FINITENESS OF THE CLASS GROUP

1. Introduction

In order to formalize, e. g. in the theorem prover *Lean*, the finiteness of the class group of rings of integers in number fields, we write some proof in detail. Much of the proof actually applies uniformly to the function field case, assuming (for the time being ...) it's a separable extension of the 'base' field $\mathbb{F}_q(t)$.

NOTE: the only actual intended use of this informal document was to use it in combination with discussions, explanations, etc. to formalize finiteness results for class groups in Lean. In particular, with very few exceptions, no attempt was made to correct errors or complete omissions unless still beneficial for the formalization process. Perhaps it will be 'polished' a little bit more in the future.

2. Notation and conventions

For ideals I, J in some commutative ring R, we use standard divisibility-notation $I|J$, meaning $IH = J$ for some ideal H in R.

3. Preliminaries on Dedekind domains

For ideals in Dedekind rings we have 'to contain is to divide'.

Proposition 3.1. *Let I, J be ideals in a Dedekind domain R. Then*

$$I \supseteq J \Leftrightarrow I|J. \tag{1}$$

Proof. '$\Leftarrow$': trivial (assuming $I|J$, which means $J = IH$ for some ideal H, it remains to show $IH \subseteq I$, which is obvious).
'$\Rightarrow$': Assume $I \supseteq J$. If $I = 0$, then $J = 0$, and hence $I|J$. We are left with the case $I \neq 0$. We take as a starting point that nonzero fractional ideals in a Dedekind domain are invertible. So in particular I is invertible. As fractional ideals we have $H := I^{-1}J \subseteq I^{-1}I = R$. So H is in fact an ideal, and $IH = II^{-1}J = J$ So $I|J$ (as ideals of R). □

It is convenient to have a characterization of prime ideals in terms of ideals only.

Lemma 3.2. *Let R be a commutative ring and P be an ideal in R. Then P is a prime ideal if and only if $P \neq R$ and*

$$\forall \text{ ideals } I, J \subseteq R : IJ \subseteq P \Rightarrow I \subseteq P \text{ or } J \subseteq P. \tag{2}$$

Proof. Unfold definitions etc.... □

Lemma 3.2 and Proposition 3.1 above, now yields the well known 'prime property', but now for ideals.

Corollary 3.3. *Let I, J, P be ideals in a Dedekind domain R with P prime. Then*

$$P|IJ \Rightarrow (P|I \text{ or } P|J)\,.$$

Another useful property is the *cancellation rule* for ideal multiplication in Dedekind domains.

Proposition 3.4. *Let H, I, J be ideals in a Dedekind domain R with H nonzero. Then*

$$IH = JH \Rightarrow I = J.$$

Proof. Again, using the characterization of Dedekind domains that all nonzero fractional ideal are invertible, the result follow by multiplying LHS and RHS of $IH = JH$ by (the fractional ideal) H^{-1}.. □

We now have enough ingredients to our disposal to establish unique factorizarion in terms of ideals in a Dedekind domian.

Theorem 3.5. *Let R be a Dedekind domain. Then every nonzero ideal I of R can be written as a product of prime ideals of R in a unique way, apart from the order of the factors.*

