The Idèle Class Group

Hendrik Lenstra

1. Definitions

Let K be an algebraic number field. Let $\mathfrak{p}$ be a prime of K. We denote by $K_\mathfrak{p}$ the completion of K at the prime $\mathfrak{p}$: if $\mathfrak{p}$ is a finite place, then $K_\mathfrak{p}$ is a non-archimedean field which is a finite extension of $\mathbb{Q}_p$; if $\mathfrak{p}$ is an infinite place, then $K_\mathfrak{p}$ is $\mathbb{R}$ or $\mathbb{C}$. If $\mathfrak{p}$ is finite, then $\mathcal{O}_\mathfrak{p}$ denotes the set of integral elements

$$\mathcal{O}_\mathfrak{p} = \{x \in K_\mathfrak{p} : |x|_\mathfrak{p} \leq 1\}.$$

The *adèle ring* of K is

$$\mathbf{A}_K = \prod_{\mathfrak{p}}{}' K_\mathfrak{p} = \left\{ (x_\mathfrak{p})_\mathfrak{p} \in \textstyle\prod_\mathfrak{p} K_\mathfrak{p} : |x_\mathfrak{p}|_\mathfrak{p} \leq 1 \text{ for all but finitely many } \mathfrak{p} \right\}.$$

This product is given a topology as follows: $U \subset \mathbf{A}_K$ is open if and only if for all $a \in \mathbf{A}_K$, one has that the set

$$(a + U) \cap \left(\textstyle\prod_{\mathfrak{p}|\infty} K_\mathfrak{p} \times \prod_{\mathfrak{p}<\infty} \mathcal{O}_\mathfrak{p} \right)$$

is open in the product topology.

This group may look big, but in fact there is a sense for which it is not so large. We embed $K \subset \mathbf{A}_K$ by $x \mapsto (x)_\mathfrak{p}$; this map is well-defined because $|x|_\mathfrak{p} > 1$ for only finitely many primes $\mathfrak{p}$ of K. The image of K in $\mathbf{A}_K$ has the discrete topology and hence it is closed in $\mathbf{A}_K$; the quotient $\mathbf{A}_K/K$ is a connected compact Hausdorff topological group. So the adèles $\mathbf{A}_K$ themselves are not far from a smaller (compact) group: it has a quotient which is compact. We say that K in $\mathbf{A}_K$ is *cocompact*. In some sense, this is like how $\mathbb{Z} \subset \mathbb{R}$: the quotient is the compact circle group $\mathbb{R}/\mathbb{Z}$.

As an example, we may take $\mathbf{A}_\mathbb{Q}/\mathbb{Q}$. This is the solenoid, $\mathbf{S}$, an infinitely winding circle. In general, $\mathbf{A}_K/K = \mathbf{S} \otimes_\mathbb{Q} K$. (For more on this, see the exercises.)

We pass now to the multiplicative situation. The *idèle group* of K is

$$\mathbf{J}_K = \mathbf{A}_K^* = \left\{ (x_\mathfrak{p})_\mathfrak{p} \in \textstyle\prod_\mathfrak{p} K_\mathfrak{p}^* : |x_\mathfrak{p}| = 1 \text{ for all but finitely many } \mathfrak{p} \right\}.$$

In the relative topology, inversion is not a continuous operation! To get the correct topology, we declare that $U \subset \mathbf{J}_K$ is open if and only if for all $a \in \mathbf{J}_K$, the set

$$aU \cap \left(\textstyle\prod_{\mathfrak{p}|\infty} K_\mathfrak{p}^* \times \prod_{\mathfrak{p}<\infty} \mathcal{O}_\mathfrak{p}^* \right)$$

is open in the product topology. In general, if R is a topological ring, R^* becomes a topological group when you give R^* the relative topology from

$$R^* \subset R \times R$$
$$u \mapsto (u, u^{-1}).$$

Just as $K \subset \mathbf{A}_K$ is discrete, $K^* \subset \mathbf{J}_K$ is also discrete, but this time it is only *almost* cocompact. So we study $C_K = \mathbf{J}_K/K^*$, the *idèle class group.*

