THE IDELIC APPROACH TO CLASS GROUPS AND UNIT GROUPS

PETE L. CLARK

Contents

7.1. **Rings of S-integers.**

Notation: Despite some misgivings, we introduce the following notation. For a global field K, we let Σ_K denote the set of all places of K, i.e., equivalence classes of nontrivial norms on K. (Recall that at this point we have associated a canonical normalized Artin absolute value to each place in K.) Further we write Σ_K^{NA} for the subset of non-Archimeden places of K, and let Σ_K^{Arch} denote the subset of Archimedean places of K, which is nonempty iff K is a number field.

Now let $S \subset \Sigma_K$ be a finite set such that $S \supset \Sigma_K^{\mathrm{Arch}}$. We define the ring R_S of **S-integers** of K to be the set of $x \in K$ such that $v(x) \geq 0$ for all $v \in \Sigma_K^{\mathrm{NA}} \setminus S$.

Exercise 7.1:
a) If K is a function field and $S = \emptyset$, show that R_S is equal to the maximal finite subfield of K (or, in other words, the "algebraic closure of $\mathbb{F}_p$ in K".)
b) Show that if $S \neq \emptyset$, then R_S is a Dedekind domain that is not a field.

Exercise 7.2: Suppose that $S \subset T$ are finite subsets of Σ_K with $\Sigma_K^{\mathrm{Arch}} \subset S$.
a) Show that $R_S \subset R_T$.
b)* Show that R_T is a localization of R_S. (The special case that R_S is a PID is straightforward. In order to do the general case, it may be necessary to use the finiteness of the ideal class group of R_S, coming up shortly.)

7.2. **Finiteness of the S-class groups.**

Because R_S is a Dedekind domain, it has an interesting invariant attached to it: its ideal class group $\mathrm{Cl}(R_S)$. This is the free abelian group generated by the nonzero prime ideals, which we may view as being in correspondence with the non-Archimedean places v of K. Inside $\mathrm{Frac}(R_S)$ we have the subgroup of principal fractional ideals (f) for $f \in K^\times$. Explicitly, we view (f) as an element of $\bigoplus_v \mathbb{Z}[v]$ by sending f to the sequence $\{v(f)\}$, which has all but finitely many elements 0. Let us write this subgroup as $\operatorname{Prin}(K)$. By definition, the **ideal class group** $\operatorname{Cl}(R_S)$ of R_S is the quotient $\operatorname{Frac}(R_S)/\operatorname{Prin}(R_S)$. To summarize, we have exact sequences

$$1 \to R_S^\times \to K^\times \to \operatorname{Prin}(R_S) \to 1,$$

$$1 \to \operatorname{Prin}(R_S) \to \operatorname{Frac}(R_S) \to \operatorname{Cl}(R_S) \to 1.$$

Note that this discussion makes perfect sense for an arbitrary Dedekind domain R. Indeed, a celebrated theorem of L. Claborn asserts that for any abelian group A whatsoever, there exists a Dedekind domain R such that $\operatorname{Cl}(R) \cong A$. However, in the arithmetic case, we have the following important result, a generalization of the second of the three fundamental finiteness theorems in classical algebraic number theory.

Theorem 1. *Let K be a global field and $S \subset \Sigma_K$ a finite set containing all the Archimedean places. Then the ideal class group $\operatorname{Cl}(R_S) = \operatorname{Frac}(K)/\operatorname{Prin}(K)$ is a finite abelian group.*

Before proving the theorem, we pause for some remarks. First, especially in the number field case, the group $\operatorname{Cl}(R_S)$ is often called the **S-class group** of the number field K. As far as the finiteness goes, there is really not any more content here than in the classical case of the finiteness of the full ring of integers $\mathbb{Z}_K$ (i.e., corresponding to the case $S = \Sigma_K^{\mathrm{Arch}}$).

