Galois Cohomology of Algebraic Groups

Ayushi Tsydendorzhiev

November 15, 2024

These notes are my rendition of the lectures given by Prof. Kammeyer to the doctoral students of GRK 2240 in Düsseldorf during winter term 24/25. Sometimes I've expanded and rewritten them sufficiently or added proofs for theorems I didn't know. As of now, I've only taken some algebraic topology and commutative algebra, so these notes may reflect my currently rather limited knowledge.

Contents

1 Introduction

1.1 Galois group actions

Lecture 1, 10.10.2024

Let L/K be a Galois extension and $G = \mathrm{Gal}(L/K)$ its Galois group. The Galois group G acts on L via field automorphisms:

- Action on the field extension L: For $\mathbb{Q}(\sqrt{2})$ its Galois group $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ acts either by identity or by sending $\sqrt{2}$ to $-\sqrt{2}$.
- Action on the dual of the field extension L^*: For $\mathbb{Q}(\sqrt{2})^*$ its Galois group acts on $f(x_1, x_2) = x_1 \cdot 1 + x_2 \cdot \sqrt{2}$ either by identity or by sending f to $f' = x_1 \cdot 1 - x_2 \cdot \sqrt{2}$.
- Action on the group of nth roots of unity $\mu_n(L)$:
  - In $\mathbb{Q}(\sqrt{2})$, the nth roots of unity consist of $\{-1, 1\}$ if n is even and $\{1\}$ if n is odd. Both automorphisms in $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ leave $\mu_n(\mathbb{Q})$ fixed, so this tells us that they all belong to the base field (are rational, in this case).
  - A more interesting example is the nth cyclotomic field $\mathbb{Q}(\zeta_n)$.In this field $\mu_n(Q(\zeta_n)) = \langle \zeta_n \rangle$, the cyclic group generated by ζ_n. The Galois group $\mathrm{Gal}(Q(\zeta_n)/Q)$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^*$. For $n = 5$ (prime), the Galois group is cyclic and consists of $\{1, \zeta_5, \zeta_5^2, \zeta_5^3, \zeta_5^4\}$. The action of the Galois group then permutes the 5th roots of unity. For $n = 8$, the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/8\mathbb{Z})^* = \{1, 3, 5, 7\}$ and is cyclic of order 4. The basis of $\mathbb{Q}(\zeta_8)$ over $\mathbb{Q}$ is given by $\{1, \zeta_8, \zeta_8^2, \zeta_8^3\}$. The actions is given as: σ_1 acts trivially, σ_3 maps ζ_8 to ζ_8^3, σ_5 acts by multiplication by -1 and σ_7 maps ζ_8 to ζ_8^7.
- Action on the cyclic group $(\mathbb{Z}/n\mathbb{Z})^*$: same as above.
- Action on a finite abelian group M: trivial action.
- Action on the general linear group $\mathrm{GL}_n(L)$ over a field L of characteristic 0: $\mathrm{GL}_n(L)$ consists of $n \times n$ invertible matrices over L. We have a Galois extension L/K. The Galois group acts by applying the field automorphisms to the entries of the matrices, so $\sigma(A) = \sigma(a_{ij}) \forall 1 \leq ij \leq n$. The fixed points contain $\mathrm{GL}_n(K)$.
  - Backstory: The determinant of a $n \times n$ matrix A is defined as

    $\mathrm{sgn}(\pi)$ is either even or odd. $+1$ if even and -1 if odd.

    $$\det(A) = \sum_{\pi \in S_n} \left(\mathrm{sgn}(\pi) \prod_{i=1}^{n} a_{i,\pi(i)} \right)$$

    Consider $\sigma(\det(A))$, where $\sigma \in \mathrm{Gal}(L/K)$ is a field automorphism. It distributes over addition and multiplication:

    $$\sigma(\det(A)) = \sum_{\pi \in S_n} \left(\mathrm{sgn}(\pi) \prod_{i=1}^{n} \sigma(a_{i,\pi(i)}) \right)$$

The signum is either $+1$ or -1, so it is always in the base field K and is fixed by σ. Thus $\sigma(\det(A)) = \det(\sigma(A))$. So the action of the Galois group preserves determinants.

1.2 *The fixed point functor and exact sequences*

All of these examples are special cases of a more general concept: a group G acting on an algebraic group $\mathbb{G} \subseteq \mathrm{GL}_n$.

An algebraic group is a matrix group defined by polynomial conditions, at least this is what "The theory of group schemes of finite type over a field." by Milne says. I guess this is the consequence of Chevalley theorem?

When studying group actions, we're often interested in fixed points

$$A^G = \{a \in A \mid \forall \sigma \in G : \sigma a = a\}$$

Here, A^G represents the set of all elements in A that are fixed by every element of G. To study fixed points more systematically, we introduce the fixed point functor $-^G$. This functor takes a $\mathbb{Z}G$-module and returns its fixed points. We're particularly interested in how this functor behaves with respect to exact sequences.

Note 1.1.
Group action perspective: A $\mathbb{Z}G$-module is an abelian group A endowed with a (left) action $(\sigma, a) \mapsto \sigma a$ of G on A such that for all $\sigma \in G$ the map $\varphi_\sigma : a \mapsto \sigma a$ from A to A is a morphism of abelian groups. This implies that the action of G is distributive, $\varphi_\sigma(ab) = \varphi_\sigma(a) + \varphi_\sigma(b)$.
Ring module perspective: Equivalently, a $\mathbb{Z}G$-module is a module over the group ring $\mathbb{Z}[G]$, where elements consist of formal linear combinations of elements from group G with integer coefficients, so something like $3g_1 + 4g_2 + 10g_3 \in \mathbb{Z}[G]$. It contains both $\mathbb{Z}$ and G as subrings.
The $\mathbb{Z}[G]$-module structure encapsulates both the abelian group structure of A and the G-action on A, which leads to the key insight:

$$\{\text{module over } \mathbb{Z}[G]\} \leftrightarrow \{\text{abelian group } A \text{ with } G\text{-action}\}$$

Lemma 1.2. Consider an exact sequence of $\mathbb{Z}G$-modules:

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} 0$$

Applying the fixed point functor $-^G$ to this sequence yields:

$$0 \longrightarrow A^G \xrightarrow{f^G} B^G \xrightarrow{g^G} C^G$$

This new sequence is exact in Ab (the category of abelian groups). Thus the functor $-^G$ is left-exact, meaning it preserves exactness at the left end of the sequence.

