Elasticity of Factorization in Number Fields

Alexander J. Barrios
Purdue University
5 October 2012

Introduction

Definition A Dedekind domain $\mathcal{O}$ is an integral domain, which is Noetherian, integrally closed, and of dimension 1.

Definition Let $\mathcal{O}$ be a ring and $K$ its quotient field. A fractional ideal of $\mathcal{O}$ in $K$ is an $\mathcal{O}$-module $\mathfrak{a}$ contained in $K$ such that there exist an element $d \in \mathcal{O}\setminus \{0\}$ for which $da \subset \mathcal{O}$.

Theorem 1. If $\mathcal{O}$ is a Dedekind domain, then every ideal of $\mathcal{O}$ can be uniquely factored into prime ideals, and the non-zero fractional ideals form a group under multiplication, $I(\mathcal{O})$.

Definition Let $\mathcal{O}$ be a Dedekind domain and $K$ its quotient field. Let $\varphi : K^* \to I(\mathcal{O})$ be defined by $\varphi(u) = u\mathcal{O}$. Define $P(\mathcal{O}) = \text{Im} \varphi$ to be the group of principal fractional ideals of $\mathcal{O}$. The ideal class group of $\mathcal{O}$ is defined to be

$$ Cl(\mathcal{O}) = I(\mathcal{O}) / P(\mathcal{O}) $$

and the class number of $\mathcal{O}$ is $h_{\mathcal{O}} = |Cl(\mathcal{O})|$. When $\mathcal{O}$ is clear from context, we shall omit reference to $\mathcal{O}$ and simply use $Cl, I, P,$ and $h$.

In particular, we have the short exact sequence,

$$ 1 \to P \to I \to Cl \to 1. $$

It is a known result, that over number fields, the ideal class group is finite.

Proposition 2. Let $\mathcal{O}$ be a Dedekind domain. Let $\{\mathfrak{p}_i\}_{i=1}^r$ be a family of prime ideals of $\mathcal{O}$ and suppose that

$$ \prod_{i=1}^r \mathfrak{p}_i = \pi \mathcal{O} $$

for some $\pi \in \mathcal{O}$.

Then $\pi$ is an irreducible element of $\mathcal{O}$ if and only if there is no proper subfamily of $\{\mathfrak{p}_i\}_{i=1}^r$ whose product is principal.

Proof. ($\Rightarrow$) Suppose that there exist a subfamily $\{\mathfrak{p}_j\}_{j=1}^s$ of $\{\mathfrak{p}_i\}_{i=1}^r$ such that

$$ \prod_{j=1}^s \mathfrak{p}_j = \tau \mathcal{O}. $$

In particular, $\tau|\pi$. Since $\pi$ is irreducible, we have that $\tau = u\pi$ for some $u \in \mathcal{O}^\times$. By Theorem 1, we have that $\{\mathfrak{p}_j\}_{j=1}^s = \{\mathfrak{p}_i\}_{i=1}^r$ and so $s = r$. 

1
(⇐) For a contradiction, suppose that \( \pi = \lambda \pi_1 \) with \( \pi_1 \) irreducible. So
\[
\pi \mathcal{O} = \prod_{i=1}^{r} p_i = (\lambda \mathcal{O})(\pi_1 \mathcal{O}).
\]
Since \( \mathcal{O} \) is a Dedekind domain, we have by Theorem 1,
\[
\pi_1 \mathcal{O} = \prod_{j=1}^{s} q_j
\]
where each \( q_j \in \text{mSpec} \mathcal{O} \). But \( \pi_1 \mathcal{O} | \pi \mathcal{O} \) and so
\[
\prod_{j=1}^{s} q_j | \prod_{i=1}^{r} p_i.
\]
By maximality of each \( q_j \) we have that for each \( j \), \( q_j = p_i \) for some \( i \). Reordering if necessary, we have that \( p_i = q_i \) for each \( i \in \{1, \ldots, s\} \). But then \( \{p_i\}_{i=1}^{s} \) is a proper subfamily whose product is principal, a contradiction. \( \square \)

**Corollary 3.** Let \( \mathcal{O} \) be a Dedekind domain and \( \psi : I \rightarrow \text{Cl} \) be the natural map. If \( p \in \text{mSpec} \mathcal{O} \), \( |\varphi(p)| = r \), and \( p^r = \pi \mathcal{O} \), then \( \pi \) is irreducible.