Let me explain this in more algebraic terms. Let R be a Dedekind domain with fraction field K – we assume $R \neq K$ – and let S be an **overring** of R, i.e., $R \subset S \subsetneq K$. Let Σ_R be the set of nonzero prime ideals of R. Then for each $\mathfrak{p} \in R$, the localization $R_\mathfrak{p}$ is a DVR with fraction field K – these are precisely the maximal overrings of R. Indeed $R = \mathfrak{p} \in \mathfrak{t}_{\mathfrak{R}} R_\mathfrak{p}$. More generally, for any nonempty subset $W \subset \Sigma_R$, we can build an overring R_W of R by taking $R_W = \bigcap_{\mathfrak{p} \in W} R_\mathfrak{p}$. It is not hard to show that R_W is again a Dedekind domain. Rather remarkably, every overring S of R is of the form R_W for some W, namely for the set of primes $\mathfrak{p}$ such that $\mathfrak{p}S \neq S$. On the other hand, although the definition of R_W is certainly "local in nature", it need not be a localization at a multiplicative subset in the precise technical sense. Indeed, there is the following beautiful result: every overring of a Dedekind domain R is a localization iff the ideal class group $\operatorname{Cl}(R)$ is a torsion abelian group. Thus one of the consequences of Theorem applied to the special case $S = \Sigma_K^{\mathrm{Arch}}$ is that every overring R_T of $R_S = \mathbb{Z}_K$ is actually the localization at a multiplicative subset (Exercise 7.2).

On the other hand, the following is a much easier exercise.

Exercise 7.3: Let R be a Dedekind domain and let $S = R_W$ be an overring of R. The map $\iota : R \hookrightarrow S$ induces a map on ideal class groups, $\iota_* : \operatorname{Cl}(R) \to \operatorname{Cl}(S)$, simply by pushing forward ideals: $I \mapsto IS$ (just note that principal ideals push forward to principal ideals). Show that ι_* is surjective. In particular, if $\operatorname{Cl}(R)$ is finite, then so is $\operatorname{Cl}(S)$.

Now we give the **proof** of Theorem 1 in the number field case: the key is that we have group homomorphism $V : \mathbb{I}_K \to \operatorname{Frac}(K)$ sending the idele (x_v) to the sequence of its valuations $(v(x_v))$ (at non-Archimedean places) which, by the definition of the ideles, is zero except at finitely many places. Certainly V is surjective:

given a finitely nonzero vector of integers n_v, for each v with $n_v \neq 0$, simply choose an element $x_v \in K_v^\times$ with $v(x_v) = n_v$; for each v with $n_v = 1$, put $x_v = 1$. Clearly a principal idele (f) gets sent to the valuation vector of the principal fractional ideal (f), so V passes to a homomorphism $C(K) \to \mathrm{Cl}(R_S)$. Because we are in the number field case and the image under V does not depend on the Archimedean places, V is also surjective when restricted to norm one ideles (because if we start with an idele with norm N, then we can modify it to have norm $\frac{1}{N}$ in exactly one of the Archimedean places). Therefore we get $\mathrm{Cl}(R_S)$ is a quotient of the compact group $\mathrm{Cl}^1(K)$. On the other hand, the kernel of V contains the open subgroup $\prod_v R_v^\times$, so the image is discrete in the natural (quotient space) topology. Thus in the quotient topology, $\mathrm{Cl}(R_S)$ is both discrete and compact, and therefore finite!

What about the function field case? There is clearly one aspect in the proof that must be changed: we do not have any Archimedean places to use to "correct" the global norm. So let's think through what changes. There are two cases: in the first case $S = \emptyset$, but as in Exercise 6.13, this is a trivial case: then $R_S = \mathbb{F}_q$ is a finite field, so of course its class group is equal to zero. Otherwise, S is nonempty. As we saw above, it suffices to consider the case in which S contains exactly one place v, because every other class group will be surjected onto by one of these S-class groups. Consider the norm map on $K_v^\times$: its image is $q^{\mathbb{Z}}$, where $q = p^a\mathcal{R}_v/\Updownarrow_v$ is the cardinality of the residue field at v. The image of the global norm map could, *a priori*, be as large as $p^{\mathbb{Z}}$. Thus we can correct at v to make the norm lie in a subgroup of index dividing f of the image of the global norm map. In other words, the homomorphism $C^0(K) \to \mathrm{Cl}(R_S)$ need not be surjective, but its cokernel has size dividing f. Ths is certainly enough to deduce the finiteness of $\mathrm{Cl}(R_S)$ in the function field case!