Example 1.1. *Take the example $K = \mathbb{Q}$. We have a canonical isomorphism*

$$\mathbb{Q}_p^* \cong \langle p \rangle \times \mathbb{Z}_p^*$$

defined by taking the p-adic valuation. If we identify $\mathbb{Z} \cong \langle p \rangle$, then

$$\mathbf{J}_\mathbb{Q} = \mathbb{R}^* \times {\prod_p}' \mathbb{Q}_p^* \cong \{\pm 1\} \times \mathbb{R}_{>0} \times \prod_p \mathbb{Z}_p^* \times \bigoplus_p \mathbb{Z}.$$

There appears a direct sum on the right-hand side because an element of the restricted direct product is a p-adic unit for all but finitely many p.

We project $\mathbf{J}_\mathbb{Q}$ onto the product of the first and last factor:

$$\mathbf{J}_\mathbb{Q} \to \{\pm 1\} \times \bigoplus_p \mathbb{Z} \to 0.$$

Looking at $\mathbb{Q}^* \subset \mathbf{J}_\mathbb{Q}$, if we write $r = \epsilon \prod_p p^{n(p)}$, where $\epsilon \in \{\pm 1\}$ and $n(p) = \mathrm{ord}_p(r)$, then $r \mapsto (\epsilon, (n(p))_p)$ in the projection. Therefore $\mathbb{Q}^*$ is canonically identified with $\{\pm 1\} \times \bigoplus_p \mathbb{Z}$ in $\mathbf{J}_\mathbb{Q}$. (Here we use that the ring of integers $\mathbb{Z}$ has unique factorization and units only ± 1; for a general number field, we face problems associated with units and the class group of the field.)

Putting these together, we see that

$$\mathbf{J}_\mathbb{Q} \cong \mathbb{Q}^* \times \mathbb{R}_{>0} \times \prod_p \mathbb{Z}_p^*.$$

By the logarithm map, $\mathbb{R}_{>0} \cong \mathbb{R}$, therefore

$$\mathbf{J}_\mathbb{Q} \cong \mathbb{Q}^* \times \mathbb{R} \times \widehat{\mathbb{Z}}^*,$$

and $C_\mathbb{Q} \cong \mathbb{R} \times \widehat{\mathbb{Z}}^*$.

Note that even for $\mathbb{Q}$ the idèle class group is neither profinite or compact. But the noncompactness is only because of the presence of the term $\mathbb{R}$; for any number field K, we map

$$J_K \to \mathbb{R}_{>0}$$
$$(x_\mathfrak{p})_\mathfrak{p} \mapsto \prod_\mathfrak{p} |x_\mathfrak{p}|_\mathfrak{p},$$

the valuation being normalized in such a way that the product formula holds. This map is clearly surjective, so we obtain an exact sequence

$$1 \to \mathbf{J}_K^0 \to \mathbf{J}_K \to \mathbb{R}_{>0} \to 1.$$

In fact, the kernel $\mathbf{J}_K^0$ is compact, a statement equivalent to the Dirichlet unit theorem and the finiteness of the class group. This exact sequence splits by mapping

$$\begin{aligned} \mathbb{R}_{>0} &\to \mathbf{J}_K \\ \lambda &\mapsto (\underbrace{1, \dots, 1}_{\mathfrak{p}<\infty}, \underbrace{\lambda^{1/n}, \dots, \lambda^{1/n}}_{\mathfrak{p}|\infty}). \end{aligned}$$

Here r_1 denotes the number of real primes, r_2 the number of complex primes. Therefore $\mathbf{J}_K \cong \mathbb{R} \times \mathbf{J}_K^0$ as topological groups. Since $K^* \subset \mathbf{J}_K^0$ (by the product formula), one gets the same story for $C_K \cong \mathbb{R} \times C_K^0$.