- A natural question arises: Is the fixed point functor also right-exact? If such a lifting always exists, then the fixed point functor preserves exactness at C,

making it right-exact. If not, we've discovered an obstruction that tells us something about the Galois action and the structure of our groups.

- To investigate this, we need to check if $\ker h^G = \operatorname{im} g^G$, or equivalently, if $\operatorname{im} g^G = C^G$. Breaking this down:
  - Take any $c \in C^G$.
  - Since $C^G \subseteq C$, there exists a $b \in B$ such that $g(b) = c$.
  - If b were fixed by G, we'd be done. But it might not be.
    - Consider $\sigma b - b$ for any $\sigma \in G$. We have $g(\sigma b - b) = g(\sigma b) - g(b) = \sigma g(b) - g(b) = \sigma c - c$.
    - Since $c \in C^G$, $\sigma c - c = 0$ and $(\sigma b - b) \in \ker g$.
    - By exactness, $\ker g = \operatorname{im} f$, so $\sigma b - b \in \operatorname{im} f$.
    - We can view this as an element of A (considering f as an inclusion $A \subseteq B$).

  Why $\sigma b = b$?

  Also, $C \cong B/\operatorname{im} f$. Or consider presentations of groups.

  So the question of right-exactness boils down to whether or not every G-invariant element of C can be lifted to a G-invariant element of B and the obstruction to it lives inside of A.

  And if b were indeed in B^G then $(\sigma b - b) = 0 \in A$.

- This analysis leads us to define a map (for a given $c \in C^G$):

$$\varphi : G \to A, \quad \sigma \mapsto \sigma b - b =: a_\sigma$$

  This map is called a crossed homomorphism (also known as a derivation or 1-cocycle). It measures how far b is from being G-invariant. If b were G-invariant, this map would be identically 0! Note that this is independent of any b taken such that $g(b) = c$. Such cocycles are cohomologous.

Proposition 1.3. The map $\sigma \mapsto a_\sigma$ satisfies:

$$a_{\sigma\tau} = a_\sigma + \sigma a_\tau$$

This property is what defines a crossed homomorphism.

- **In the abelian case**, we define
  - $Z^1(G, A) = \{a' : G \to A \mid a'_{\sigma\tau} = a'_\sigma + \sigma a'_\tau\}$, the set of all crossed homomorphisms from G to A.
  - $B^1(G, A) = \{a : \sigma \in Z^1(G, A) \mid \exists a' \in A : a_\sigma = \sigma a' - a'\}$.
  - The quotient $H^1(G, A) = Z^1(G, A)/B^1(G, A)$ is called the **first cohomology group** of G with coefficients in A. It measures the obstruction to the right-exactness of the fixed point functor.

  The functor $A \mapsto H^1(G, A)$ is a derived functor of the $A \mapsto A^G$ functor.

The obstructions for right-exactness: find $\sigma b - b \in A$ such that it is 0 under projection in $Z^1(G,A)/B^1(G,A)$. It is given by $\delta(c) = [a_\sigma] \in H^1(G,A) = Z^1(G,A)/B^1(G,A)$. We can extend our original sequence to a longer exact sequence:

$$0 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G \xrightarrow{\delta} H^1(G,A) \longrightarrow H^1(G,B) \longrightarrow H^1(G,C) \longrightarrow 0$$

This sequence is exact in Ab, and the map δ (called the connecting homomorphism) measures the failure of right-exactness of the fixed point functor, since $\ker\delta$ represents all elements of C^G which can be lifted to elements of B^G.

In field theory, $H^1(G,A)$ can represent the obstruction to an element being a norm. In the theory of algebraic groups, $H^1(G,A)$ can represent the obstruction to a torsor having a rational point.

- The key idea of the 1-cocycle is to encode the failure of G-invariance in a way that's compatible with the group structures involved. It allows us to move from concrete elements (b and c) to cohomological objects ($[\varphi]$) that capture essential information about the Galois action and the relationship between our groups A, B, and C. This approach transforms specific lifting problems into more general cohomological questions, allowing us to apply powerful theoretical tools and gain deeper insights into the structures we're studying.

Exercise 1.4. Show that $H^1(G,-)$ is functorial and

$$0 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G \longrightarrow H^1(G,A) \longrightarrow H^1(G,B) \longrightarrow H^1(G,C) \longrightarrow 0$$

is exact. Find example with $\delta \neq 0$.

- *Solution:* Consider $\mathbb{Z}_2 = \{e,\sigma\}$. For a function $f : \mathbb{Z}_2 \to \mathbb{Z}$ the cocycle condition states $f(\sigma\tau) = f(\sigma) + \sigma f(\tau)$ for $\sigma,\tau \in \mathbb{Z}_2$. When $\sigma = \tau = e$, we get $f(e) = f(ee) = f(e) + ef(e) = 2f(e)$, implying $f(e) = 0$. When $\sigma = \tau$ we get $f(\sigma\sigma) = f(\sigma) + \sigma f(\sigma)$. Since $\sigma^2 = e$, we get $f(\sigma) = -\sigma(f(\sigma))$. Since σ acts by negation, we get $f(\sigma) = f(\sigma)$, so there is really no condition on σ. Each integer gives a different cocycle. Lets calculate coboundaries now. We have the coboundary condition $f(g) = g(a) - a$ for some $a \in \mathbb{Z}$. So we have $f(e) = e(a) - a = a - a = 0$ and $f(\sigma) = \sigma(a) - a = -a - a = -2a$. So every coboundary has form $e \mapsto 0$, $\sigma \mapsto -2a$. This implies that $H^1(\mathbb{Z}_2;\mathbb{Z}) = \mathbb{Z}/\mathbb{Z}_2$. Alternatively we can look at the left resolution of $\mathbb{Z}/2\mathbb{Z}$ and compute by hand.