I would like also to discuss a more geometric approach which shows finiteness of a related group $\mathrm{Cl}^0(K)$. Let K be a finite separable field extension of $\mathbb{F}_p(t)$. We define the divisor group $\mathrm{Div}(K)$ to be the free abelian group on the places of K. Note that this is much the same as in the number field case, except we have not removed the Archimedean places because we do not have any. Again, we have a notion of principal divisors: for any $f \in K^\times$, we send f to its valuation vector $(v(f))$. And we may define the class group $\mathrm{Cl}(K) = \mathrm{Div}(K)/\mathrm{Prin}(K)$ exactly as above.

However, there is something different in the function field case: the class group $\mathrm{Cl}(K)$ will in fact be *infinite* in all cases for a rather shallow reason: there exists a numerical invariant of divisors on K, the **degree**, which takes arbitrarily large values, but any principal divisor has degree 0.

For example, consider $K = \mathbb{F}_p(t)$. For each $n \in \mathbb{Z}^+$ let $D_n = n[\infty]$, where $[\infty]$ is the point at infinity. I claim that the D_n's are all distinct elements of $\mathrm{Cl}(K)$, which is therefore infinite. To see this, suppose not. Then there exist $m < n$ and a nonzero rational function $f \in \mathbb{F}_p(t)$ such that $f = (n-m)[\infty]$. But a rational function which is integral away from the place at ∞ is a polynomial, whereas the fact that $v_\infty(f) = n - m > 0$ means that f has negative degree: contradiction!

Those who have studied even a little algebraic geometry or Riemann surface theory will know a more convincing explanation: for any $f \in K^{\times}$, the principal divisor (f) has, in a natural sense, exactly as many zeros as it has poles. More precisely it has **degree zero**, whereas there are divisors on $\mathbb{F}_p(t)$ of any integer degree, so $\mathrm{Cl}(\mathbb{F}_p(t))$ must contain a copy of $\mathbb{Z}$.

Our task now is to define the degree map. To preserve the analogy with Riemann surface theory, we might as well work in a little more generality: in place of $\mathbb{F}_p$ we will take an arbitary field k as our constant field, and we will let K be a finite, separable extension of $k(t)$. For each place v of K which is trivial on k, the residue field $k_v = R_v/\mathfrak{m}_v$ is a finite extension of k; let f_v be the residual degree. Then for an element $D = \sum n_v[v]$ of the divisor group, we define its degree

$$\deg(D) = \sum_v n_v f_v \in \mathbb{Z}.$$

As usual, we note that this sum is a finite sum because by definition $n_v = 0$ for all but finitely many places v.

Proposition 2. *For any $f \in K^{\times}$, $\deg(f) = 0$.*

Proof. For the case of a general ground field k, see e.g. Dino's book *Invitation to Arithmetric Geometry.* The basic idea is as follows: a nonconstant function $f \in K$ is equivalent to finite map of algebraic curves $\pi : C \to \mathbb{P}^1$. For any closed point $x \in \mathbb{P}^1$, one can define the preimage of $\pi^*(x)$: as a divisor it is $\sum_{y \to x} e(y)[y]$, where valuation theoretically y runs through the places of K lying over the place corresponding to x on $\mathbb{P}^1$ and $e(y)$ and $f(y)$ are the usual ramification index. Thus by the fundamental degree equality (because $K/k(t)$ need not be separable, some argument is required to show that this is applicable here) each of these degrees is equal to $[K : k(t)]$, and in particular they are all equal to each other. But the divisor of f is equal to $\pi^*(0) - \pi^*(\infty)$, so it has degree 0.