For example, $C_{\mathbb{Q}}^0 \cong \widehat{\mathbb{Z}}^*$, and note that this is exactly $G_{\mathbb{Q}}^{\mathrm{ab}}$.

2. Interpreting C_K

Now we interpret elements of C_K in terms of modules just as we may interpret elements of the class group and the Picard group.

Recall that the class group of K, Cl_K, is the quotient of the set of $\mathcal{O}$-ideals by the principal ideals. The class group can also be realized by the group $\mathrm{Pic}\,\mathcal{O}$, the set of isomorphism classes of projective $\mathcal{O}$-modules of rank 1, by the map

$$\begin{aligned} \mathrm{Cl}_K &\cong \mathrm{Pic}\,\mathcal{O} \\ [I] &\mapsto I, \end{aligned}$$

where we view I as an $\mathcal{O}$-module.

The Picard group of K, Pic_K, is defined to be the set of isomorphism classes of metrized projective $\mathcal{O}$-modules of rank 1, defined as follows. A projective $\mathcal{O}$-module P of rank 1 is *metrized* if it is equipped with a positive definite symmetric bilinear form $\langle , \rangle : P_{\mathbb{R}} \to \mathbb{R}$, where

$$P_{\mathbb{R}} = P \otimes_{\mathbb{Z}} \mathbb{R} = P \otimes_{\mathcal{O}} K_{\mathbb{R}},$$

such that for all $x, y \in P_{\mathbb{R}}$ and $\lambda \in K_{\mathbb{R}}$, $\langle \lambda x, y \rangle = \langle x, \overline{\lambda} y \rangle$, where $z \mapsto \overline{z}$ is the canonical involution of $K_{\mathbb{R}}$ as an $\mathbb{R}$-algebra. (For more information on this construction, see the notes by René Schoof.) There is an obvious surjection $\mathrm{Pic}_K \to \mathrm{Cl}_K$ which forgets the metric.

Finally, we have a surjection $C_K \to \mathrm{Pic}_K$. We view C_K as the set of isomorphism classes of pairs (V, ϕ) where V is a 1-dimensional K-vector space and $\phi : V \to \mathbf{A}_K$ is a K-linear map inducing an isomorphism $V \otimes_K \mathbf{A}_K \xrightarrow{\sim} \mathbf{A}_K$. To obtain an element of Pic_K, one takes as the projective module the elements of V which are units at all places and uses the infinite primes to get a suitable metric.

Altogether, we have the system:

$$\begin{array}{c}
\mathrm{Cl}_K \cong \{\text{Projective } \mathcal{O}\text{-modules of rank } 1\}/\cong_{\mathcal{O}} \\
\uparrow \\
\mathrm{Pic}_K \cong \{\text{Metrized projective } \mathcal{O}\text{-modules of rank } 1\}/\cong_{\mathcal{O}} \\
\uparrow \\
C_K \cong \{(V, \phi : V \to \mathbf{A}_K) : \phi \text{ induces } V \otimes_K \mathbf{A}_K \xrightarrow{\sim} \mathbf{A}_K\}
\end{array}$$

We then have

$$1 \to \mu \to \textstyle\prod_{\mathfrak{p}} \{x \in K_{\mathfrak{p}} : |x|_{\mathfrak{p}} = 1\} \to C_K \to \mathrm{Pic}_K \to 1.$$

At a complex prime, the product $\prod_{\mathfrak{p}} \{x \in K_{\mathfrak{p}} : |x|_{\mathfrak{p}} = 1\}$ is the circle group; at a real prime, it is $\{\pm 1\}$; and at a finite prime, it is the group of units $\mathcal{O}_{\mathfrak{p}}^*$.

