Math 129: Algebraic Number Theory
Lectures 23–24: Strong Approximation, Ideles, and Ideals

William Stein (based closely on Cassels's *Global Fields* article in Cassels-Fröhlich)

Tuesday, May 4, 2004

We first prove a technical lemma and corollary, then use them to deduce the strong approximation theorem, which is an extreme generalization of the Chinese Remainder Theorem; it asserts that K^+ is dense in the analogue of the adeles with one valuation removed.

Next we introduce the ideles $\mathbb{I}_K$, and relate ideles to ideals, and use what we've done so far to give an alternative interpretation of class groups and their finiteness, thus linking the adelic point of view with the classical point of view of the first part of this course.

14 The Adele Ring (continued)

The proof of Lemma 14.1 below will use in a crucial way the normalized Haar measure on $\mathbb{A}_K$ and the induced measure on the compact quotient $\mathbb{A}_K^+/K^+$. Since I am not formally developing Haar measure on locally compact groups, and since I didn't explain induced measures on quotients well in the last lecture, hopefully the following discussion will clarify what is going on.

The real numbers $\mathbf{R}^+$ under addition is a locally compact topological group. Normalized Haar measure μ has the property that $\mu([a,b]) = b - a$, where $a \leq b$ are real numbers and $[a,b]$ is the closed interval from a to b. The subset $\mathbf{Z}^+$ of $\mathbf{R}^+$ is discrete, and the quotient $S^1 = \mathbf{R}^+/\mathbf{Z}^+$ is a compact topological group, which thus has a Haar measure. Let $\overline{\mu}$ be the Haar measure on S^1 normalized so that the natural quotient $\pi : \mathbf{R}^+ \to S^1$ preserves the measure, in the sense that if $X \subset \mathbf{R}^+$ is a measurable set that maps injectively into S^1, then $\mu(X) = \overline{\mu}(\pi(X))$. This determine $\overline{\mu}$ and we have $\overline{\mu}(S^1) = 1$ since $X = [0,1)$ is a measurable set that maps bijectively onto S^1 and has measure 1. The situation for the map $\mathbb{A}_K \to \mathbb{A}_K/K^+$ is pretty much the same.

It is a general fact that a Haar measure of a compact topological group G is finite. If U is an open set with finite measure α, then the translates of U are also open sets with the same measure α (by definition of Haar measure). The translates certainly cover G, and G is compact, so there is a finite subcover. The measure of G is then at most the sum of the measures of those finitely many translates of U, hence finite.

Lemma 14.1. *There is a constant $C > 0$ that depends only on the global field K with the following property:*

Whenever $\mathbf{x} = \{x_v\}_v \in \mathbb{A}_K$ is such that

$$\prod_v |x_v|_v > C, \tag{14.1}$$

then there is a nonzero principal adele $a \in K \subset \mathbb{A}_K$ such that

$$|a|_v \le |x_v|_v \qquad \text{for all } v.$$

Proof. This proof is modelled on Blichfeldt's proof of Minkowski's Theorem in the Geometry of Numbers, and works in quite general circumstances.

First we show that (14.1) implies that $|x_v|_v = 1$ for almost all v. Because $\mathbf{x}$ is an adele, we have $|x_v|_v \le 1$ for almost all v. If $|x_v|_v < 1$ for infinitely many v, then the product in (14.1) would have to be 0. (We prove this only when K is a finite extension of $\mathbf{Q}$.) Excluding archimedean valuations, this is because the normalized valuation $|x_v|_v = |\text{Norm}(x_v)|_p$, which if less than 1 is necessarily $\le 1/p$. Any infinite product of numbers $1/p_i$ must be 0, whenever p_i is a sequence of primes.