- *Solution 2:* Let's consider a simple elliptic curve E over $\mathbb{Q}$, $f(x,y) = y^2 = x^3 - x$. it has an obvious 2-torsion point $(0,0)$. For an elliptic curve E, its quadratic twist E^d is another elliptic curve that becomes isomoprhic to E over the quadratic extension $\mathbb{Q}(\sqrt{d})$ but is not isomorphic to E over $\mathbb{Q}$. It is given by $dy^2 = x^3 - x$. The isomorphism is given by $E \to E^d, (x,y) \mapsto (x,\sqrt{d}y)$ as we have $dy^2 = x^3 - x \mapsto d(\frac{y}{\sqrt{d}})^2 = x^3 - x$ which is equivalent to $y^2 = x^3 - x$ over $\mathbb{Q}$ (if we can multiply by $\sqrt{d}$, we can transform one equation into the other). The practical use is that over $\mathbb{Q}(\sqrt{d})$ we might get new torsion points,

and Galois group $\{1, \sigma\}$ acts on these points by sending $\sqrt{d}$ to $-\sqrt{d}$. This tells us about how different the twist is from the original curve.

- We have $E(\mathbb{Q}(\sqrt{2}))^G = E(\mathbb{Q})$, the fixed points on $E(K)$ are precisely the $\mathbb{Q}$-rational points (both coordinates in $\mathbb{Q}$). For any elliptic curve E we have a short exact sequence $0 \to E[n] \to E \xrightarrow{\times n} E \to 0$. Applying the fixed point functor $(-)^G$ to it gives us the long exact sequence

  $$0 \to E[2]^G \to E(K)^G \xrightarrow{\times n} E(K)^G \to H^1(G, E[2]) \to H^1(G, E(K)) \xrightarrow{\times 2} H^1(G, E(K)) \to 0$$

  Since $E[2] = \{(0,0), (1,0), (-1,0), \infty\}$, we have $E[2]^G = E[2]$.

- **In the non-abelian case**, we define
  - $H^0(G, A) = A^G$, the fixed points as before.
  - $H^1(G, A) = Z^1(F, A)/\sim$, where $\sim$ is an equivalence relation defined by: $a_\sigma \sim b_\sigma \iff \exists a' \in A : b_\sigma = (a')^{-1} \cdot a_\sigma \cdot {}^\sigma a'$.

We cannot expect $B^1(G, A)$ to be a subgroup. Why?
${}^\sigma a$ denotes the action of σ on a.

In this case, $H^1(G, A)$ doesn't have a group structure, but is a pointed set (a set with a distinguished element). We can still define a notion of exactness for sequences of pointed sets.

Exactness in pointed sets $(A, *)$ is defined as $\operatorname{im} f = \ker g = g^{-1}(*)$
$A \leq_G B$ is G-equivariant inclusion.

Proposition 1.5. For $A \leq_G B$, we obtain $G \curvearrowright B/A$ and

$$1 \longrightarrow H^0(G, A) \longrightarrow H^0(G, B) \longrightarrow H^0(G, C) \longrightarrow H^1(G, A) \longrightarrow H^1(G, B)$$

is exact.

This is the **Galois cohomology**. Why do we care? In the non-commutative case $H^1(G, A)$ classifies "K-objects". In our lecture we will use this to classify simple and simply connected linear algebraic k-groups $\mathbb{G}$.

2 *Preliminaries from algebraic number theory.*

Lecture 2, 17.10.24
User: GRK, password: 2240.

2.1 *Number fields*

Definition 2.1. An algebraic number field is a finite field extension $k/\mathbb{Q}$.

- This definition implies the following properties:
  - The field k has characteristic 0.
  - By the Primitive Element Theorem, $k = \mathbb{Q}(a)$ for some $a \in K$.
  - There exists a unique minimal polynomial $f \in \mathbb{Q}[X]$ for a, with $\deg(f) = d = [k : \mathbb{Q}]$.
- Let $(a_1, \ldots, a_d)$ be the roots of f in the algebraic closure of $\mathbb{Q}$ within $\mathbb{C}$. These roots are called the **Galois conjugates** of a. Note that these roots do not lie in $\mathbb{Q}$.

"The concept of algebraic integer was one of the most important discoveries of number theory. It is not easy to explain quickly why it is the right definition to use, but roughly speaking, we can think of the leading coefficient of the primitive irreducible polynomials $f(x)$ as a 'denominator'.If α is the root of an integer polynomial $f(x)=dx^n + a_{n-1}x^{n-1} + \ldots$, then $d\alpha$ is an algebraic integer, because it is a root of the monic integer polynomial $x^n + a_{n-1}x_{n-1} + \ldots + d^{n-1}a_0$. Thus we can 'clear the denominator' in any algebraic number by multiplying it with a suitable integer to get an algebraic integer." — Artin, Algebra.

- Properties of embeddings:
  - For each i, the map $a \mapsto a_i$ defines an isomorphism $\mathbb{Q}(a) \cong \mathbb{Q}(a_i)$.
  - Any embedding $k \to \mathbb{C}$ must send a to some a_i.
  - There are exactly d embeddings $k \to \mathbb{C}$, denoted $\sigma_1, \ldots, \sigma_d$.
- Classification of embeddings:
  - Note that $(a_1, \ldots, a_d) = \overline{(a_1, \ldots, a_d)}$, so $\sigma_i(k) \subseteq \mathbb{R}$ if and only if $\overline{a_i} = a_i$.
  - We can thus classify the embeddings as:
    * Real embeddings (real places of K): r_1
    * Complex embeddings (complex places of K): $2r_2$ (counted in pairs due to complex conjugation)
  - This classification implies $d = r_1 + 2r_2$
- Examples:
  - For $k = \mathbb{Q}(\sqrt[3]{2})$: $r_1 = 1, r_2 = 1$
  - For $k = \mathbb{Q}(\exp(2\pi i/n))$, $n \geq 3$: $r_1 = 0, r_2 = \varphi(n)/2$ (odd n)

Definition 2.2. For any $\alpha \in K$, we define two rational numbers:
1. The norm: $N_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^{d} \sigma_i(\alpha)$
2. The trace: $Tr_{K/\mathbb{Q}}(\alpha) = \sum_{i=1}^{d} \sigma_i(\alpha)$

Note: $N_{K/\mathbb{Q}}(\alpha) = \det(\alpha : K \to K)$, and similarly for the trace.