3. Idèlic Class Field Theory

Fixing an algebraic closure $\overline{K} \supset K$, we have a bijection

$$\begin{aligned}
\{L \subset \overline{K} : L \supset K \text{ finite abelian}\} &\leftrightarrow \{H \subset C_K : H \text{ open subgroup}\} \\
L &\mapsto N_{L/K} C_L.
\end{aligned}$$

This is a main theorem of idèlic class field theory.

What are these open subgroups? Let $\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n(\mathfrak{p})}$ be a cycle, where $n(\mathfrak{p}) \geq 0$ for all $\mathfrak{p}$, $n(\mathfrak{p}) = 0$ for almost all $\mathfrak{p}$, and

$$n(\mathfrak{p}) = \begin{cases} 0 \text{ or } 1, & \mathfrak{p} \text{ real}, \\ 0, & \mathfrak{p} \text{ complex}. \end{cases}$$

Given such a cycle $\mathfrak{m}$, we have an open subgroup $W_{\mathfrak{m}} \subset \mathbf{J}_K$, where

$$W_{\mathfrak{m}} = \prod_{n(\mathfrak{p})=0}' K_{\mathfrak{p}}^* \times \prod_{\substack{\mathfrak{p} \text{ real} \\ n(\mathfrak{p}) \neq 0}} K_{\mathfrak{p},>0}^* \times \prod_{\substack{\mathfrak{p} < \infty \\ n(\mathfrak{p}) > 0}} (1 + \mathfrak{p}^{n(\mathfrak{p})}).$$

A subgroup of $\mathbf{J}_K$ is open if and only if it contains an $W_{\mathfrak{m}}$: one can read this off almost immediately from the definition of the topology. Note that for such an open subgroup, at every complex place one has the entire component and at every real place one has the component up to finite index. We may take the image $\overline{W_{\mathfrak{m}}} = (W_{\mathfrak{m}} K^*)/K^* \subset C_K$, and we see that a subgroup of C_K is open if and only if it contains $\overline{W_{\mathfrak{m}}}$ for some $\mathfrak{m}$. Then under the above correspondence, we have the isomorphisms $\mathrm{Gal}(L/K) \cong C_K/H$ and in $C_K/\overline{W_{\mathfrak{m}}} \cong \mathrm{Cl}_{\mathfrak{m}}$, where $\mathrm{Cl}_{\mathfrak{m}}$ is the ray class group.

Combining the surjections $C_K \to \mathrm{Gal}(L/K)$, we obtain a surjective map

$$C_K \to \varprojlim_L \mathrm{Gal}(L/K) = G_K^{\mathrm{ab}}.$$

Let D_K be the connected component of 1 in C_K. Then D_K is a closed subgroup, and it is exactly the kernel of the above map, so $C_K/D_K \cong G_K^{\mathrm{ab}}$. In fact, the topological group D_K is isomorphic to

$$D_K \cong \mathbb{R} \times (\mathbb{R}/\mathbb{Z})^{r_2} \times \mathbf{S}^{r_1+r_2-1}$$

where r_1 is the number of real primes, r_2 the number of complex primes, and $\mathbf{S}$ is the solenoid defined in the beginning of these notes.

Exercises

Exercise 6.1. View $\mathbb{Z}$ as a subgroup of $\mathbb{R}\times\widehat{\mathbb{Z}}$ by identifying $n \in \mathbb{Z}$ with $(n, n) \in \mathbb{R}\times\widehat{\mathbb{Z}}$. Give $\mathbb{R} \times \widehat{\mathbb{Z}}$ the product topology, and give $\mathbf{S} = (\mathbb{R} \times \widehat{\mathbb{Z}})/\mathbb{Z}$ the quotient topology. The topological group $\mathbf{S}$ is called the *solenoid*.

(a) Prove that $\mathbf{S}$ is compact, Hausdorff, and connected.
(b) Prove that $\mathbf{S}$ has the structure of a vector space over $\mathbb{Q}$.