Let c_0 be the Haar measure of $\mathbb{A}_K^+/K^+$ induced from normalized Haar measure on $\mathbb{A}_K^+$, and let c_1 be the Haar measure of the set of $\mathbf{y} = \{y_v\}_v \in \mathbb{A}_K^+$ that satisfy

$$\begin{aligned} |y_v|_v &\le \frac{1}{2} && \text{if } v \text{ is archimedean,} \\ |y_v|_v &\le 1 && \text{if } v \text{ is non-archimedean.} \end{aligned}$$

(As we will see, any positive real number $\le 1/2$ would suffice in the definition of c_1 above. For example, in Cassels's article he uses the mysterious $1/10$.)

Then $0 < c_0 < \infty$ since $\mathbb{A}_K/K^+$ is compact, and $0 < c_1 < \infty$ because the number of archimedean valuations v is finite. We show that

$$C = \frac{c_0}{c_1}$$

will do. Thus suppose $\mathbf{x}$ is as in (14.1).

The set T of $\mathbf{t} = \{t_v\}_v \in \mathbb{A}_K^+$ such that

$$\begin{aligned} |t_v|_v &\le \frac{1}{2}\,|x_v|_v && \text{if } v \text{ is archimedean,} \\ |t_v|_v &\le |x_v|_v && \text{if } v \text{ is non-archimedean} \end{aligned}$$

has measure

$$c_1 \cdot \prod_v |x_v|_v > c_1 \cdot C = c_0.$$

Hence in the quotient map $\mathbb{A}_K^+ \to \mathbb{A}_K^+/K^+$ there must be a pair of distinct points of T that have the same image in $\mathbb{A}_K^+/K^+$, say

$$\mathbf{t}' = \{t'_v\}_v \in T \quad \text{and} \quad \mathbf{t}'' = \{t''_v\}_v \in T$$

and

$$a = \mathbf{t}' - \mathbf{t}'' \in K^+$$

is nonzero. Then

$$|a|_v = |t'_v - t''_v|_v \leq \begin{cases} |t'_v| + |t''_v| \leq 2 \cdot \frac{1}{2} |x_v|_v \leq |x_v|_v & \text{if } v \text{ is archimedean, or} \\ \max(|t'_v|, |t''_v|) \leq |x_v|_v & \text{if } v \text{ is non-archimedean,} \end{cases}$$

for all v, as required. □

Corollary 14.2. *Let v_0 be a normalized valuation and let $\delta_v > 0$ be given for all $v \neq v_0$ with $\delta_v = 1$ for almost all v. Then there is a nonzero $a \in K$ with*

$$|a|_v \leq \delta_v \qquad (\textit{all } v \neq v_0).$$

Proof. This is just a degenerate case of Lemma 14.1. Choose $x_v \in K_v$ with $0 < |x_v|_v \leq \delta_v$ and $|x_v|_v = 1$ if $\delta_v = 1$. We can then choose $x_{v_0} \in K_{v_0}$ so that

$$\prod_{\text{all } v \text{ including } v_0} |x_v|_v > C.$$

Then Lemma 14.1 does what is required. □

Remark 14.3. The character group of the locally compact group $\mathbb{A}_K^+$ is isomorphic to $\mathbb{A}_K^+$ and K^+ plays a special role. See Chapter XV (Tate's thesis), Lang *Algebraic Numbers* (Addison-Wesley), Weil *Adeles and Algebraic Groups* (Princeton lecture notes) and Godement's Bourbaki seminars 171 and 176. This duality lies behind the functional equation of ζ and L-functions. Iwasawa has shown (*Annals of Math.* **57** (1953), 331–356) that the rings of adeles are characterized by certain general topologico-algebraic properties.

15 The Strong Approximation Theorem

We proved before that K is discrete in $\mathbb{A}_K$. If one valuation is removed, the situation is much different.

Theorem 15.1 (Strong Approximation). *Let v_0 be any normalized nontrivial valuation of the global field K. Let $\mathbb{A}_{K,v_0}$ be the restricted topological product of the K_v with respect to the $\mathcal{O}_v$, where v runs through all normalized valuations $v \neq v_0$. Then K is dense in $\mathbb{A}_{K,v_0}$.*

Proof. This proof was suggested by Prof. Kneser at the Cassels-Frohlich conference.