**Proposition 4.** Let \( \mathcal{O} \) be a Dedekind domain and \( \alpha \in \mathcal{O} \) be such that
\[
\alpha \mathcal{O} = \prod_{i=1}^{r} p_i
\]
where each \( p_i \in \text{mSpec} \mathcal{O} \). Then for every irreducible factorization
\[
\alpha = \prod_{j=1}^{n} \pi_i
\]
of \( \alpha \in \mathcal{O} \), there exist a partition \( P = \{P_k\}_{k=1}^{n} \) of \( \{1, \ldots, r\} \) such that
(i.) \( \pi_k \mathcal{O} = \prod_{j \in P_k} p_j \)
(ii.) no proper subfamily of \( \{p_j\}_{j \in P_k} \) has principal product for each \( k \).

**Proof.** Since \( \mathcal{O} \) is a Dedekind domain, we have by Theorem 1 that for each \( i \),
\[
\pi_i \mathcal{O} = \prod_{j=1}^{s_i} q_{ij}.
\]
Since each \( \pi_i | \alpha \), we have that for each \( i \), \( \pi_i \mathcal{O} | \alpha \mathcal{O} \). Thus for each \( i,j \), \( q_{ij} = p_l \) for some \( l \in \{1, \ldots, r\} \). Let
\[
P_k = \left\{ t \in \{1, \ldots, r\} \mid q_{kj} = p_l \text{ where } \pi_k \mathcal{O} = \prod_{j=1}^{s_k} q_{kj} \right\}.
\]
In particular, we have partition \( P = \{P_k\}_{k=1}^{r} \) of \( \{1, \ldots, r\} \) with the property that
\[
\pi_k \mathcal{O} = \prod_{j \in P_k} p_j.
\]
Since each \( \pi_k \) is irreducible, we have by Proposition 2 that for each \( k \), no proper subfamily of \( \{p_j\}_{j \in k} \) has a principal product. \( \square \)
Characterization of Algebraic Number Fields with Class Number 2

Theorem 5 (Carlitz, 1959). Let $K$ be a number field.

The ring of integers $\mathcal{O}_K$ has class number $h \leq 2$ if and only if for every nonzero $\alpha \in \mathcal{O}_K$, the number of irreducible elements $\pi_j$ in every factorization

$$\alpha = \prod_{i=1}^{k} \pi_i$$

depends only on $\alpha$.

Proof. ($\Rightarrow$) If $h = 1$, the $\mathcal{O}_K$ is a UFD and there is nothing to show. So suppose $h = 2$. Let $\alpha \in \mathcal{O}_K$ be nonzero. Since $\mathcal{O}_K$ is a Dedekind domain we have that

$$\alpha \mathcal{O}_K = \prod_{i=1}^{s} p_i \prod_{j=1}^{t} q_j$$

where each $p_i, q_j$ is a prime of $\mathcal{O}_K$ and each $p_i \in P(I_K)$ and $q_j \notin P(I_K)$.

Since each $p_i$ is principal, we have that

$$p_i = \pi_i \mathcal{O}_K$$

where each $\pi_i \in \mathcal{O}_K$ is irreducible. Since $h = 2$, we have that $q_i, q_j \in P(I_K)$ for each $i, j$. In particular, since $\alpha \mathcal{O}_K$ is principal and $\prod_{i=1}^{s} p_i$ is principal, we have that $\prod_{j=1}^{t} q_j$ is principal. By the above we have that $\prod_{j=1}^{t} q_j$ is principal if and only if $t$ is even. So suppose $t = 2u$. Let $q_j q_{j+1} = \tau_j \mathcal{O}_K$ where $j \in \{1, 3, \ldots, t-1\}$ and $k \in \{1, \ldots, u\}$. Thus

