text{ is even.} \end{cases}$$

Since D_n has at least one (trivial) 1-dimensional representation, this shows that it has exactly 2 (if n is odd) and 4 (if n is even) of them, in addition to l two-dimensional representations described above. This shows that

$$[D_n : [D_n, D_n]] = 2 \quad \text{or} \quad 4.$$

Notice that $rsr^{-1}s^{-1} = r^2$, which generates a cyclic subgroup Γ of order n (if n is odd) or $n/2$ (if n is even). Since the index of Γ is precisely 2 or 4, we must have $[D_n, D_n] = \Gamma$. If n is odd then $D_n/\Gamma = \mathbb{Z}_2$ and if n is even then D_n/Γ is generated by cosets of s and r which both have order 2, so $D_n/\Gamma \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2$ is the Klein's 4-group. We also see that D_n has $2 + l$ (if n is odd) and $4 + l$ (if n is even) conjugacy classes. What are they? A little inspection shows that if n is odd, the conjugacy classes are

$$\{e\}, \quad \{s, sr, sr^2, \ldots, sr^{n-1}\}, \quad \{r, r^{-1}\}, \quad \{r^2, r^{-2}\}, \quad \ldots, \quad \{r^l, r^{-l}\}.$$

If n is even, the conjugacy classes are

$$\{e\}, \quad \{r^{l+1}\}, \quad \{s, sr^2, sr^4, \ldots, sr^{2l}\}, \quad \{sr, sr^3, sr^5, \ldots, sr^{2l+1}\},$$

$$\{r, r^{-1}\}, \quad \{r^2, r^{-2}\}, \quad \ldots, \quad \{r^l, r^{-l}\}.$$

We can use this information to build a *character table* of G. It is a square matrix with s rows and columns, where s is the number of conjugacy classes of G (and the number of its irreducible representations). The (i, j)-th entry is the value of the i-th irreducible character on some representative of the j-th conjugacy classes. In the same table, it is also convenient to record the size of each conjugacy class. For example, here is a character table of D_{2l+1}:

	e	$s \quad \times (2l+1)$	$r \quad \times 2$	$r^2 \quad \times 2$	$\ldots$	$r^l \quad \times 2$
Id	1	1	1	1	$\ldots$	1
M	1	-1	1	1	$\ldots$	1
T_1	2	0	$2\cos\frac{2\pi}{2l+1}$	$2\cos\frac{4\pi}{2l+1}$	$\ldots$	$2\cos\frac{2\pi l}{2l+1}$
T_2	2	0	$2\cos\frac{4\pi}{2l+1}$	$2\cos\frac{8\pi}{2l+1}$	$\ldots$	$2\cos\frac{4\pi l}{2l+1}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
T_l	2	0	$2\cos\frac{2\pi l}{2l+1}$	$2\cos\frac{4\pi l}{2l+1}$	$\ldots$	$2\cos\frac{2\pi l^2}{2l+1}$

where M is a non-trivial 1-dimensional representation. Notice that Schur's orthogonal relations give some interesting identities, for example (for T_1):

$$4 + 8\cos^2\frac{2\pi}{2l+1} + 8\cos^2\frac{4\pi}{2l+1} + \ldots + 8\cos^2\frac{2\pi l}{2l+1} = 4l + 2.$$

§13.7. **Dimension of an irreducible representation divides $|G|$.**

THEOREM 13.7.1. *Let $\rho : G \to \mathrm{GL}(V)$ be an irreducible complex representation of a finite group G. Then $\dim V$ divides $|G|$.*

Proof. Let $\bar{\mathbb{Z}}$ be the integral closure of $\mathbb{Z}$ in $\mathbb{C}$, *the ring of algebraic integers*. For any $g \in G$, all eigenvalues of $\rho(g)$ are roots of unity, and therefore algebraic integers. It follows that $\chi_V(g) \in \bar{\mathbb{Z}}$ for any $g \in G$.