Note however that in case the residue field k is finite, this relation is precisely the product formula! □

If we define $I(K)$ to be the gcd of all degrees of divisors v on K, then a moment's thought shows that $I(K)$ is a positive integer and $\deg(\mathrm{Div}(K)) = I(K)\mathbb{Z}$. Therefore the proposition implies that $\mathrm{Cl}(K)$ contains a subgroup isomorphic to $I(K)\mathbb{Z}cong\mathbb{Z}$, so it is always infinite!

Remark: In fact, if k is a finite field, we have $I(K) = 1$ always, i.e., the degree map is surjective. This was first proved by F.K. Schmidt around 1915 using (what would later be called!) the Hasse-Weil zeta function. For those who know some algebraic geometry, it should not be hard to use the Riemann hypothesis for curves over finite fields (proven by Weil) to show that for any smooth, projective curve $X_{/\mathbb{F}_q}$, for all sufficiently large n, X has degree n rational points. In particular, for some n it has a degree n rational point and also a degree $n+1$ rational point, and hence it has a divisor of degree 1. (But we will not use this result in the sequel.)

Because of Proposition 2, we may define $\mathrm{Div}^0(K) = \mathrm{Ker}(\deg)$, the kernel of the degree map and then $\mathrm{Prin}(K) \subset \mathrm{Div}^0(K)$. Thus finally we may define $\mathrm{Cl}^0(K) = \mathrm{Div}^0(K)/\mathrm{Prin}(K)$, the degree 0 divisor class group.

Theorem 3. *For any finite separable extension $K/\mathbb{F}_p(t)$, the degree zero divisor class group $\operatorname{Cl}^0(K)$ is a finite abelian group.*

Proof. If we look back at the proof of the number field case, we see immediately what needs to be modified: because we do not have Archimedean places, it is not clear that the norm one idele class group surjects onto $\operatorname{Cl}(K)$. However, let $D = \sum_v n_v[v] \in \operatorname{Div}(K)$. We define an idele x_D as follows: for each v with $n_v \neq 0$, let $x_v \in K_v^\times$ be such that $v(x_v) = n_v$; as above, for every place v with $n_v = 0$, we define $x_v = 1$. Then $|x| = p^{\sum f_v n_v}$, whereas $\deg D = \sum f_v n_v$. Thus $\deg(D) = 0 \iff |x_D| = 1$. It follows that $C^1(K)$ surjects onto $\operatorname{Cl}^0(K)$, and the remainder of the proof proceeds as above. □

Theorem 4. *(Rosen) Let $C^\circ = C \setminus S$ be a nonsingular, geometrically integral affine curve over a field k. Let $D^0(S)$ be the subgroup of $\operatorname{Div}^0(C)$ of degree 0 divisors supported on S, and let $P^0(S) = \operatorname{Prin}(K) \cap D^0(S)$ be the principal divisors supported on S. Let d be the least positive degree of a divisor supported on S (so $d = 1$ iff S contains a k-rational point), and let $I(C)$ be the least positive degree of a divisor on C. Then there exists an exact sequence*

$$0 \to D^0(S)/P^0(S) \to \operatorname{Pic}^0(C) \to \operatorname{Pic}(C^\circ) \to C(d/i) \to 0,$$

where $C(d/i)$ is a finite cyclic group of order d/i.

Proof. □

Exercise: Suppose that S consists of a single k-rational point of S. Show that the exact sequence reduces to an isomorphism $\operatorname{Pic}^0(C) \to \operatorname{Pic}^(C^\circ)$. Now prove this directly.

7.3. Structure of the S-unit groups.

With K and S as above, we now wish to study the structure of the unit group $U_S = R_S^\times$. Again, in the number field case this is often called the **S-unit group**. We will give a generalization of the celebrated Dirichlet unit theorem to S-class groups of either number fields or function fields.