Recall that if $\mathbf{x} = \{x_v\}_v \in \mathbb{A}_{K,v_0}$ then a basis of open sets about $\mathbf{x}$ is the collection of products

$$\prod_{v \in S} B(x_v, \varepsilon_v) \times \prod_{v \notin S,\ v \neq v_0} \mathcal{O}_v,$$

where $B(x_v, \varepsilon_v)$ is an open ball in K_v about x_v, and S runs through finite sets of normalized valuations (not including v_0). Thus denseness of K in $\mathbb{A}_{K,v_0}$ is equivalent to the following statement about elements. Suppose we are given (i) a finite set S of valuations $v \neq v_0$, (ii) elements $x_v \in K_v$ for all $v \in S$, and (iii) an $\varepsilon > 0$. Then there is an element $b \in K$ such that $|b - x_v|_v < \varepsilon$ for all $v \in S$ and $|b|_v \leq 1$ for all $v \notin S$ with $v \neq v_0$.

By the corollary to our proof that $\mathbb{A}_K^+/K^+$ is compact, there is a $W \subset \mathbb{A}_K$ that is defined by inequalities of the form $|y_v|_v \leq \delta_v$ (where $\delta_v = 1$ for almost all v) such that ever $\mathbf{z} \in \mathbb{A}_K$ is of the form

$$\mathbf{z} = \mathbf{y} + c, \qquad \mathbf{y} \in W, \quad c \in K. \tag{15.1}$$

By Corollary 14.2, there is a nonzero $a \in K$ such that

$$\begin{aligned} |a|_v &< \frac{1}{\delta_v} \cdot \varepsilon && \text{for } v \in S, \\ |a|_v &\leq \frac{1}{\delta_v} && \text{for } v \notin S,\ v \neq v_0. \end{aligned}$$

Hence on putting $\mathbf{z} = \frac{1}{a} \cdot \mathbf{x}$ in (15.1) and multiplying by a, we see that every $\mathbf{x} \in \mathbb{A}_K$ is of the shape

$$\mathbf{x} = \mathbf{w} + b, \qquad \mathbf{w} \in a \cdot W, \quad b \in K,$$

where $a \cdot W$ is the set of $a\mathbf{y}$ for $\mathbf{y} \in W$. If now we let $\mathbf{x}$ have components the given x_v at $v \in S$, and (say) 0 elsewhere, then $b = \mathbf{x} - \mathbf{w}$ has the properties required. □

Remark 15.2. The proof gives a quantitative form of the theorem (i.e., with a bound for $|b|_{v_0}$). For an alternative approach, see K. Mahler: Inequalities for ideal bases, *J. Australian Math. Soc.* **4** (1964), 425–448.

16 The Idele Group

The set of invertible elements of any commutative topological ring R form a group R^* under multiplication. In general R^* is not a topological group if it is endowed with the subset topology because inversion need not be continuous (only multiplication and addition on R are required to be continuous). It is usual therefore to give R^* the following topology. There is an injection

$$x \mapsto \left(x, \ \frac{1}{x}\right) \tag{16.1}$$

of R^* into the topological product $R \times R$. We give R^* the corresponding subset topology. Then R^* with this topology is a topological group and the inclusion map $R^* \hookrightarrow R$ is continous. To see continuity of inclusion, note that this topology is finer (has at least as many open sets) than the subset topology induced by $R^* \subset R$, since the projection maps $R \times R \to R$ are continuous.

Example 16.1. This is a "non-example". The inverse map on $\mathbf{Z}_p^*$ is continuous with respect to the p-adic topology. If $a, b \in \mathbf{Z}_p^*$, then $|a| = |b| = 1$, so if $|a - b| < \varepsilon$, then

$$\left|\frac{1}{a} - \frac{1}{b}\right| = \left|\frac{b-a}{ab}\right| = \frac{|b-a|}{|ab|} < \frac{\varepsilon}{1} = \varepsilon.$$

Definition 16.2 (Idele Group). The idele group $\mathbb{I}_K$ of K is the group $\mathbb{A}_K^*$ of invertible elements of the adele ring $\mathbb{A}_K$.