$$\alpha \mathcal{O}_K = \prod_{i=1}^{s} \pi_i \mathcal{O}_K \prod_{k=1}^{u} \tau_k \mathcal{O}_K$$

and so

$$\alpha = \epsilon \prod_{i=1}^{s} \pi_i \prod_{k=1}^{u} \tau_k$$

where $\epsilon \in \mathcal{O}_K^\times$. Thus $\alpha$ factors into $s + u$ irreducibles.

($\Leftarrow$) We proceed by contradiction. Suppose the $h > 2$. We will consider two cases, namely when an element $g$ of the class group has order greater two and equal to two.

Let $g \in Cl$ be of order $m > 2$. By the generalized Dirichlet Theorem\(^1\), there exists prime ideals $p$ and $p'$ representing $g$ and $g^{-1}$ in $Cl$. By Proposition 2 and Corollary 3,

$$p p' = \pi_1 \mathcal{O}_K \quad p^m = \pi \mathcal{O}_K \quad p'^m = \pi' \mathcal{O}_K$$

with $\pi, \pi'$, and $\pi_1$ being irreducible in $\mathcal{O}_K$. In particular, $(p p')^m = \pi_1^m \mathcal{O}_K = \pi \pi' \mathcal{O}_K$ and so we have that

$$\pi_1^m = \epsilon \pi \pi'$$

for some $\epsilon \in \mathcal{O}_K^\times$. Thus for $m > 2$, the number of irreducible is not independent of the factorization.

Now we show the case when $m = 2$. Now suppose that there exist $g_1, g_2 \in Cl$ such that $g_1^2 = g_2^2 = e$ but $g_1 g_2 = g_3 \neq e$. Now let $p_1, p_2$, and $p_3$ be prime ideals of $\mathcal{O}_K$ representing the ideal classes $g_1, g_2$, and $g_3$, respectively. Then we have

$$p_j^2 = \pi_j \mathcal{O}_K \quad \text{for } j \in \{1, 2, 3\} \quad \text{and} \quad p_1 p_2 p_3 = \pi \mathcal{O}_K$$

\(^1\)Let $\mathcal{C} \subseteq \mathcal{H}^m \subseteq \mathcal{I}_K^m$ be a chain of subgroups. Then any coset of $\mathcal{H}^m$ in $\mathcal{I}_K^m$ contains infinitely many primes. The density of this set is $[\mathcal{I}_K^m : \mathcal{H}^m]^{-1}$.

For our case, we have that any coset of $P$ in $I$ contains infinitely many primes.
with $\pi, \pi_1, \pi_2, \pi_3 \in \mathcal{O}_K$ being irreducible. In particular, $\pi^2\mathcal{O}_K = (p_1p_2p_3)^2 = \pi_1\pi_2\pi_3\mathcal{O}_K$ and so
\[ \pi^2 = \delta\pi_1\pi_2\pi_3 \]
for some $\delta \in \mathcal{O}_K^\times$. We conclude that when $h > 2$, the number of irreducibles is not independent of the factorization.

**Example** As an example consider $K = \mathbb{Q}(\sqrt{-5})$. It is known that $\text{Cl}_K$ has class number 2 and
\[ 2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \]
and so 6 factorizations consisting of the product of two irreducibles, by Theorem 5, any element of $\mathcal{O}_K$ will yield the same number of irreducible factors.

### Elasticity of Factorization in Number Fields

**Definition** Let $R$ be a Noetherian domain which is not a field. Define
\[ X = \left\{ \frac{m}{n} \in \mathbb{Q} \mid \text{there exist sequences } \{\pi_i\}_{i=1}^m, \{\tau_j\}_{j=1}^n \text{ of irreducible of } R \text{ with } \prod_{i=1}^m \pi_i = \prod_{j=1}^n \tau_j \right\}. \]
The **elasticity** of $R$ is $\sup X$, denoted by $\rho(R)$.