Proof. Existence. If $I = R$, then we are done by the canonical convention that the empty product (of ideals) gives the unit ideal, i.e. R. So Let $I \neq R$. By Zorn's Lemma we get that I is contained in a maximal ideal, which is a nonzero prime ideal P_1. (If one does not like the appeal to Zorn's lemma, which is equivalent to the axiom of choice, then for $R = \mathcal{O}_K$ one can also use R/I is finite instead.) By Proposition 3.1 we see that $P_1|I$, i.e. $I = P_1 I_1$ for some nonzero ideal I_1 of R. Continuing inductively we get $I = P_1 P_2 \dots P_k I_k$ for nonzero prime ideals $P_1, P_2, \dots, P_k$ and nonzero ideal I_k of R. If this process would continue indefinitely, then this woud give us an infinite ascending chain of ideals $I \subsetneq I_1 \subsetneq I_2 \subsetneq \dots$. Since R is Noetherian, this cannot happen, so we must have that for some k the ideal I_k is not divisible by a prime ideal, i.e. $I_k = R$ and consequently $I = P_1 P_2 \dots P_k$. This completes the existence part of the proof.
Uniqueness. Let $I = P_1 P_2 \dots P_k = Q_1 Q_2 \dots Q_l$ be two factorizations of I into (nonzero) prime ideals. By Corollary 3.3 (and induction) we get that P_1 divides Q_i for some $i = 1, 2, \dots, l$. Since Q_i is maximal we get $P_1 = Q_i$. Change notation so that $i = 1$. Now the cancellation rule, i.e. Propostion 3.4, gives $P_2 \dots P_k = Q_2 \dots Q_l$. With induction we get that $k = l$ and, after permuting the indices of the Q_i's, that $P_i = Q_i$ for all i. This yields Theorem 3.5. □

Proposition 3.6. *Let I be a nonzero ideal in a Dedekind domain R. Then there are only finitely many ideals J in R such that $J|I$.*

Proof. This follows e. g. from unique factorization 3.5. □

4. Further preliminaries

An *absolute value* on a ring R with values in an ordered ring S is a function

$$R \to S, \quad x \mapsto |x|$$

satisfying for all $x, y \in R$

- $|x| \geq 0$;
- $|x| = 0 \Leftrightarrow x = 0$;
- $|xy| = |x||y|$;
- $|x + y| \leq |x| + |y|$.

If R and S are domains, with fields of fractions K and L respectively, then an absolute value on R with values in S extends uniquely to an absolute value on K with values in L by letting $|x/y| := |x|/|y|$ for any $x, y \in R$ with $y \neq 0$.

We note that it follows very quickly that

$$|1| = |-1| = 1.$$

Two easy examples are as follows.

Lemma 4.1. *The following functions are absolute values.*

- $$|.|_{arch} : \mathbb{Z} \to \mathbb{Z}, \quad x \mapsto \operatorname{sign}(x)x$$
- *For any domain D and integer $c > 1$*

  $|.|_{\deg} : D[t] \to \mathbb{Z}, \quad f \mapsto c^{\deg f}$ *(if necessary, treat separately $0 \mapsto 0$).*

  In particular, taking $D = \mathbb{F}_q$ (a finite field with q elements) and $c = q$, we get

  $$|.|_{\deg} : \mathbb{F}_q[t] \to \mathbb{Z}, \quad |f|_{\deg} = q^{\deg f}.$$

Proof. Write out definitions, and use standard properties of the degree function, i.e. $\deg(fg) = \deg f + \deg g$ and $\deg(f+g) \leq \max(\deg f, \deg g)$ (treating the zero polynomials separately, or setting $\deg(0) = -\infty$ with the appropriate operations/inequalities for $-\infty$). The second case gives the stronger triangel inequality $|f+g|_{\deg} \leq \max(|f|_{\deg}, |g|_{deg})$, which immediately implies the weaker 'normal' triangle inequality. □

We note that taking $c = q$ for the last absolute value is just some natural normalisation choice. It is of no importance for the results here. So if e. g. taking $c = 2$ would make things easier, that choice would be fine too. Also, just considering $q = p$ (so $\mathbb{F}_q = \mathbb{F}_p \simeq \mathbb{Z}/p\mathbb{Z}$) suffices for our purposes.

A crude estimate for the determinant of a matrix is given below.

Lemma 4.2. *Let R and S be commutative rings with S ordered, and $|.| : R \to S$ an absolute value. Let A be a matrix of size $n \times n$ (for some $n \in \mathbb{N}$) with coefficients in R. Then*

$$|\det(A)| \leq n! \left(\max_{1 \leq i,j \leq n} |A_{i,j}| \right)^n$$

Proof. Induction using row expansion, or using permutation formula/definition for determinant. □

The following will be used for estimating norms.