- Basis criterion: Let $(\alpha_1, \ldots, \alpha_d) \in k$ and $\lambda_1, \ldots, \lambda_d \in \mathbb{Q}$. Then $\sum_{i=1}^{d} \lambda_i \alpha_i = 0 \iff \sum_{i=1}^{d} \lambda_i \sigma_j(\alpha_i) = 0$ for all j. Moreover, $\{\alpha_i\}_{i=1}^{d}$ is a basis of k if and only if $\det(\sigma_i(\alpha_j)) \neq 0$.

Definition 2.3. The **discriminant** of a basis $\{\alpha_1, \ldots, \alpha_d\}$ of a number field k of degree d over $\mathbb{Q}$ is defined as: $\operatorname{discr}(\{\alpha_1, \ldots, \alpha_d\}) = \det^2(\sigma_i(\alpha_j)) \in \mathbb{Q}$, where $\sigma_1, \ldots, \sigma_d$ are the d distinct embeddings of k into $\mathbb{C}$.

Exercise 2.4. Prove that $\operatorname{discr}(\alpha_i) = \det(Tr_{k/\mathbb{Q}}(\alpha_i \alpha_j))_{1 \leq i,j \leq d}$. Show that if $k = \mathbb{Q}(a)$ for some $a \in k$, then $\operatorname{discr}(\{1, a, a^2, \ldots, a^{d-1}\}) = \prod_{1 \leq i < j \leq d} (\sigma_i(a) - \sigma_j(a))^2$.

To introduce relative versions for an extension l/k, we define the relative discriminant $\operatorname{discr}()_{l/k}$ using only those embeddings $\sigma_i : l \hookrightarrow \mathbb{C}$ which restrict to the identity on k.

2.2 *Integrality in number fields*

Let k be an algebraic number field for the following discussion.

Algebraic number theory is not (algebraic) number theory but rather (algebraic number) theory.

Definition 2.5. The ring of integers in k is defined as:

$$\mathcal{O}_k = \{\alpha \in k : f(\alpha) = 0 \text{ for some monic } f \in \mathbb{Z}[X]\} = \overline{\mathbb{Z}}^k.$$

- Example: $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$. It is often referred to as the ring of "rational integers".

Proposition 2.6. For $(\alpha_1, \ldots, \alpha_r) \in k$, the following are equivalent:
1. $(\alpha_1, \ldots, \alpha_r) \in \mathcal{O}_k$
2. $\mathbb{Z}[\alpha_1, \ldots, \alpha_r]$ is finitely generated as a $\mathbb{Z}$-module.

Proof: $\implies$ If each $\alpha_i \in \mathcal{O}_k$, then it satisfies a monic polynomial with integer coefficients. Let the minimal polynomial of α_i be: $f_i(x) = x^{n_i} + a^{(i)}_{n_i-1}x^{n_i-1} + \ldots + a^{(i)}_1 x + a^{(i)}_0$ where each $a^{(i)}_j \in \mathbb{Z}$. From the minimal polynomial, we can express any higher power of α_i as a $\mathbb{Z}$-linear combination of lower powers:

$$\alpha_i^{n_i} = -\sum_{j=1}^{n_i} a^{(i)}_{n_i-j}\alpha_i^{n_i-j}$$

This means that the set $\{1, \alpha_i, \alpha_i^2, \ldots, \alpha_i^{n_i-1}\}$ spans $\mathbb{Z}[\alpha_i]$ as a $\mathbb{Z}$-module. (As any higher power is a $\mathbb{Z}$-linear combination of elements from the set and any lower power is already in the set). Now consider all monomials of the form $\alpha_1^{e_1}\alpha_2^{e_2}\ldots\alpha_r^{e_r}$, where $0 \leq e_i < n_i$. They cover all possible combination of the α_i's up to the power $n_i - 1$ for each α_i. Any higher powers can be reduced to linear combinations of these monomials using the minimal polynomials. As such, $\mathbb{Z}[\alpha_1, \ldots, \alpha_r]$ is spanned by $N = n_1 n_2 \ldots n_r$ such monomials and therefore is finitely generated over $\mathbb{Z}$. $\impliedby$ This part is trickier, so we will skip it (keyword transformations, Cayley-Hamilton, characteristic polynomial). □

- Since for $\alpha, \beta \in \mathcal{O}_k$ their sum $\mathbb{Z}[\alpha + \beta]$ and multiplication $\mathbb{Z}[\alpha \cdot \beta]$ are also finitely generated, $\mathcal{O}_k$ is a ring.

Lemma 2.7. For $\alpha \in k$, there exist $\beta \in \mathcal{O}_k, n \in \mathbb{Z}$ such that $\alpha = \frac{\beta}{n}$.

From now on we can assume that our algebraic number field is generated by a primitive element which is an algebraic integer.

Proposition 2.8. Let k be of degree d over $\mathbb{Q}$, and let a be a primitive element of k. Then

$$\mathbb{Z}[a] \subseteq \mathcal{O}_k \subseteq \frac{1}{\operatorname{discr}(1, a, \ldots, a^{d-1})}\mathbb{Z}[a]$$

Because $\mathcal{O}_k$ lies between two free abelian groups of the same rank, it must be a free abelian group of the same rank.

(Note: $\frac{1}{\operatorname{discr}(1,a,\ldots,a^{d-1})}$ is in $\mathbb{Z}$ because it is in the intersection of algebraic integers in k and $\mathbb{Q}$.)

Corollary 2.9. $\mathcal{O}_k$ has a $\mathbb{Z}$-basis of rank d. Any such basis is called an integral basis.

(Note: This relates to the theory of lattices in $\mathbb{Q}$-vector spaces and Minkowski's geometry of numbers. The covolumes of these lattices play a crucial role in understanding the structure of $\mathcal{O}_k$.)

Corollary 2.10. $\mathcal{O}_k$ is noetherian.

Definition 2.11. The discriminant of k, denoted by $\mathrm{discr}()_k$ or d_k is given by $\mathrm{discr}(\alpha_1, \ldots, \alpha_d)$ for any integral basis $\{\alpha_1, \ldots, \alpha_d\}$. This is well-defined because the change of basis matrix has determinant $\det(T...) = \pm 1$.