In this terminology we have that Theorem 5 can be restated as:

Given a number field $K$, $\rho(\mathcal{O}_K) = 1$ if and only if $h(\mathcal{O}_K) \leq 2$.

Now we introduce some group theoretic notions, that alongside Proposition 4 will allow us to make the connection to elasticity.

**Definition** Let $G$ be a nontrivial group with identity $e$. Define
\[ Y = \left\{ r \in \mathbb{N} \mid \text{there exists sequence } \{s_i\}_{i=1}^r \subset G \text{ such that } \prod_{j \in J} s_j \neq e \text{ with } J \subseteq \{1, \ldots, r\} \right\}. \]
Set $\sigma(G) = 1 + \sup (Y)$. We call $\sigma(G)$ the **sequential depth** of $G$.

In practice, we will consider $G$ to be $\text{Cl}$.

**Remark** If $\sigma(G)$ is finite, then any family of $\sigma(G)$ elements of $G$ admits a subfamily whose product is $e$.

**Proposition 6.** If $G$ is a nontrivial finite group, then $\sigma(G) \leq |G|$.

**Proof.** Let $|G| = n$. Define
\[ G^{(0)} = \{e\} \]
\[ G^{(1)} = \{g_1, \ldots, g_n\} = G \]
\[ G^{(2)} = \{g_1g_j \mid g_1, g_j \in G\} \]
\[ \vdots \]
\[ G^{(k)} = \{g_{i_1} \cdots g_{i_k} \mid g_{i_j} \in G\}. \]

4
That is, \( G^{(k)} \) represents the \( k \)-fold product of elements of \( G \).

Let \( \{s_i\}_{i=1}^n \) be any sequence of elements in \( G \). For each \( k \in \{1, \ldots, n\} \), and set
\[
t_k = \prod_{i=1}^k s_i.
\]

We claim that if for each \( k \), \( t_k \neq e \), then \( t_k = t_l \) for some \( k \) and \( l \) with \( 1 \leq k < l \leq n \). Note that \( t_j \in G^{(j)} \) for each \( j \).

Since \( \{t_1, \ldots, t_n\} \subset G \)
and no \( t_i \) is \( e \), then \( \{t_1, \ldots, t_n\} \) has a repeated term, and so \( t_k = t_l \) for some \( k \) and \( l \) where \( 1 \leq k < l \leq n \). But then,
\[
t_k^{-1}t_l = \prod_{i=k+1}^l s_i = e
\]
and so \( \sigma(G) \leq |G| \). \( \square \)

**Corollary 7.** Let \( Z_n \) denote the cyclic group of order \( n \). Then \( \sigma(Z_n) = n \) for all \( n > 1 \).

**Proof.** Let \( Z_n = \langle s \rangle \). Then the constant sequence, \( \{s_i\}_{i=1}^{n-1} \) has the property that \( s^k \neq e \) for each \( k \in \{1, \ldots, n-1\} \) and so \( n \leq \sigma(Z_n) \leq n \) and so \( \sigma(Z_n) = n \), as desired. \( \square \)

**Remark** The equality, \( \sigma(G) = |G| \) does not hold in general. Observe that if \( G = Z_3 \times Z_3 \) and \( a, b \in Z_3 \) are generators, then the sequence
\[
\{s_1 = (a, b), s_2 = (a, b), s_3 = (e, b), s_4 = (a, e)\}
\]
is as "maximal" as we can get in \( G \) such that \( \prod_{i=1}^4 s_i = (e, e) \). Thus \( \sigma(G) = 5 \).