For any conjugacy class $C \subset G$, let

$$I_C = \sum_{g \in C} [g]$$

be its characteristic function. It acts in V as a scalar operator $\lambda_C \operatorname{Id}_V$ by Schur's Lemma (see the proof of Theorem 13.5.3).

CLAIM 13.7.2. $\lambda_C \in \bar{\mathbb{Z}}$.

Given the Claim, we use Schur's orthogonality:

$$1 = (\chi_V, \chi_V) = \frac{1}{|G|} \sum_{g \in G} \chi_V(g)\overline{\chi_V(g)} =$$

(pick representatives $g_i \in C_i$ in all conjugacy classes $C_1, \dots, C_r$ and use that χ_V is constant on conjugacy classes)

$$= \frac{1}{|G|} \sum_{i=1}^{r} |C_i| \chi_V(g_i)\overline{\chi_V(g_i)} = \frac{1}{|G|} \sum_{i=1}^{r} \operatorname{Tr}_V(I_{C_i})\overline{\chi_V(g_i)} =$$

$$= \frac{1}{|G|} \sum_{i=1}^{r} \dim V \lambda_{C_i} \overline{\chi_V(g_i)}.$$

It follows that

$$\frac{|G|}{\dim V} = \sum_{i=1}^{r} \lambda_{C_i} \overline{\chi_V(g_i)}$$

is an algebraic integer. But it is also a rational number, and so must be an integer since $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$. So $\dim V$ divides $|G|$.

It remains to prove the Claim. For any conjugacy classes $C, C' \subset G$, $I_C \cdot I_{C'}$ is a class function and an integral linear combination of group elements. It follows that we have

$$I_C \cdot I_{C'} = \sum_{C''} a_{C''} I_{C''}, \quad a_{C''} \in \mathbb{Z}. \tag{13.7.1}$$

Next we look how both sides act on V, and (13.7.1) gives

$$\lambda_C \lambda_{C'} = \sum a_{C''} \lambda_{C''}. \tag{13.7.2}$$

Let $C_1, \dots, C_r$ be all conjugacy classes of G. Then (13.7.2) gives

$$\lambda_C \begin{bmatrix} \lambda_{C_1} \\ \vdots \\ \lambda_{C_r} \end{bmatrix} = A \begin{bmatrix} \lambda_{C_1} \\ \vdots \\ \lambda_{C_r} \end{bmatrix}$$

for some integral matrix A. This column-vector is non-trivial, for example $\lambda_{\{e\}} = 1$. It follows that each λ_C is an eigenvalue of a matrix with integer coefficients, and therefore each λ_C is an algebraic integer (as a root of the monic characteristic polynomial). $\square$

§13.8. **Burnside's Theorem.**

THEOREM 13.8.1. *Any group of order $p^a q^b$, where p and q are primes, is solvable.*

When Burnside proved this result, he made an astonishing conjecture that in fact any finite group of odd order is solvable. This was proved in 1963 by Feit and Thompson in a dense 250-page long argument, which many at the time thought was the most complicated proof ever. This has started in the earnest the quest to classify all finite simple groups, which was completed only recently.

The proof of Burnside's theorem is based on the following lemma:

LEMMA 13.8.2. *Suppose a finite group G has a conjugacy class C of size p^k, where p is prime and $k > 0$. Then G has a proper normal subgroup.*

Given the lemma, let's see how to finish the proof of Burnside's theorem. Arguing by induction, it suffices to prove that G has a proper normal subgroup. Since a p-group has a non-trivial center, we can assume that $p \neq q$ and $a, b > 0$. Let H be a Sylow q-group. Let x be a non-trivial element of the center of H. Let $Z(x)$ be the the centralizer of x in G. If $Z(x) = G$ then the cyclic group generated by x is a proper normal subgroup of G. If $Z(x) \neq G$ then $[G : Z(x)] = p^k$ for some $k > 0$ (because $H \subset Z(x)$). But $[G : Z(x)]$ is equal to the number of elements in the conjugacy class of x, and therefore G contains a proper normal subgroup by Lemma 13.8.2.

Proof of the Lemma. Let $x \in C$.