An exact sequence $0 \to B \to C \to D \to 0$ of topological abelian groups with continuous group homomorphisms is said to *split* if there is an isomorphism $f\colon C \to B\times D$ of topological groups such that (i) the map $B \to C \to B\times D$ is the canonical inclusion $B \to B \times D$; and (ii) the map $C \to B \times D \to D$ is the given map $C \to D$.

Exercise 6.2.

(a) Prove that there is an exact sequence $0 \to \widehat{\mathbb{Z}} \to \mathbf{S} \to \mathbb{R}/\mathbb{Z} \to 0$ of groups with continuous group homomorphisms.
(b) Prove that the sequence does not split, even if in the definition given above the map f is only required to be an isomorphism of *topological spaces* satisfying (i) and (ii).
(c) Prove that the sequence does not split, even if in the definition given above the map f is only required to be a *group* isomorphism satisfying (i) and (ii).

Exercise 6.3.

(a) Prove: $\widehat{\mathbb{Z}} \cong \mathrm{End}(\mathbb{Q}/\mathbb{Z})$ (as rings).
(b) Prove: $\mathbf{S} \cong \mathrm{Hom}(\mathbb{Q}, \mathbb{R}/\mathbb{Z})$ (as groups).
(c) Prove: $\mathbf{S} \cong \mathbf{A}_{\mathbb{Q}}/\mathbb{Q}$ (as topological groups), with $\mathbf{A}_{\mathbb{Q}}$ denoting the ring of adèles of $\mathbb{Q}$.

Below, we let K be an algebraic number field, with ring of integers $\mathcal{O}$, idèle group $\mathbf{J}_K$, idèle class group C_K, and connected component of the idèle class group D_K.

Exercise 6.4.

(a) Prove: $C_{\mathbb{Q}} \cong \mathbb{R} \times \widehat{\mathbb{Z}}^*$ and $D_{\mathbb{Q}} \cong \mathbb{R}$.
(b) Give similar descriptions of C_K and D_K for $K = \mathbb{Q}(i)$ and for $K = \mathbb{Q}(\sqrt{2})$.

Exercise 6.5. Denote by $\widehat{\mathcal{O}}$ the profinite completion of the additive group of $\mathcal{O}$.

(a) Prove that the ring multiplication map $\mathcal{O}\times\mathcal{O} \to \mathcal{O}$ has a unique continuous extension to a map $\widehat{\mathcal{O}} \times \widehat{\mathcal{O}} \to \widehat{\mathcal{O}}$ that makes $\widehat{\mathcal{O}}$ into a topological ring.
(b) Prove that there are isomorphisms $\widehat{\mathcal{O}} \cong \prod_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}$ and $\widehat{\mathcal{O}}^* \cong \prod_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}^*$ of topological rings and topological groups, respectively; in both cases, $\mathfrak{p}$ ranges over the set of finite primes of K, and $\mathcal{O}_{\mathfrak{p}}$ denotes the completion of $\mathcal{O}$ at $\mathfrak{p}$.

Exercise 6.6. Let μ be the group of all roots of unity in K, and write $w = \#\mu$.

(a) Prove that the set of finite primes $\mathfrak{p}$ of K for which the natural group homomorphism $\mu \to (\mathcal{O}/\mathfrak{p})^*$ is split injective has a density, and that this density equals $\varphi(w)/w$, with φ denoting the Euler function. (A homomorphism $f\colon A \to B$ of abelian groups is said to be *split injective* if there is a group homomorphism $g\colon B \to A$ for which gf is the identity on A.)
(b) Let m be a positive integer, and let $\zeta \in \mu$ be such that for all but finitely many finite primes $\mathfrak{p}$ of K the image of ζ in $\mathcal{O}/\mathfrak{p}$ is an mth power in $\mathcal{O}/\mathfrak{p}$. Prove that ζ is an mth power in μ.

Exercise 6.7.