More generally, we can also define relative discriminants $d_{L/K}$ for a field extension L/K as $d_{L/K} = \mathrm{discr}(\beta_i)$ where β_i is a relative integral basis. This $d_{L/K}$ is an ideal in $\mathcal{O}_K$, as we might not be in a principal ideal domain anymore.

Exercise 2.12. Let $k = \mathbb{Q}(\sqrt{D})$, where D is a square-free integer. Show that:
a) If $D \equiv 1 \pmod 4$, then an integral basis is $1, \frac{1+\sqrt{D}}{2}$ and $d_k = D$.
b) If $D \equiv 2, 3 \pmod 4$, then an integral basis is $1, \sqrt{D}$ and $d_k = 4D$.

Solution:

Fun fact: for any x in a number field, TFAE:
a) The norm $N(x)$,
b) The determinant of x in matrix representation A,
c) The constant term of the characteristic polynomial of A.
Fun fact 2: for any x in a number field,
a) The trace of A is the coefficient of second highest degree in the characteristic polynomial of A.
Thus trace $\mathrm{tr}_k(x)$ and $\det_k(x)$ completely determine $\mathrm{char}_k(x, T)$ of degree 2.

- Suppose $a + b\sqrt{D} \in \mathcal{O}_k$ with $a, b \in \mathbb{Q}$. Then

$$a + b\sqrt{D} = \begin{pmatrix} a & bD \\ b & a \end{pmatrix} =: A \in M_2(\mathbb{Q}),$$

  since $(a + b\sqrt{D})(x + y\sqrt{D}) = ax + (ay + bx)\sqrt{D} + byD$. This is the product of multiplation with the "real" part $ax + byD$ and the "imaginary" part $(ay + bx)\sqrt{D}$.

- Since multiplication by $a + b\sqrt{D}$ acts like multiplication by the matrix representation, consider its characteristic polynomial $\mathrm{char}(x, T) = T^2 - 2aT + a^2 - b^2D$.
  - The constant term is $N_k(x)$.
  - The coefficient of T is $-\mathrm{tr}_k(x)$.
- For x to be an algebraic integer, we need
  - $N_k(a + b\sqrt{D}) = a^2 - b^2D \in \mathbb{Z}$
  - $\mathrm{tr}_k(x) = 2a \in \mathbb{Z}$.
- Case-by-case: assume the above is true.
  - If $a \in \mathbb{Z}$, then $b^2D \in \mathbb{Z}$. Since D is square-free and $b^2 = \frac{q^2}{p^2}$, it cannot cancel out the denominator p^2 completely. So $b^2 \in \mathbb{Z}$, thus $b \in \mathbb{Z}$ since we are working in $\mathbb{Q}$. This implies that $\{1, \sqrt{D}\}$ is the integral basis and $\mathbb{Z} + \mathbb{Z}\sqrt{D} = \mathcal{O}_k$
  - If $a \notin \mathbb{Z}$, then from trace condition it is a completely reduced proper fraction of the form $\frac{2k+1}{2} \in \mathbb{Q}$. By the norm equation, $(\frac{2k+1}{2})^2 - b^2D \in \mathbb{Z}$.
    - Let's look at $(2a)^2 - (2b)^2D \in \mathbb{Z}$. We have $2(a)^2 = (2k+1)^2 \in \mathbb{Z}$, so $(2b)^2D \in \mathbb{Z}$. Since D is square-free, $(2b)^2 \in \mathbb{Z}$, therefore $2b \in \mathbb{Z}$.

* Say, $2b = m \in \mathbb{Z}$, then $b = \frac{m}{2}$. Plug this back into the original norm equation:

$$N(a+b\sqrt{D}) = a^2 - b^2D = (\frac{2k+1}{2})^2 - (\frac{m}{2})^2D = \frac{4k^2+4k+1}{4} - \frac{m^2D}{4} \in \mathbb{Z}$$

– This fraction is integer if the numerator is $0 \bmod (4)$.
  * If m is odd, then $m = 2l+1$ and $m^2 = 4l^2+4l+1$, so we have $4(k^2 - l^2D + k - lD) + (1-D)$, which is divisible by 4 when $1 - D = 4$ or $D = 1 \bmod (4)$.
  * If m is even, then we have $\frac{1}{4} \notin \mathbb{Z}$. This implies that if $D = 2, 3 \bmod (4)$, then half-integers don't work and $a, b \in \mathbb{Z}$.
  * Normalizing a and b for $D = 1 \bmod (4)$ gives: $\frac{(2k+1}{2} + \frac{(2l+1)}{2}\sqrt{D} = k + l\sqrt{D} + \frac{1+\sqrt{D}}{2}$, so $\mathcal{O}_k = \mathbb{Z} + \mathbb{Z}(\frac{1+\sqrt{D}}{2})$.

2.3 *The arithmetic of algebraic integers*

- Example: Consider the number field $k = \mathbb{Q}(\sqrt{-5})$. In this field:
  – The ring of integers is $\mathcal{O}_k = \mathbb{Z}[\sqrt{-5}]$.
  – We have the factorization: $21 = 3 \cdot 7 = (1+2\sqrt{-5}) \cdot (1-2\sqrt{-5})$. All factors in this factorization are irreducible. This demonstrates that $\mathcal{O}_k$ is not a Unique Factorization Domain (UFD). (Consider norm of an algebraic number...)
  – Kummer's idea of ideal numbers was to address this lack of unique factorization. He proposed the concept of "ideal numbers" p_1, p_2, p_3, p_4 such that: $p_1 \cdot p_2 = 3$, $p_3 \cdot p_4 = 7$, $p_1 \cdot p_3 = 1+2\sqrt{-5}$, $p_2 \cdot p_4 = 1-2\sqrt{-5}$. This would lead to: $21 = p_1p_2p_3p_4 = p_1p_3p_2p_4$, differing only by permutation.
  – Properties of these ideal numbers:
    * $p_1 | 3$ and $p_1 | (1+2\sqrt{-5})$
    * $p_1 | (\lambda \cdot 3 + \mu \cdot (1+2\sqrt{-5}))$ for any $\lambda, \mu \in \mathcal{O}_k$
  – This suggests defining p_1 as the set of all $\alpha \in \mathcal{O}_k$ that it divides. We can thus represent these "ideal numbers" as ideals: $p_1 = (3, 1+2\sqrt{-5})$, $p_2 = (3, 1-2\sqrt{-5}) \ldots$

  This approach leads to the idea of achieving unique factorization in terms of ideals rather than elements.