Corollary 4.3. *Let R and S be commutative rings with S ordered, and $|.| : R \to S$ an absolute value. Let $A_1, \ldots A_n$ be a matrix of size $n \times n$ (for some nonzero $n \in \mathbb{N}$) with coefficients in R. Let $s_1 \ldots s_n \in R$. Then*

$$\left| \det(\sum_{k=1}^{n} s_k A_k) \right| \leq n! \left(n \max_{1 \leq i,j,k \leq n} |(A_k)_{i,j}| \right)^n \left(\max_{1 \leq k \leq n} (|s_k|) \right)^n$$

5. Generalized division with remainder

R is a PID (hence Dedekind domain) with nontrivial absolute value $|.| : R \to \mathbb{Z}$, and field of fractions K. L is a finite and separable (for the time being..) field extension of K, and we let S be the integral closure of R in L. So S is a Dedekind domain. We have the norm map $\mathrm{Norm} : L \to K$, restricting to a function $S \to R$. Denote $n := [L : K]$. Also assume R to be infinite (our main theorem becomes trivial if R is finite).

We also assume that $|.| : R \to \mathbb{Z}$ is a *Euclidean function*, i.e. for all $a, b \in R$ with $b \neq 0$ there exists a $q \in R$ such that $|a - qb| < |b|$. In fact, we take R to be a Euclidean domain as defined in Lean. So it comes with a choice of quotient function $q : R^2 \to \mathbb{Z}$ (ignoring currying in this math writeup).

Since R is a PID, S contains an R-integral basis, i.e. there are (basis elements) $b_1, b_2, \ldots, b_n \in S$ such that for every $x \in S$ there are unique (scalars) $s_1, s_2, \ldots s_n \in R$ with $x = \sum_{i=1}^n s_i b_i$. The scalars define a function $s : S \to R^n, x \mapsto (s_1, \ldots, s_n)$, which is obviously R-linear.

We start with an estimate on norms.

Lemma 5.1. *There exists a constant $C \in \mathbb{R}_{>0}$, depending only on the R-integral basis $b_1, \ldots, b_n \in S$, such that for any $x = \sum_{i=1}^n s_i b_i \in S$*

$$|\operatorname{Norm}(x)| \leq C(\max_i |s_i|)^n.$$

Proof. Follows from Corollary 4.3. □

We will focus on Euclidean domains with the property that 'sufficiently many remainders come arbitrary close to each other'(in higher dimensions) in the following sense.

Definition 5.2. We call R *admissible* if both:

- We have a function $\mathfrak{M} : \mathbb{R}_{>0} \times \mathbb{N} \to \mathbb{N}$;
- For all $\epsilon \in \mathbb{R}_{>0}$, $n \in \mathbb{N}$, $b \in R$, and $A : \mathbb{N}_{\leq \mathfrak{M}(\epsilon,n)} \to R^n$ there exists $j, k \in \mathbb{N}_{\leq \mathfrak{M}(\epsilon,n)}$ such that

$j \neq k$ and for all $i \in \{1, \ldots, n\}$, $|\operatorname{remainder}(A(k)_i, b) - \operatorname{remainder}(A(j)_i, b)| < \epsilon|b|$.

There are equivalent, arguably cleaner, definitions (e. g. without actually incorporating division with remainder), but for the time being this one seems to work just fine. (And will probably be handy for actual computations at some point.)

We will show later that $\mathbb{Z}$ and $\mathbb{F}_q[t]$ are admissible domains. Now our main ingredient for the finiteness of the class group.

Theorem 5.3. *Assume R is admissible. There exists a finite set $M \subset R - \{0\}$, depending only on the R-integral basis $b_1, \ldots, b_n \in S$, such that for all $a \in S$ and $b \in R - \{0\}$ there exist $q \in S$ and $r \in M$ with $|\operatorname{Norm}(ra - qb)| < |\operatorname{Norm}(b)|$.*

Proof. Let C be as in Lemma 5.1 and choose $\epsilon \in \mathbb{R}_{>0}$ such that

$$\epsilon \leq 1/\sqrt[n]{C}. \tag{3}$$

Let $\mathfrak{M}$ be as in Definition 5.2.