We shall usually speak of $\mathbb{I}_K$ as a subset of $\mathbb{A}_K$, and will have to distinguish between the $\mathbb{I}_K$ and $\mathbb{A}_K$-topologies.

Example 16.3. For a rational prime p, let $\mathbf{x}_p$ be the adele whose pth component is p and whose vth component, for $v \neq p$, is 1. Then $\mathbf{x}_p \to 1$ as $p \to \infty$ in $\mathbb{A}_K$. However, there is no way that $\mathbf{x}_p \to 1$ in $\mathbb{I}_K$, for the following reason. If $\mathbf{x}_p \to 1$ in $\mathbb{I}_K$, then since inversion is continuous, we have $\mathbf{x}_p^{-1} \to 1^{-1} = 1$. However, the $\mathbf{x}_p^{-1}$ have component at p equal to p^{-1}, which has valuation p, hence the valuation of $\mathbf{x}_p^{-1} - 1$ goes to ∞ as $p \to \infty$.

Lemma 16.4. *The group of ideles $\mathbb{I}_K$ is the restricted topological project of the K_v^* with respect to the units $U_v = \mathcal{O}_v^* \subset K_v$, with the restricted product topology.*

We omit the proof of Lemma 16.4, which is a matter of thinking carefully about the definitions. The main point is that inversion is continuous on $\mathcal{O}_v^*$ for each v. (See Example 16.1.)

We have seen that K is naturally embedded in $\mathbb{A}_K$, so K^* is naturally embedded in $\mathbb{I}_K$.

Definition 16.5 (Principal Ideles). We call K^*, considered as a subgroup of $\mathbb{I}_K$, the *principal ideles.*

Lemma 16.6. *The principal ideles K^* are discrete as a subgroup of $\mathbb{I}_K$.*

Proof. For K is discrete in $\mathbb{A}_K$, so K^* is embedded in $\mathbb{A}_K \times \mathbb{A}_K$ by (16.1) as a discrete subset. (Alternatively, the subgroup topology on $\mathbb{I}_K$ is finer than the topology coming from $\mathbb{I}_K$ being a subset of $\mathbb{A}_K$, and K is already discrete in $\mathbb{A}_K$.) □

Definition 16.7 (Content of an Idele). The *content* of $\mathbf{x} = \{x_v\}_v \in \mathbb{I}_K$ is

$$c(\mathbf{x}) = \prod_{\text{all } v} |x_v|_v \in \mathbf{R}_{>0}.$$

Lemma 16.8. *The map $\mathbf{x} \to c(\mathbf{x})$ is a continuous homomorphism of the topological group $\mathbb{I}_K$ into $\mathbf{R}_{>0}$, where we view $\mathbf{R}_{>0}$ as a topological group under multiplication. If K is a number field, then c is surjective.*

Proof. That the content map c satisfies the axioms of a homomorphisms follows from the multiplicative nature of the defining formula for c. For continuity, suppose (a, b) is an open interval in $\mathbf{R}_{>0}$. Suppose $\mathbf{x} \in \mathbb{I}_K$ is such that $c(\mathbf{x}) \in (a, b)$. By considering small intervals about each non-unit component of $\mathbf{x}$, we find an open neighborhood $U \subset \mathbb{I}_K$ of $\mathbf{x}$ such that $c(U) \subset (a, b)$. It follows the $c^{-1}((a, b))$ is open.

For surjectivity, use that each archimedean valuation is surjective, and choose an idele that is 1 at all but one archimedean valuation. □

Remark 16.9. Note also that the $\mathbb{I}_K$-topology is that appropriate to a group of operators on $\mathbb{A}_K^+$: a basis of open sets is the $S(C, U)$, where $C, U \subset \mathbb{A}_K^+$ are, respectively, $\mathbb{A}_K$-compact and $\mathbb{A}_K$-open, and S consists of the $\mathbf{x} \in \mathbb{I}_J$ such that $(1 - \mathbf{x})C \subset U$ and $(1 - \mathbf{x}^{-1})C \subset U$.