Theorem 2.13. *The ring $\mathcal{O}_k$ is noetherian, integrally closed and of dimension* 1.

These three properties characterize a fundamental class of rings in algebraic number theory:

Definition 2.14. An integral domain satisfying these three properties is called a **Dedekind domain**.

The significance of Dedekind domains lies in their unique factorization property for ideals, which generalizes the unique factorization of elements in UFDs. Basically, Dedekind domains are to ideals what UFDs are to elements.

Lecture 3, 31.11.24

Theorem 2.15 (Unique Prime Ideal Factorization)**.** *Let R be a Dedekind domain. Then every nonzero fractional ideal $\mathfrak{a} \neq R$ has a unique factorization $\mathfrak{a} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\dots\mathfrak{p}_n^{e_n}$ where $\mathfrak{p}_i$ are prime ideals and $e_i \in \mathbb{Z}$.*

Let $\mathcal{O}$ be a Dedekind domain with field of fractions K.

Definition 2.16. A **fractional ideal** of $\mathcal{O}$ is a finitely generated $\mathcal{O}$-submodule $\mathfrak{a}$ of K.

- Key examples and properties:
  - Every integral ideal $\mathfrak{a} \subseteq \mathcal{O}$ is a fractional ideal.
  - For any $a \in K^*$, the principal fractional ideal (a) is a fractional ideal.
  - If $\mathfrak{a}$ is a fractional ideal, then $\alpha\mathfrak{a}$ is also a fractional ideal for any $\alpha \in K^*$.
- A key characterization: An $\mathcal{O}$-submodule $\mathfrak{a} \subseteq K$ is a fractional ideal if and only if there exists a nonzero element $c \in \mathcal{O}$ such that: $c \cdot \mathfrak{a} \subseteq \mathcal{O}$ This c effectively "clears the denominators" in $\mathfrak{a}$, making $c\mathfrak{a}$ an integral ideal.
- For a nonzero fractional ideal $\mathfrak{a}$, we define its inverse: $\mathfrak{a}^{-1} = \{x \in K : x \cdot \mathfrak{a} \subseteq \mathcal{O}\}$. This set is itself a fractional ideal, since it's clearly an $\mathcal{O}$-module and for the c that clears denominators in $\mathfrak{a}$, we have $c\mathfrak{a}^{-1} \subseteq \mathcal{O}$.

Definition 2.17. The fractional ideals form the **ideal group** J_K under multiplication where:
1) Multiplication: $\mathfrak{ab} = \sum_i a_i b_i : a_i \in \mathfrak{a}, b_i \in \mathfrak{b}$.
2) Inverse: $\mathfrak{a}^{-1} = x \in K : x\mathfrak{a} \subseteq \mathcal{O}$.
3) Identity: the ring $\mathcal{O}$ itself, denoted (1).

Corollary 2.18. Every $\mathfrak{a} \in J_K$ has a unique decomposition: $\mathfrak{a} = \prod_{(0)\neq\mathfrak{p}} \mathfrak{p}^{v_\mathfrak{p}}$ where $v_\mathfrak{p} \in \mathbb{Z}$ and almost all $v_\mathfrak{p} = 0$. This shows J_K is free abelian with basis $\mathrm{Spec}(\mathcal{O}) \setminus (0)$.

Let $P_K = \{(a) : a \in K^*\}$ be the **principal fractional ideals**.

$Cl_K = \{$ fractional ideals / principal fractional ideals $\}$.

Definition 2.19. The **class group** $Cl_K = J_K/P_K$ fits in the exact sequence:

$$1 \to \mathcal{O}^* \to K^* \to J_K \to Cl_K \to 1$$

Here $K^*/\mathcal{O}^*$ measures the gain/loss in passing from numbers to ideal numbers.

Loss or gain, are the same.

- Further without proofs: For number fields $K = k$ with ring of integers $\mathcal{O}_k$, we have the Gauss-Minkowski theorem.

Theorem 2.20 (Gauss-Minkowski)**.** *The class group Cl_k of a number field k is finite.*

- The order $|Cl_k| = h_k$ is called the **class number** of k. This invariant measures how far $\mathcal{O}_k$ is from being a principal ideal domain.
  - Notable example: For square-free $D > 0$, the class number $h_{\mathbb{Q}(\sqrt{-D})} = 1$ if and only if: $D \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$. This result (Gauss' conjecture) was proven by Baker-Stark-Heegner.
  - Still open: The class number problem remains challenging. For instance, it's unknown whether infinitely many D exist with $h_{\mathbb{Q}(\sqrt{D})} = 1$.
- For Dedekind domains: $Cl_k = 1 \iff \mathcal{O}_k$ is a PID, PID $\implies$ UFD (always) and in Dedekind domains specifically UFD $\implies$ PID (exercise).

Theorem 2.21 (Dirichlet's Unit Theorem)**.** *The unit group of $\mathcal{O}_k$ has the structure:*

$$\mathcal{O}_k^* \cong \mu(k) \oplus \mathbb{Z}^{r_1+r_2-1}$$

where μ_k is the gro7up of roots of unity in k, r_1 is the number of real embeddings and r_2 is the number of pairs of complex embeddings.

Proof strategy: "Geometry of numbers", lattice, convex closed subsets, etc...

Exercise 2.22. Prove that $\mathcal{O}_k/\mathfrak{a}$ is finite for every nonzero ideal $\mathfrak{a}$. Hint: First consider the case where $\mathfrak{a} = \mathfrak{p}$ is prime.

Definition 2.23. The **absolute norm** of a nonzero ideal $\mathfrak{a}$ is: $n(\mathfrak{a}) = |\mathcal{O}_k/\mathfrak{a}|$

- Key properties:
  - For principal ideals: $n((a)) = |N_{k/\mathbb{Q}}(a)|$
  - Multiplicative: $n(\mathfrak{ab}) = n(\mathfrak{a})n(\mathfrak{b})$
  - Defines a homomorphism: $J_K \to \mathbb{R}_{>0}$

Exercise 2.24. Prove the above properties.