CLAIM 13.8.3. *There exists an irreducible representation $\rho : G \to \mathrm{GL}(V)$ with character χ such that p is coprime to $\dim V$ and $\chi(x) \neq 0$.*

Proof of the Claim. We have a decomposition of the regular representation

$$\mathbb{C}[G] = V_{reg} \simeq \bigoplus_{i=1}^{r} V_i^{\dim V_i},$$

the sum over all irreducible representations. Since $x \neq e$, we have

$$0 = \chi_{reg}(x) = 1 + \sum{}' (\dim V_i)\chi_{V_i}(x),$$

the summation over non-trivial irreducible representations. Unless there exists i such that $\chi_{V_i}(x) \neq 0$ and p is coprime to $\dim V_i$, we can write $\frac{1}{p}$ as an integral linear combination of $\chi(x)$ over various χ. But then $\frac{1}{p}$ is an algebraic integer, which is impossible because $\mathbb{Z}$ is integrally closed. □

CLAIM 13.8.4. *The linear operator $\rho(x)$ is scalar.*

Given the Claim, let's show that G has a proper normal subgroup. Indeed, there are two cases. If $\dim V = 1$ then G has a non-trivial one-dimensional irreducible representation, and therefore $[G, G]$ is a proper normal subgroup (G is not Abelian because it has a conjugacy class of size $p^k > 1$). If $\dim V > 1$ then the preimage of the normal subgroup $\mathbb{C}^* \operatorname{Id} \subset \mathrm{GL}(V)$ is proper (this preimage is not equal to G because V is irreducible and it is not equal to $\{e\}$ because x is in the preimage).

It remains to prove the Claim. Since $|C| = p^k$ and $\dim V$ are coprime, we can choose a and b such that

$$a|C| + b \dim V = 1.$$

Then

$$\alpha := \frac{\chi(x)}{\dim V} = a\frac{\chi(x)|C|}{\dim V} + b\chi(x).$$

While proving Theorem 13.7.1, we have noticed that

$$\frac{\chi(x)|C|}{\dim V} = \lambda_C$$

is an algebraic integer (see Claim 13.7.2). Therefore, α is also an algebraic integer. Notice that $\chi(x) = \zeta_1 + \ldots + \zeta_d$ is a sum of $d = \dim V$ n-th roots of unity (eigenvalues of $\rho(x)$), where n is the order of x in G.

There are two possibilities: either all these eigenvalues ζ_i are equal (in which case $\rho(x)$ is a scalar operator) or not, in which case

$$|\alpha| = \frac{1}{d}|\zeta_1 + \ldots + \zeta_d| < 1.$$

However, we claim that this is impossible. Let L be the cyclotomic field spanned by n-th roots of unity. Any element $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ preserves the set of n-th roots of unity, and therefore

$$|\sigma(\alpha)| = \frac{1}{d}|\sigma(\zeta_1) + \ldots + \sigma(\zeta_d)| < 1.$$

It follows that the norm of α

$$\beta := N(\alpha) = \prod_{\sigma \in \mathrm{Gal}(L/\mathbb{Q})} \sigma(\alpha) \in \mathbb{Q}$$

also satisfies $|\beta| < 1$. But each $\sigma(\alpha)$ is an algebraic integer, therefore β is an algebraic integer, and so $\beta \in \mathbb{Z}$. This gives a contradiction. □

This argument contains a wealth of ideas worth exploring. For example, in the last step we were studying algebraic integers α such that $|\beta| \leq 1$ for any conjugate of α and proved that in this case $|\beta| = 1$ for any conjugate β. In fact we have the following beautiful theorem of Kronecker.