**Proposition 8.** Let \( K \) be a number field and \( \mathcal{O} \) its ring of integers.

If \( \text{Cl} \) is nontrivial, then
\[
\rho(\mathcal{O}) \leq \frac{\sigma(\text{Cl})}{2} \leq \frac{h}{2}.
\]

**Proof.** By Proposition 6,
\[
\frac{\sigma(\text{Cl})}{2} \leq \frac{h}{2}.
\]

For the other inequality, let \( \alpha \in \mathcal{O} \setminus (\mathcal{O}^\times \cup \{0\}) \) and suppose that \( \alpha \mathcal{O} \) has prime factorization,
\[
\alpha \mathcal{O} = \prod_{i=1}^{s_\alpha} p_i.
\]

Now define
\[
X_\alpha = \{ r \in \mathbb{N} \mid \text{there exists an irreducible factorization of } \alpha \text{ of length } r \}.
\]
Let \( n_\alpha = \inf(X_\alpha) \), \( m_\alpha = \sup(X_\alpha) \), and set \( \rho_\alpha = \frac{m_\alpha}{n_\alpha} \). Thus
\[
\rho(\mathcal{O}) = \sup \left\{ \rho_\alpha \in \mathbb{Q} \mid \alpha \in \mathcal{O} \setminus (\mathcal{O}^\times \cup \{0\}) \right\}.
\]

By Proposition 4, we have that \( X_\alpha \) is equivalent to
\[
X_\alpha = \left\{ r \in \mathbb{N} \left| \begin{array}{l}
\text{there exists a partition } P = \{P_k\}_{k=1}^r \text{ of } \{1, \ldots, s_\alpha\} \text{ such that } \prod_{j \in P_k} p_j \text{ is principal, but the product of any proper subfamily is not for } k \in \{1, \ldots, r\}.\end{array} \right. \right\}.
\]
Since we are only interested in maximal $\rho_\alpha$, we observe:

(1) The prime factorization $\alpha O$ contains nonprincipal prime ideals since $h \neq 1$.

(2) The prime factorization of $\alpha O$ contains only nonprincipal prime ideals. For if we delete the principal ideals, say $d$ of such ideals, then there exist $\beta \in O \setminus (O^\times \cup \{0\})$ such that $X_\beta = X_\alpha - d$ and so $\rho_\beta > \rho_\alpha$.

Maintaining assumptions (1) and (2) we have that every component $P_k$ of every partition $P$ in the definition of $X_\alpha$ satisfies the inequality

$$2 \leq |P_k| \leq \sigma(Cl). \quad (2)$$

By properties of partitions,

$$2 \leq |P_k| \leq \sum_{k=1}^r |P_k| = s_\alpha$$

and since $n_\alpha = \inf (X_\alpha)$ and $m_\alpha = \sup (X_\alpha)$, we have that $n_\alpha \leq r \leq m_\alpha$ for each $k$. This coupled with (2) gives us that

$$2 \leq |P_k| \implies \sum_{k=1}^r 2 \leq \sum_{k=1}^r |P_k| \implies 2r \leq s_\alpha \implies r \leq \frac{s_\alpha}{2} \text{ and}$$

$$|P_k| \leq \sigma(Cl) \implies \sum_{k=1}^r |P_k| \leq \sum_{k=1}^r \sigma(Cl) \implies s_\alpha \leq r \sigma(Cl) \implies \frac{s_\alpha}{\sigma(Cl)} \leq r.$$

Since these inequalities hold for all maximal partitions $P = \{P_k\}_{k=1}^r$ of $\{1, \ldots, s_\alpha\}$, we conclude that

$$m_\alpha \leq \frac{s_\alpha}{2} \text{ and } \frac{s_\alpha}{\sigma(Cl)} \leq n_\alpha.$$

Hence

$$\rho_\alpha \leq \frac{\sigma(Cl)}{2} \text{ and so } \rho(O) \leq \frac{\sigma(Cl)}{2}.$$

**Remark** The sequential depth of the class group is precisely the supremum of prime factorizations of ideals $\alpha O_K$ where $\alpha$ varies over the irreducible elements of $O$.