Lemma 5. *Let $0 < c < C$. Then the set $\mathcal{S} = \mathcal{S}(S, c, C)$ of S-units x with $c \leq |x|_v \leq C$ for all $v \in S$ is finite.*

Proof. The set W of ideles $x = (x_v)$ with $|x_v|_v = 1$ for all $v \notin S$ and $c \leq |x_v|_v \leq C$ for all $s \in S$ is visibly compact. We have $\mathcal{S} = W \cap K^\times$, so $\mathcal{S}$ is compact and discrete, thus finite. □

Lemma 6. *The set of elements $x \in K$ such that $|x|_v = 1$ for all places v of K is precisely the group of roots of unity of K, which is a finite abelian group.*

Proof. Let $\mu(K)$ be the group of roots of unity of K and let $\mathcal{T}$ be the subgroup of elements of $K^\times$ which have norm one at every place v of K. By Exercise 1.3a), $\mu(K) \subset \mathcal{T}$. Applying Lemma 5 (with any fnite set S containing Σ_K^{Arch}) and $c = C = 1$ shows that $\mathcal{T}$ is finite. In particular, each element of $\mathcal{T}$ has finite order, so $\mathcal{T} \subset \mu(K)$. Thus $\mathcal{T} = \mu(K)$ is finite. □

Remark: In fact, it follows from our work on locally compact fields that in any locally compact field except $\mathbb{C}$, the group of roots of unity is finite. This is obvious for $\mathbb{R}$. For a non-Archimedean field of residue characteristic p, the case of roots of unity of order prime to p is Proposition X.X. For p-adic fields, that the group of roots of unity of p-power is finite follows from the fact that for all n, the Eisenstein criterion can be used to show that the cyclotomic polynomial $\Phi_{p^n}(t)$ is irreducible over $\mathbb{Q}_p$ and generates a totally ramified extension. For local fields of positive characteristic, there is nothing to worry about because there are no p-power roots of unity even over the algebraic closure!

Lemma 7. *Let $r, s \in \mathbb{Z}$ with $s \geq r \geq 0$, and let $G = \mathbb{R}^r \times \mathbb{Z}^{s+1-r}$. Let $\lambda : G \rightarrow (\mathbb{R}, +)$ be a nontrivial homomorphism of topological groups. Moreover:*
• *When $r = 0$, we assume that $\lambda(\mathbb{Z}^{s+1-r}) \cong (\mathbb{Z}, +)$*
•, *When $r > 0$, we assume that $\lambda|_{\mathbb{R}^r} \cong (\mathbb{R}, +)$.*
Let $\mathcal{K} = \operatorname{Ker}(\lambda)$ and let Γ be any discrete, cocompact subgroup of $\mathcal{K}$. Then $\Gamma \cong \mathbb{Z}^s$.

Proof. Write $\lambda = \lambda_1 + \lambda_2$, where $\lambda_1 = \lambda|_{\mathbb{R}^r}$ and $\lambda_2 = \lambda|_{\mathbb{Z}^{s+1-r}}$.
Case 1: $r = 0$. Then $\lambda_1 = 0$, so (by assumption!) $\mathbb{Z}^{s+1}/\mathcal{K} \cong \mathbb{Z}$ and thus $\mathcal{K} \cong \mathbb{Z}^s$. In this case every subgroup of $\mathcal{K}$ is discrete and is cocompact iff it has maximal rank, so indeed $\Gamma \cong \mathbb{Z}^s$.
Case 2: $\lambda_2 = 0$. Then $\mathcal{K} = \ker(\lambda_1) \oplus \mathbb{Z}^{s+1-r} \cong \mathbb{R}^{r-1} \oplus \mathbb{Z}^{s+1-r}$. A discrete cocompact subgroup of this is obtained by choosing a rank $r-1$ lattice of $\mathbb{R}^{r-1}$ together with $\mathbb{Z}^{s+1-r}$, hence is isomorphic to $\mathbb{Z}^s$.
Case 3: Finally, we assume that λ_1 and λ_2 are both nontrivial. Then the image of λ_2 is isomorphic to $\mathbb{Z}^t$ for some $1 \leq t \leq s+1-r$. Then

$$K_0 := \{(x, y) \in G \mid \lambda_1(x) = \lambda_2(x) = 0\}$$

is a subgroup of $\mathcal{K}$ and $\mathcal{K}/K_0 \cong \mathbb{Z}^t$. Explicitly, $K_0 \cong \mathbb{R}^{r-1} \times \mathbb{Z}^{s+1-r-t}$, and thus $\mathcal{K} \cong \mathbb{R}^{r-1} \times \mathbb{Z}^{s-r+1}$, so again a discrete cocompact subgroup must have rank s. □

We now give the following attractive generalization of Dirichlet's Unit Theorem, the third basic finiteness theorem in algebraic number theory.