Write $a = \sum_{i=1}^n s_i b_i$ ($s_i \in R$).

Choose $\mathfrak{M}(\epsilon, n) + 1$ *distinct* elements $\mu^{(0)}, \ldots, \mu^{(\mathfrak{M}(\epsilon,n))}$ of R (possible since we assumed R to be infinite). And let $M := \{\mu^{(k)} - \mu^{(j)} : 0 \leq j < k \leq \mathfrak{M}(\epsilon, n)\}$, so $M \subseteq R - \{0\}$ (the containment is in fact strict since M is finite and R is not).

For any $j \in \{0, \dots, \mathfrak{M}(\epsilon, n)\}$ and $i \in \{1, \dots n\}$ we let $q_i^{(j)} := \text{quotient}(\mu^{(j)} s_i, b)$ and $r_i^{(j)} := \text{remainder}(\mu^{(j)} s_i, b)$. So $q_i^{(j)}, r_i^{(j)} \in R$ and

$$\mu^{(j)} s_i = q_i^{(j)} b + r_i^{(j)} \text{ and } |r_i^{(j)}| < |b|,$$

and hence

$$\mu^{(j)} a = \sum_{i=1}^{n} \mu^{(j)} s_i b_i = \sum_{i=1}^{n} (q_i^{(j)} b + r_i^{(j)}) b_i = \left(\sum_{i=1}^{n} q_i^{(j)} b_i \right) b + \sum_{i=1}^{n} r_i^{(j)} b_i. \tag{4}$$

Consider the function $A : \mathbb{N}_{\leq \mathfrak{M}(\epsilon,n)} \to R^n,\ j \mapsto (\mu^{(j)} s_1, \dots, \mu^{(j)} s_n)$. Then by Definition 5.2 we have indices j, k with $0 \leq j < k \leq \mathfrak{M}(\epsilon, n)$ such that

$$\text{for all } i \in \{1, \dots, n\},\ |r_i^{(k)} - r_i^{(j)}| < \epsilon |b|. \tag{5}$$

Now define

$$r := \mu^{(k)} - \mu^{(j)} \in M$$

and

$$q := \sum_{i=1}^{n} (q_i^{(k)} - q_i^{(j)}) b_i \in S.$$

Then by (4) (with that j specialised to both (the new) j and k), we have

$$ra - qb = \sum_{i=1}^{n} \left(r_i^{(k)} - r_i^{(j)} \right) b_i.$$

So it remains to show that

$$\left| \text{Norm} \left(\sum_{i=1}^{n} \left(r_i^{(k)} - r_i^{(j)} \right) b_i \right) \right| < |\,\text{Norm}(b)|. \tag{6}$$

Note that since $b \in R$ (coerced into S before taking the norm), we get

$$\text{Norm}(b) = b^n. \tag{7}$$

Now we have

$$\begin{aligned}
\left| \text{Norm} \left(\sum_{i=1}^{n} \left(r_i^{(k)} - r_i^{(j)} \right) b_i \right) \right| &\leq C \left(\max_i |r_i^{(k)} - r_i^{(j)}| \right)^n && \text{(by Lemma 5.1)} \\
&< C(\epsilon |b|)^n && \text{(by (5))} \\
&\leq |b|^n && \text{(by (3))} \\
&= |\,\text{Norm}(b)| && \text{(by multiplicativity of } |.| \text{ and (7)).}
\end{aligned}$$

This proves (6) and thereby finishes the proof of the theorem. □

Now we need to generalize the result above from $b \in R$ to $b \in S$ (nonzero).