Definition 16.10 (Principal 1-Ideles). The subgroup $\mathbb{I}_K^1$ of 1-*ideles* is the subgroup of ideles $\mathbf{x} = \{x_v\}$ such that $c(\mathbf{x}) = 1$. Thus $\mathbb{I}_K^1$ is the kernel of c, so we have an exact sequence

$$1 \to \mathbb{I}_K^1 \to \mathbb{I}_K \xrightarrow{c} \mathbf{R}_{>0} \to 1,$$

where the surjectivity on the right is only if K is a number field.

Lemma 16.11. *The subset $\mathbb{I}_K^1$ of $\mathbb{A}_K$ is closed as a subset, and the $\mathbb{A}_K$-subset topology on $\mathbb{I}_K^1$ coincides with the $\mathbb{I}_K$-subset topology on $\mathbb{I}_K^1$.*

Proof. Let $\mathbf{x} \in \mathbb{A}_K$ with $\mathbf{x} \notin \mathbb{I}_K^1$. To prove that $\mathbb{I}_K^1$ is closed in $\mathbb{A}_K$, we find an $\mathbb{A}_K$-neighborhood W of $\mathbf{x}$ that does not meet $\mathbb{I}_K^1$.

1st Case. Suppose that $\prod_v |x_v|_v < 1$ (possibly $= 0$). Then there is a finite set S of v such that

1. S contains all the v with $|x_v|_v > 1$, and

2. $\prod_{v \in S} |x_v|_v < 1$.

Then the set W can be defined by

$$\begin{aligned} |w_v - x_v|_v &< \varepsilon \qquad v \in S \\ |w_v|_v &\leq 1 \qquad v \notin S \end{aligned}$$

for sufficiently small ε.

2nd Case. Suppose that $C := \prod_v |x_v|_v > 1$. Then there is a finite set S of v such that

1. S contains all the v with $|x_v|_v > 1$, and
2. if $v \notin S$ an inequality $|w_v|_v < 1$ implies $|w_v|_v < \frac{1}{2C}$. (This is because for a non-archimedean valuation, the largest absolute value less than 1 is $1/p$, where p is the residue characteristic. Also, the upper bound in Cassels's article is $\frac{1}{2}C$ instead of $\frac{1}{2C}$, but I think he got it wrong.)

We can choose ε so small that $|w_v - x_v|_v < \varepsilon$ (for $v \in S$) implies $1 < \prod_{v \in S} |w_v|_v < 2C$. Then W may be defined by

$$\begin{aligned} |w_v - x_v|_v &< \varepsilon \qquad v \in S \\ |w_v|_v &\leq 1 \qquad v \notin S. \end{aligned}$$

This works because if $\mathbf{w} \in W$, then either $|w_v|_v = 1$ for all $v \notin S$, in which case $1 < c(\mathbf{w}) < 2c$, so $\mathbf{w} \notin \mathbb{I}_K^1$, or $|w_{v_0}|_{v_0} < 1$ for some $v_0 \notin S$, in which case

$$c(\mathbf{w}) = \left(\prod_{v \in S} |w_v|_v \right) \cdot |w_{v_0}| \cdots < 2C \cdot \frac{1}{2C} \cdots < 1,$$

so again $\mathbf{w} \notin \mathbb{I}_K^1$.

We next show that the $\mathbb{I}_K$- and $\mathbb{A}_K$-topologies on $\mathbb{I}_K^1$ are the same. If $\mathbf{x} \in \mathbb{I}_K^1$, we must show that every $\mathbb{A}_K$-neighborhood of $\mathbf{x}$ contains an $\mathbb{A}_K$-neighborhood and vice-versa.