THEOREM 13.8.5. *Let $\alpha \in \bar{\mathbb{Z}}$ and suppose $|\beta| \leq 1$ for any conjugate β of α. Then α is a root of unity.*

Proof. Let

$$f(x) = f_1(x) = \prod_{i=1}^{r}(x - \alpha_i)$$

be the minimal polynomial of α over $\mathbb{Q}$ and let

$$f_n(x) = \prod_{i=1}^{r}(x - \alpha_i^n) \quad \text{for any } n = 1, 2, \ldots.$$

Then $\alpha_1, \ldots, \alpha_r$ are all conjugates of α, and so $|\alpha_i^n| \leq 1$. It follows that coefficients of $f_n(x)$ are bounded by 2^r. These coefficients are rational algebraic integers, and therefore integers because $\mathbb{Z}$ is integrally closed. It follows that there are only finitely many possible choices for $f_1, f_2, \ldots$, and therefore any infinite subsequence of $f_1, f_2, \ldots$ contains repetitions. Taking the

sequence of powers of 2 (any other number would also work), we can find $n, m > 0$ such that $f_{2^n} = f_{2^{n+m}}$. If we compare roots of these polynomials, we see that

$$\alpha_i^{2^{n+m}} = \alpha_{\sigma(i)}^{2^n} \quad \text{for any } i,$$

where $\sigma \in S_r$ is a permutation. If s is the order of this permutation then

$$\alpha_i^{2^{n+ms}} = \alpha_i^{2^n} \quad \text{for any } i,$$

i.e. each α_i is a root of unity. □

§13.9. **Exercises.**

In this worksheet the base field is always $\mathbb{C}$ unless otherwise stated.

1. Describe explicitly all irreducible representations and build the character table for A_4.

2. Let V be the standard irreducible $(n-1)$-dimensional representation of S_n and let sgn be the 1-dimensional sign representation. Find all n such that $V \simeq V \otimes \mathrm{sgn}$.

3. Describe explicitly all irreducible representations and build the character table for S_4.

4. Let G be the group of affine transformations of $\mathbb{F}_7$ of the form

$$x \mapsto ax + b, \quad \text{where } a, b \in \mathbb{F}_7 \text{ and } a^3 = 1.$$

(a) Show that $|G| = 21$ and describe its conjugacy classes. (b) Describe explicitly all irreducible complex representations of G.

5. (continuation of the previous problem). Let V be the 7-dimensional representation of G in the algebra of functions $\mathbb{F}_7 \to \mathbb{C}$ induced by the action of G on $\mathbb{F}_7$ by affine transformation. Decompose V as a direct sum of irreducible representations.

6. In this problem k can be any field. (a) Show that if V is a representation of G then $\Lambda^n V$ is also naturally a representation. (b) Let V_1 and V_2 be representations of G. Show that

$$\Lambda^n(V_1 \oplus V_2) \simeq \sum_{a+b=n} \Lambda^a V_1 \otimes \Lambda^b V_2.$$

7. Let V be a representation of G with character χ_V. Show that

$$\chi_{\Lambda^2 V}(g) = \frac{\chi_V(g)^2 - \chi_V(g^2)}{2}.$$

8. Let V be the standard 4-dimensional irreducible representation of S_5. Show that $\Lambda^2 V$ is an irreducible 6-dimensional representation.

9. Show that columns of the character matrix are orthogonal, and more precisely that

$$\sum_{\chi} \chi(g)\overline{\chi(g)} = \frac{|G|}{c(g)},$$

where the summation is over all irreducible characters of G and $c(g)$ is the number of elements of G conjugate to g. Also show that

$$\sum_{\chi} \chi(g)\overline{\chi(g')} = 0$$

if g and g' are not conjugate.

10. For any two 2-dimensional representations V_1 and V_2 of D_5, decompose $V_1 \otimes V_2$ as a direct sum of irreducible representations.

11. Let G be a finite Abelian group of odd order $2k+1$. Let $\tau : G \to G$ be an automorphism of order 2 defined by formula

$$\tau(x) = -x.$$

Let $\hat{G}$ be a semidirect product of $\mathbb{Z}_2$ and G defined using τ. Find the number of irreducible representations of $\hat{G}$ and their dimensions.

12. Let G be a subgroup of $\mathrm{GL}_3(\mathbb{F}_5)$ of all matrices of the form

$$\begin{bmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{bmatrix}$$

(a) Compute the center and the commutator subgroup of G. (b) Find the number of irreducible representations of G and their dimensions.