Corollary 5.4. *Assume R is admissible. There exists a finite set $M \subset R - \{0\}$, depending only on the R-integral basis $b_1, \dots, b_n \in S$, such that for all $a, b \in S$ with $b \neq 0$ there exist $q \in S$ and $r \in M$ with $|\,\text{Norm}(ra - qb)| < |\,\text{Norm}(b)|$.*

Proof. Unfold definitions (via $\gamma = a/b$) and use multiplicativity of the norm ... □

6. Finiteness of the class group in the admissible case

Notation as in previous section.

The following is a trivial statement about choosing an element of minimal nonzero absolute norm in a nonzero ideal (which obviously also holds for any subset containing a nonzero element).

Lemma 6.1. *Let I be a nonzero ideal of S. Then there exists a nonzero $b \in I$ such that for all $c \in I$*

$$|\operatorname{Norm}(c)| < |\operatorname{Norm}(b)| \Rightarrow c = 0. \tag{8}$$

Proof. Trivial, namely $\{|\operatorname{Norm}(b)| : b \in I - \{0\}\}$ contains a smallest element, which is a positive integer ... □

Theorem 6.2. *Let M be as in Corollary 5.4 and let m be a nonzero common multiple of all elements in M (e. g. the product, so it exists). Then for any nonzero ideal I of S, there exists an ideal J of S such that $I \sim J$ and $J|\langle m\rangle_S$.*

Proof. Let I be a nonzero ideal of S.

- Choose a nonzero $b \in I$ such that for all $c \in I$ we have (8). (Possible by Lemma6.1
- Let $a \in I$. Since M is as in Corollary 5.4, we get $q \in S$ and $r \in M$ with $|\operatorname{Norm}(ra - qb)| < |\operatorname{Norm}(b)|$. Let $c := ra - qb \in I$ (since $a, b \in I$), then the previous item gives us $ra - qb = 0$, i.e.

$$ra = qb.$$

- So $\langle m\rangle_S I \subseteq \langle b\rangle$.
- Now $\langle m\rangle I = \langle b\rangle J$ for a nonzero ideal J of S, and consequently $I \sim J$. Furthermore, $b \in I$, so $\langle b\rangle \subset I$, so $\langle m\rangle\langle b\rangle \subset \langle m\rangle I = \langle b\rangle J$. This gives $\langle m\rangle \subset J$, and hence $J|\langle m\rangle$.

□

Theorem 6.3. *The class group of S is finite.*

Proof. Previous theorem, together with Proposition 3.6 gives finitely may possibilities for J. So finitely many possibilities for $\overline{I} \in \operatorname{Cl}(S)$. Hence $\operatorname{Cl}(S)$ is finite. □

7. Admissibility of $\mathbb{Z}$ and $\mathbb{F}_q[t]$

Lemma 7.1. *$\mathbb{Z}$ (with $|.|_{arch}$) is admissible.*

Proof. This easily follows directly from the box principle... □

The remainder of this section is about the admissibility of $\mathbb{F}_q[t]$, where $\mathbb{F}_q$ denotes a finite field wit q elements. The key is the following result.

Lemma 7.2. *Let $D \in \mathbb{N}$, $b \in \mathbb{F}_q[t]$ (nonzero if that makes live easier), and define $M := q^D$. Then for every function $A_1 : \mathbb{N}_{\leq M} \to \mathbb{F}_q[t]$ with $\forall j \in \mathbb{N}_{\leq M}, \deg A_1(j) < \deg b$, there exists $j, k \in \mathbb{N}_{\leq M}$ such that*

$$j \neq k \text{ and } \deg(A_1(k) - A_1(j)) < \deg b - D.$$

Proof. WLOG $D \leq \deg b$ (note we use $\deg 0 = -\infty <$ any integer).