Let $W \subset \mathbb{I}_K^1$ be an $\mathbb{A}_K$-neighborhood of $\mathbf{x}$. Then it contains an $\mathbb{A}_K$-neighborhood of the type

$$\begin{aligned} |w_v - x_v|_v &< \varepsilon \qquad v \in S \\ |w_v|_v &\leq 1 \qquad v \notin S \end{aligned} \tag{16.2}$$

where S is a finite set of valuations v. This contains the $\mathbb{I}_K$-neighborhood in which $\leq$ in (16.2) is replaced by $=$.

Next let $H \subset \mathbb{I}_K^1$ be an $\mathbb{I}_K$-neighborhood. Then it contains an $\mathbb{I}_K$-neighborhood of the form

$$\begin{aligned} |w_v - x_v|_v &< \varepsilon \qquad v \in S \\ |w_v|_v &= 1 \qquad v \notin S, \end{aligned} \tag{16.3}$$

where the finite set S contains at least all archimedean valuations v and all valuations v with $|x_v|_v \neq 1$. Since $\prod |x_v|_v = 1$, we may also suppose that ε is so small that (16.3) implies

$$\prod_v |w_v|_v < 2.$$

Then the intersection of (16.3) with $\mathbb{I}_K^1$ is the same as that of (16.2) with $\mathbb{I}_K^1$, i.e., (16.3) defines an $\mathbb{A}_K$-neighborhood. □

By the product formula we have that $K^* \subset \mathbb{I}_K^1$. The following result is of vital importance in class field theory.

Theorem 16.12. *The quotient $\mathbb{I}_K^1/K^*$ with the quotient topology is compact.*

Proof. After the preceeding lemma, it is enough to find an $\mathbb{A}_K$-compact set $W \subset \mathbb{A}_K$ such that the map

$$W \cap \mathbb{I}_K^1 \to \mathbb{I}_K^1/K^*$$

is surjective. We take for W the set of $\mathbf{w} = \{w_v\}_v$ with

$$|w_v|_v \leq |x_v|_v\,,$$

where $\mathbf{x} = \{x_v\}_v$ is any idele of content greater than the C of Lemma 14.1.

Let $\mathbf{y} = \{y_v\}_v \in \mathbb{I}_K^1$. Then the content of $\mathbf{x}/\mathbf{y}$ equals the content of $\mathbf{x}$, so by Lemma 14.1 there is an $a \in K^*$ such that

$$|a|_v \leq \left|\frac{x_v}{y_v}\right|_v \qquad \text{all } v.$$

Then $a\mathbf{y} \in W$, as required. □

Remark 16.13. The quotient $\mathbb{I}_K^1/K^*$ is totally disconnected in the function field case. For the structure of its connected component in the number field case, see papers of Artin and Weil in the "Proceedings of the Tokyo Symposium on Algebraic Number Theory, 1955" (Science Council of Japan) or Artin-Tate: "Class Field Theory", 1951/2 (Harvard, 1960(?)). The determination of the character group of $\mathbb{I}_K/K^*$ is global class field theory.

17 Ideals and Divisors

Suppose that K is a finite extension of $\mathbf{Q}$. Let F_K be the the free abelian group on a set of symbols in bijection with the non-archimedean valuation v of K. Thus an element of F_K is a finite formal linear combination

$$\sum_{v \text{ non arch.}} n_v \cdot v$$

where $n_v \in \mathbf{Z}$ and all but finitely many n_v are 0.

Lemma 17.1. *There is a natural bijection between F_K and the group of nonzero fractional ideals of $\mathcal{O}_K$. The correspondence is induced by*

$$v \mapsto \wp_v = \{x \in \mathcal{O}_K : v(x) < 1\},$$

where v is a non-archimedean valuation.

Endow F_K with the discrete topology. Then there is a natural continuous map $\pi : \mathbb{I}_K \to F_K$ given by

$$\mathbf{x} = \{x_v\}_v \mapsto \sum_v \mathrm{ord}_v(x_v) \cdot v.$$

This map is continuous since the inverse image of a valuation v (a point) is the product

$$\pi^{-1}(v) = \pi \mathcal{O}_v^* \quad \times \prod_{w \text{ archimedean}} K_w^* \quad \times \prod_{w \neq v \text{ non-arch.}} \mathcal{O}_w^*,$$

which is an open set in the restricted product topology on $\mathbb{I}_K$. Moreover, the image of K^* in F_K is the group of nonzero principal fractional ideals.