This is all we need about integrality in number fields.

2.4 *Decomposition and ramification*

Let k be a number field of degree d and $\mathfrak{p}$ a rational prime. In $\mathcal{O}_k$, $\mathfrak{p}$ decomposes as $\mathcal{O}_k = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$. Note that each $\mathcal{O}_k/\mathfrak{p}_i$ is a finite field, so if we let $f_i = [\mathcal{O}_k/\mathfrak{p}_i : \mathbb{F}\mathfrak{p}]$, then $n(\mathfrak{p}_i) = \mathfrak{p}^{f_i}$. Applying n to the decomposition of $\mathfrak{p}\mathcal{O}_k$, we get: $\mathfrak{p}^d = \mathfrak{p}^{e_1 f_1} \cdots \mathfrak{p}^{e_r f_r}$. Therefore $e_1 f_1 + \cdots + e_r f_r = d$ (fundamental equation). We call e_i the ramification index of $\mathfrak{p}_i$ over p and f_i the inertia degree of $\mathfrak{p}_i$ over p.

- Extreme cases: for prime ideals in $\mathcal{O}_k$ over rational primes:

- $r = d$: $\mathfrak{p}$ is **split**.
- $r = 1, f_1 = 1$: $\mathfrak{p}$ **ramifies completely**.
- $r = 1, e_1 = 1$: $\mathfrak{p}$ is **inert**.

We say $p_i|p$ if and only if $p\mathcal{O}_k \subseteq p_i$ for a unique rational prime p, and say "$\mathfrak{p}_i$ lies over p".

Definition 2.25. A rational prime p is called ramified in k if $e_p > 1$ for some prime ideal $\mathfrak{p}$ lying over p.

Theorem 2.26. *A rational prime p is ramified in k if and only if $p|d_k$ (where d_k is the discriminant).*

Theorem 2.27. *Only finitely many rational primes ramify in k.*

Logically, everything now is ideals (except for maybe ramification).

- The Galois group acts on prime ideals lying over rational primes. This action:
  - Is transitive (exercise)
  - Preserves ramification indices e_i and inertia degrees f_i

  Therefore, in the Galois case, the fundamental equation becomes: $d = efr$. For cyclic extensions of prime degree over $\mathbb{Q}$, this constrains possible decomposition types to the three extreme cases listed above.

2.5 *Valuations and completions*

Note 2.28. In a number field k, we can study its arithmetic through two equivalent perspectives. The first approach uses ideal theory, where we study the factorization behavior of prime ideals $\mathfrak{p}$ in $\mathcal{O}_k$. The second approach uses valuations, where each prime ideal $\mathfrak{p}$ naturally gives rise to a $\mathfrak{p}$-adic valuation $v_\mathfrak{p} : k^* \to \mathbb{Z}$. This valuation comes from the prime factorization of principal ideals: when we write $x\mathcal{O}_k = \prod \mathfrak{p}_\mathfrak{p}^{v_\mathfrak{p}(x)}$, the exponent $v_\mathfrak{p}(x)$ is our valuation. We can then define a non-archimedean absolute value by setting $|x|_\mathfrak{p} = q^{-v_\mathfrak{p}(x)}$. This transition from ideals to valuations leads naturally to completions and local fields, providing powerful analytical tools for studying number theoretic questions.

Definition 2.29. A **valuation** of k is a map $|\cdot| : k \to \mathbb{R}$ satisfying for all $x, y \in k$:
1) $|x| \geq 0$ (non-negativity)
2) $|xy| = |x||y|$ (multiplicativity)
3) $|x + y| \leq |x| + |y|$ (triangle inequality)

The term "valuation" typically refers to the exponential valuation.

- We exclude the trivial valuation $|x| = 1 \iff x \neq 0$.

- A valuation is **non-archimedean** if $|x+y| \leq \max|x|,|y|$, and **archimedean** otherwise.
- Example:
  - Archimedean: For $\sigma : k \hookrightarrow \mathbb{C}$, define $|x|_\sigma = |\sigma(x)|$
  - Non-archimedean: For prime ideal $\mathfrak{p}_0 \subseteq \mathcal{O}_k$:
    * Write $x\mathcal{O}k = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(x)}$ for $x \in k^*$
    * Set $|x|_{\mathfrak{p}_0} = q^{-v_{\mathfrak{p}_0}(x)}$ where $q = |\mathcal{O}_k/\mathfrak{p}_0| = p^{f_p}$ for $\mathfrak{p}_0 \cap \mathbb{Z} = (p)$ (p-adic valuation)

Definition 2.30. Two valuations are equivalent if they differ by scaling or induce the same topology.

Theorem 2.31 (Ostrowski)**.** *These examples give all valuations on k up to equivalence.*

Lecture 4, 07.11.24

Definition 2.32. The equivalence classes of these valuations are called places. We have finite places (from non-archimedean valuations) and infinite places (from archimedean valuations).

- Intuitively, places correspond to different ways to "view" elements of a field. Finite places correspond to prime ideals in the ring of integers. Infinite places correspond to real and complex embeddings. Each place gives us a different notion of "being small" or "being close". For any place v, we can create a complete field by adding all limits of Cauchy sequences:

Definition 2.33. The completion k_v of k with respect to the place v is: $k \hookrightarrow k_v$ where k_v is complete with respect to the metric $d_v(x,y) = |x-y|_v$. Formally: $k_v = \frac{\{\text{ Cauchy sequences in } k\}}{\{\text{null sequences}\}}$.

- Examples: For a prime p, completing $\mathbb{Q}$ with respect to the p-adic valuation gives the p-adic numbers $\mathbb{Q}_p$. Completing $\mathbb{Q}$ with respect to the usual absolute value gives $\mathbb{R}$.

Definition 2.34. For a place v, we have two important rings:
1) $O_{(v)} = \{x \in k : v(x) \leq 1\} \subset k$.
2) $O_v = \{x \in k : v(x) \leq 1\} \subset k_v$.

- Key properties:
  - Both are principal ideal domains (PIDs),
  - Both have unique maximal ideals πO_v and $\pi O_{(v)}$ respectively, these are discrete valuation rings (DVRs),
  - A uniformizer π generates these maximal ideals.