(a) Let m be a positive integer, and let w be as in the previous exercise. Let $a \in \mathcal{O}$ be such that for all but finitely many finite primes $\mathfrak{p}$ of K the image of a in $\mathcal{O}/\mathfrak{p}$ is an mwth power in $\mathcal{O}/\mathfrak{p}$. Prove that a is an mth power in $\mathcal{O}$. (*Hint*: use Schinzel's theorem.)
(b) Prove that (16 mod p) is an 8th power in $\mathbb{F}_p$ for all primes p, but that 16 is not an 8th power in $\mathbb{Z}$.

Exercise 6.8. Prove that the closure of $\mathcal{O}^*$ in $\widehat{\mathcal{O}}^*$ may be identified with the profinite completion $\widehat{\mathcal{O}^*}$ of $\mathcal{O}^*$.

Exercise 6.9. Let μ be the group of all roots of unity in K, and for a prime $\mathfrak{p}$ of K write $U_{\mathfrak{p}} = \{x \in K_{\mathfrak{p}}^* : |x|_{\mathfrak{p}} = 1\}$. Denote by Pic_K the Arakelov class group of K. Prove that there is an exact sequence

$$1 \to \mu \to \prod_{\mathfrak{p}} U_{\mathfrak{p}} \to C_K \to \mathrm{Pic}_K \to 1$$

of abelian groups, with continuous group homomorphisms; here the product ranges over all primes $\mathfrak{p}$ of K.

Exercise 6.10. Let J_K^0 be the kernel of the group homomorphism $J_K \to \mathbb{R}^*$ sending $(x_{\mathfrak{p}})_{\mathfrak{p}}$ to $\prod_{\mathfrak{p}} |x_{\mathfrak{p}}|_{\mathfrak{p}}$. Write $C_K^0 = J_K^0/K^*$ and $D_K^0 = D_K \cap C_K^0$. Prove that there are isomorphisms

$$J_K \cong J_K^0 \times \mathbb{R}, \qquad C_K \cong C_K^0 \times \mathbb{R}, \qquad D_K \cong D_K^0 \times \mathbb{R}$$

of topological groups.

Exercise 6.11.

(a) For a real prime $\mathfrak{p}$ of K, write $K^*_{\mathfrak{p}>0}$ for the multiplicative group of positive elements of $K_\mathfrak{p}$, and write $H = \prod_{\mathfrak{p} \text{ complex}} K^*_\mathfrak{p} \times \prod_{\mathfrak{p} \text{ real}} K^*_{\mathfrak{p}>0}$. For $u \in \mathcal{O}^*$, let $u' \in H$ be obtained from the natural image of u in $\prod_{\mathfrak{p} \text{ infinite}} K^*_\mathfrak{p}$ by replacing the coordinates at the real primes by their absolute values. Embed $\mathcal{O}^*$ into $H \times \widehat{\mathcal{O}^*}$ by identifying $u \in \mathcal{O}^*$ with (u', u). Prove:

$$D_K \cong (H \times \widehat{\mathcal{O}^*})/\mathcal{O}^*$$

as topological groups.

(b) Prove that there is a split exact sequence of topological groups

$$1 \to \prod_{\mathfrak{p} \text{ complex}} U_\mathfrak{p} \to D_K^0 \to \mathcal{O}^* \otimes_\mathbb{Z} \mathbf{S} \to 1,$$

with $U_\mathfrak{p}$ as in Exercise 6.9 and D_K^0 as in Exercise 6.10. How should $\mathcal{O}^* \otimes_\mathbb{Z} \mathbf{S}$ be topologized?

(c) Let r be the number of real primes of K and s the number of complex primes. Prove that D_K is, as a topological group, isomorphic to $\mathbf{S}^{r+s-1} \times (\mathbb{R}/\mathbb{Z})^s \times \mathbb{R}$.

Mathematisch Instituut,
Universiteit Leiden,
Postbus 9512,
2300 RA Leiden,
The Netherlands
E-mail address: `hwl@math.leidenuniv.nl`