Recall that the *class group* C_K of the number field K is by definition the quotient of F_K by the image of K^*.

Theorem 17.2. *The class group C_K of a number field K is finite.*

Proof. We first prove that the map $\mathbb{I}_K^1 \to F_K$ is surjective. Let ∞ be an archimedean valuation on K. If v is a non-archimedean valuation, let $\mathbf{x} \in \mathbb{I}_K^1$ be a 1-idele such that $x_w = 1$ at ever valuation w except v and infinity. At v, choose $x_v = \pi$ to be a generator for the maximal ideal of $\mathcal{O}_v$, and choose x_∞ to be such that $|x_\infty|_\infty = 1/|x_v|_v$. Then $\mathbf{x} \in \mathbb{I}_K$ and $\prod_w |x_w|_w = 1$, so $\mathbf{x} \in \mathbb{I}_K^1$. Also $\mathbf{x}$ maps to $v \in F_K$.

Thus the group of ideal classes is the continuous image of the compact group $\mathbb{I}_K^1/K^*$ (see Theorem 16.12), hence compact. But a compact discrete group is finite. □

17.1 The Function Field Case

When K is a finite separable extension of $\mathbf{F}(t)$, we define the divisor group D_K of K to be the free abelian group on all the valuations v. For each v the number of elements of the residue class field $\mathbf{F}_v = \mathcal{O}_v/\wp_v$ of v is a power, say q^{n_v}, of the number q of elements in $\mathbf{F}_v$. We call n_v the degree of v, and similarly define $\sum n_v d_v$ to be the degree of the divisor $\sum n_v \cdot v$. The divisors of degree 0 form a group D_K^0. As before, the principal divisor attached to $a \in K^*$ is $\sum \mathrm{ord}_v(a) \cdot v \in D_K$. The following theorem is proved in the same way as Theorem 17.2.

Theorem 17.3. *The quotient of D_K^0 modulo the principal divisors is a finite group.*

For those familiar with algebraic geometry and algebraic curves, one can prove Theorem 17.3 from an alternative point of view. There is a bijection between nonsingular geometrically irreducible projective curves over $\mathbf{F}$ and function fields K over $\mathbf{F}$ (which we assume are finite separable extensions of $\mathbf{F}(t)$ such that $\overline{\mathbf{F}} \cap K = \mathbf{F}$). Let X be the curve corresponding to K. The group D_K^0 is in bijection with the divisors of degree 0 on X, a group typically denoted $\mathrm{Div}^0(X)$. The quotient of $\mathrm{Div}^0(X)$ by principal divisors is denoted $\mathrm{Pic}^0(X)$. The *Jacobian* of X is an abelian variety $J = \mathrm{Jac}(X)$ over the finite field $\mathbf{F}$ whose dimension is equal to the genus of X. Moreover, assuming X has an $\mathbf{F}$-rational point, the elements of $\mathrm{Pic}^0(X)$ are in natural bijection with the $\mathbf{F}$-rational points on J. In particular, with these hypothesis, the class group of K, which is isomorphic to $\mathrm{Pic}^0(X)$, is in bijection with the group of $\mathbf{F}$-rational points on an algebraic variety over a finite field. This gives an alternative more complicated proof of finiteness of the degree 0 class group of a function field.

Without the degree 0 condition, the class group won't be finite. It is an extension of $\mathbf{Z}$ by a finite group.

$$0 \to D_K^0/i(K^*) \to C_K \xrightarrow{\deg} n\mathbf{Z} \to 0,$$

where n is the greatest common divisor of the degrees of elemetns of D_K, and $i(K^*)$ is the image of K^* in D_K^0.