Theorem 2.35 (Extensions of valuations)**.** *Let K be complete with valuation v and L/K be algebraic. Then v extends uniquely to L and if $[L : K] = d < \infty$, then for $x \in L$: $\nabla(x) = \sqrt[d]{v(N_{L/K}(x)}$.*

- Important special case: for the p-adic valuation v_p on $\mathbb{Q}_p$:
  - Extends uniquely to $\overline{\mathbb{Q}}_p$,
  - Given embedding $\sigma : k \hookrightarrow \overline{\mathbb{Q}}_p$, get valuation $v_\sigma = \overline{v_p} \circ \sigma$,
  - If $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$, then $v_\sigma = v_{\tau\circ\sigma}$.

Theorem 2.36 (Classification of Extended Valuations)**.** *Let k be a number field and v_p be the p-adic valuation on $\mathbb{Q}$. Then:*
1) Every extension w of v_p from $\mathbb{Q}$ to k is of the form $w = v_\sigma$ for some embedding $\sigma : k \hookrightarrow \overline{\mathbb{Q}}_p$.
2) Two such extensions are equal ($v_\sigma = v_{\sigma'}$) if and only if there exists $\tau \in Gal(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ such that $\sigma' = \tau \circ \sigma$.

Note 2.37. This theorem tells us that all possible ways to extend the p-adic valuation come from embeddings into $\overline{\mathbb{Q}}_p$. Two different embeddings give the same valuation precisely when they differ by an automorphism of $\overline{\mathbb{Q}}_p$ over $\mathbb{Q}_p$. This explains why we get a finite number of extensions for each prime $\mathfrak{p}$, corresponding to the different prime ideals lying over p.

- Places can be classified according to their completions:
  - Finite places correspond 1-1 with:
    - Conjugacy classes of embeddings $\sigma : k \hookrightarrow \overline{\mathbb{Q}}_p$
    - Non-zero prime ideals $\mathfrak{p}$ of O_k lying over p
  - Infinite places correspond 1-1 with:
    - Real: Embeddings $\sigma : k \hookrightarrow \mathbb{R}$
    - Complex: Conjugate pairs of embeddings $\sigma : k \hookrightarrow \mathbb{C}$, $\sigma(k) \not\subset \mathbb{R}$
- For a place w lying over p, we have the following fundamental diagram:

$$\begin{array}{ccc} k & \longrightarrow & k_w \\ \uparrow & & \uparrow \\ \mathcal{O}_k & \longrightarrow & \mathcal{O}_p \end{array}$$

This square is commutative and shows: the vertical arrows represent inclusions, the horizontal arrows represent completions, $\mathcal{O}_k$ is the ring of integers of k, $\mathcal{O}_p$ is the ring of integers in the completion. This diagram illustrates how the local and global perspectives interact: completing the global field k and its ring of integers O_k at a prime gives us the local field k_w and its ring of integers O_p.

Theorem 2.38 (Local Decomposition). *For a rational prime $p < \infty$, we have $k \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong \prod_{w|p} k_w$. Moreover, for each place $w|p$: $[k_w : \mathbb{Q}_p] = e_w \cdot f_w$.*

Note 2.39. This theorem lets us understand the relationship between a number field k and its completions above a prime p.
The tensor product $k \otimes_{\mathbb{Q}} \mathbb{Q}_p$ represents what happens when we view our number field k "through p-adic glasses" - mathematically speaking, this is called base change to $\mathbb{Q}_p$. Remarkably, this decomposes into pieces, one for each place w of k lying above p. Each piece is a completion k_w, which is itself a finite extension of $\mathbb{Q}_p$.
To understand each piece k_w, we look at its degree over $\mathbb{Q}_p$. This degree factors as $[k_w : \mathbb{Q}_p] = e_w \cdot f_w$, where:
1) e_w is the ramification index, telling us how much ramification occurs above p
2) f_w is the inertia degree, measuring how much the residue field grows
This decomposition explains precisely how a rational prime p can "split" when we move up to our number field k. In fact, we can recover the global degree of our number field from these local pieces: $[k : \mathbb{Q}] = \sum_{w|p} [k_w : \mathbb{Q}_p]$. Each completion k_w thus represents a "local piece" of k sitting above p, and together these pieces contain all the local information about how p behaves in k. For example, if $k = \mathbb{Q}(\sqrt{5})$ and $p = 5$, there is only one place above 5, and we have $e = 2$, $f = 1$, matching the global degree $[k : \mathbb{Q}] = 2$. In contrast, for $p = 11$, which splits completely, we get two places each with $e = f = 1$, and again their degrees sum to 2.

Definition 2.40. The ring of adeles $\mathbb{A}_k$ combines all completions:
1) $\mathbb{A}k = \prod w \in V(k) k_w$ with restriction that elements lie in O_w for almost all w
2) The idele group $\mathbb{I}_k = \mathbb{A}_k^*$ (multiplicative group of adeles)
3) k embeds diagonally in both with discrete image

2.6 *Local-global principle*

The fundamental question: If an equation has solutions in all completions k_v (local solutions), does it have a solution in k (global solution)?

- Success Cases: The principle works for:
  - Quadratic forms (Minkowski-Hasse)
  - Norm equations for cyclic extensions
  - Some other special polynomials
- Famous Counterexamples:
  - Selmer's cubic: $3x^3 + 4y^3 + 5z^3 = 0$
  - Genus 1 curves can fail
  - Higher degree forms often fail

- Modern Understanding:
  - Obstruction is measured by the Shafarevich-Tate group
  - For genus 0 curves, principle holds
  - For genus ≥ 1, additional cohomological obstructions appear
  - Brauer-Manin obstruction explains many failures

Theorem 2.41. *Hasse norm principle. Let $k/\mathbb{Q}$ be cyclic and $x \in \mathbb{Q}$. Then $x = N_{k/\mathbb{Q}}(y)$ for some $y \in k$ iff $x = N_{k_v/\mathbb{Q}_p}(y_v)$ for some $y_k \in k_v$ for all $v|p$ and all $p \geq \infty$.*

Theorem 2.42. *Hasse principle for central simple algebras.*

Lecture 5, 22.11.2024