Every $A_1(j)$ is of the form $\sum_{i \in \mathbb{N}_{<\deg b}} c_i^{(j)} t^i$ with coefficients $c_i^{(j)} \in F_q$. There are a priori $M = q^D$ possibilities for the coefficients $c^{(j)}_{\deg b-1}, c^{(j)}_{\deg b-2}, \ldots, c^{(j)}_{\deg b-D}$. So by the box principle, among the $q^D + 1$ polynomials $A_1(0), \ldots A_1(M)$, there must be at least two, say $A_1(j), A_1(k),\ j \neq k$ with coefficients

$$c^{(j)}_{\deg b-1} = c^{(k)}_{\deg b-1}, c^{(j)}_{\deg b-2} = c^{(k)}_{\deg b-2}, \ldots, c^{(j)}_{\deg b-D} = c^{(k)}_{\deg b-D}.$$

Hence we can write

$$A_1(k) - A_1(j) = \sum_{i \in \mathbb{N}_{<\deg b-D}} (c_i^{(k)} - c_i^{(j)} t^i,$$

i.e. $\deg(A_1(k) - A_1(j)) < \deg b - D$, as was to be shown. □

We now translate the previous lemma.

Lemma 7.3. *Let $\epsilon \in \mathbb{R}_{>0}$, $b \in \mathbb{F}_q[t]$, and choose $D \in \mathbb{N}$ such that $M := q^D \geq 1/\epsilon$ (e. g. $D :=$ ceiling$(-\log \epsilon / \log q)$). Then for every function $A_1 : \mathbb{N}_{\leq M} \to \mathbb{F}_q[t]$ there exists $j, k \in \mathbb{N}_{\leq M}$ such that*

$$j \neq k \text{ and } |\operatorname{remainder}(A_1(k), b) - \operatorname{remainder}(A_1(j), b)| < \epsilon |b|.$$

Proof. Choose A_1 and write $f_i := |\operatorname{remainder}(A_1(i), b)$, so $\deg f_i < \deg b$. By the previous Lemma we have $j \neq k$ such that

$$\deg(f_k - f_j) < \deg b - D.$$

It suffices to show that

$$|f_k - f_j| < \epsilon |b|.$$

This holds, since:

$$|f_k - f_j| = q^{\deg(f_k - f_j)} < q^{\deg b - D} = q^{\deg b}/M = |b|/M \leq \epsilon |b|.$$

□

Lemma 7.4. *For $R = \mathbb{F}_q[t]$ both:*

- *We have a function $\mathfrak{M}_1 : \mathbb{R}_{>0} \to \mathbb{N}$;*
- *For all $\epsilon \in \mathbb{R}_{>0}$, $b \in R$, and $A_1 : \mathbb{N}_{\leq \mathfrak{M}_1(\epsilon)} \to R$ there exists $j, k \in \mathbb{N}_{\leq \mathfrak{M}_1(\epsilon)}$ such that*

$$j \neq k \text{ and } |\operatorname{remainder}(A_1(k), b) - \operatorname{remainder}(A_1(j), b)| < \epsilon |b|.$$

Proof. Follows from previous lemma (with $\mathfrak{M}_1(\epsilon) = M = q^D$). □

Lemma 7.5. *$\mathbb{F}_q[t]$ (with $|.|_{\deg}$) is admissible.*

Proof. Follows from Lemma 7.4 for any R with a nonarchimedean absolute value, by using the box principle... (Taking $\mathfrak{M}(\epsilon, n) = \mathfrak{M}_1(\epsilon)^n$.) □

8. On the finiteness of the class group for global fields

Let $\mathbb{F}$ be a finite field. Let us specialise to $R = \mathbb{Z}$ or $R = \mathbb{F}[t]$, with fraction field $K = \mathbb{Q}$ or $K = \mathbb{F}(t)$ respectively. As before, we let L be a finite separable field extension of K (where separability is automatic if $K = \mathbb{Q}$) and denote by S the integral closure of R in L, called the ring of integers of L (which strictly speaking depends on R in the positive characteristic case).

From Lemmata 7.1 and 7.5 together with Theorem 6.3 we now get our main theorem.

Theorem 8.1. *The class group of S is finite.*