Theorem 8. *Let K be a global field, S a finite nonempty set of places of K containing all Archimedean places (if any). Let U_S be the group of S-units. Then U_S is a finitely generated abelian group. More precisely, its torsion subgroup is the finite group of roots of unity in K, and its rank is $\#S - 1$.*

Proof. (Ramakrishnan-Valenza) Step 1: For $v \in \Sigma_K$, let $C_v = \{x \in K_v \mid |x|_v = 1\}$. This is a compact subgroup of $K_v^\times$. Therefore, by Tychonoff, $C := \prod_v C_v$ is a compact subgroup of $I_K(S)$, the "adelic circle group". We have a short exact sequence of topological groups

$$1 \rightarrow C \rightarrow \mathbb{I}_K(S) \rightarrow \prod_{v \in S} K_v^\times / C_v \rightarrow 1.$$

Now $K_v^\times / C_v$ is isomorphic to $\mathbb{R}^{>0} \cong (\mathbb{R}, +)$ if v is Archimedean and isomorphic to $\mathbb{Z}$ if v is non-Archimedean. If we put $r = \#S$, $r_1 = \#(S \cap \Sigma_K^{\text{Arch}})$, $r_2 = s - r_1$, then we may rewrite the exact sequence as

$$1 \rightarrow C \rightarrow \mathbb{I}_K(S) \rightarrow \mathbb{R}^{r_1} \oplus \mathbb{Z}^{r_2} \rightarrow 0.$$

We wish to first restrict this sequence of norm one S-ideles and then further to elements of $K^\times \cap \mathbb{I}_K^1(S)$.

Step 2: Consider the norm map restricted to the subgroup of S-ideles: $|| \ || : \mathbb{I}_K(S) \rightarrow \mathbb{R}^{>0}$. The circle group C lies in the kernel of λ, so the norm map factors through a homomorphism $\mathbb{R}^{r_1} \oplus \mathbb{Z}^{r_2} \to \mathbb{R}^{>0} \overset{\log}{\to} (\mathbb{R}, +)$, which we will call λ. We claim that λ satisfies the hypotheses of Lemma 7 with $r_1 = r$, $r_2 = s + 1 - r$. Indeed, if $r_1 = 0$ then we are in the function field case, so the image of the norm map is contained in $p^{\mathbb{Z}}$ hence is a rank one subgroup of $\mathbb{R}^{>0}$, whereas if $r_1 > 0$ then we are in the number field case and the norm map is surjective. It follows that any discrete, cocompact subgroup of $\mathcal{K} = \ker(\lambda)$ is isomorphic to $\mathbb{Z}^s \cong \mathbb{Z}^{\#S-1}$.

Step 3: Now consider the S-unit group $R_S^\times = K \cap \mathbb{I}_S(K)$. By Lemma 6, $R_S^\times \cap C = \mu(K)$, the finite group of roots of unity in K. Therefore we may define Γ to be the image of $R_S^\times$ in $G \cong \mathbb{R}^{r_1} \oplus \mathbb{Z}^{r_2}$; note that $\Gamma \cong R_S^\times/\mu(K)$. Moreover, since $K^\times$ is discrete and cocompact in $\mathbb{I}_K^1$ and $\mathbb{I}_K(S)$ is closed in $\mathbb{I}_K$, $R_S^\times = K^\times \cap \mathbb{I}_K(S)$ is discrete and cocompact in $\mathbb{I}_K^1(S) = \mathbb{I}_K^1 \cap \mathbb{I}_K(S)$. Therefore we may apply Lemma 7 to $\Gamma := R_S^\times/\mu(K)$, getting the desired result. □