**Proposition 9.** Let $O$ be a Dedekind domain. If $Cl$ contains a nontrivial subgroup $N$ with elementary divisor decomposition

$$N = Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_t}$$

so that $n_k | n_{k+1}$ for $k \in \{1, \ldots, t-1\}$. Let

$$\zeta = \frac{1}{n_t} + \sum_{k=1}^{t-1} \frac{1}{n_k}.$$

Then

$$\max \{\zeta, \zeta^{-1}\} \leq \rho(O).$$

**Proof.** Let $p_k$ for $k \in \{1, \ldots, t\}$ be a prime ideal representing a generator for the $k^{th}$ factor of the elementary divisor decomposition of $N$. By the generalized Dirichlet Theorem, there exist a prime ideal $p_{t+1}$ such that $p_{t+1}$ represents the ideal class inverse to $\prod_{j=1}^t p_j$ in $Cl$. By Proposition 2 and Corollary 3,

$$\prod_{j=1}^{t+1} p_j = \pi O$$

$$p_{n_k}^k = \pi_k O \text{ for } k \in \{1, \ldots, t\}$$

$$p_{t+1}^{\pi_{t+1}} = \pi_{t+1} O$$
with \( \pi \) and each \( \pi_k \) being irreducible. Thus

\[
\pi^{n_{t}} \mathcal{O} = \prod_{j=1}^{t+1} \pi_{j}^{n_{j}} \implies \pi^{n_{t}} \mathcal{O} = \pi_{1}^{n_{1}/n_{t}} \pi_{2}^{n_{2}/n_{t}} \cdots \pi_{t+1}^{n_{t+1}/n_{t}}
\]

and so

\[
\pi^{n_{t}} = u \pi_{1}^{n_{1}/n_{t}} \pi_{2}^{n_{2}/n_{t}} \cdots \pi_{t+1}^{n_{t+1}/n_{t}}
\]

for some \( u \in \mathcal{O}^{\times} \). Thus

\[
\rho(\mathcal{O}) \geq \frac{\frac{n_{1}}{n_{t}} + \frac{n_{2}}{n_{t}} + \cdots + \frac{n_{t}}{n_{t}}}{n_{t}} = \frac{1}{n_{t}} + \sum_{k=1}^{t} \frac{1}{n_{k}} = \zeta
\]

and

\[
\rho(\mathcal{O}) \geq \frac{n_{t}}{n_{t} + \frac{n_{2}}{n_{t}} + \cdots + \frac{n_{t}}{n_{t}} + \frac{n_{t}}{n_{t}}} = \left( \frac{1}{n_{t}} + \sum_{k=1}^{t} \frac{1}{n_{k}} \right)^{-1} = \zeta^{-1}.
\]

We conclude that \( \rho(\mathcal{O}) \geq \max \{ \zeta, \zeta^{-1} \} \).

**Corollary 10.** Suppose that \( \text{Cl} \) contains a subgroup of type \( Z_{n} \) where \( n > 1 \) and \( t \geq 1 \). Then

\[
\rho(\mathcal{O}) \geq \max \left\{ \frac{n_{t}}{n_{t} + 1}, \frac{t+1}{n} \right\}.
\]

**Proof.** Take \( N = \prod_{i=1}^{t} Z_{n_{i}} \) in Proposition 9. Then

\[
\zeta = \frac{1}{n} + \sum_{i=1}^{t} \frac{1}{n_{i}} = \frac{1}{n} + \frac{t}{n} = \frac{t+1}{n}
\]

and \( \zeta^{-1} = \frac{n}{t+1} \).

thus \( \rho(\mathcal{O}) \geq \max \left\{ \frac{n}{t+1}, \frac{t+1}{n} \right\} \).

**Corollary 11.** If \( \text{Cl} \) contains a subgroup of type \( Z_{n} \), \( n > 1 \), then \( \rho(\mathcal{O}) \), then \( \rho(\mathcal{O}) \geq \frac{n}{2} \). In particular, if \( \text{Cl} = Z_{n} \), \( n > 1 \), then \( \rho(\mathcal{O}) = \frac{n}{2} \).

**Proof.** Let \( Z_{n} \subset \text{Cl} \) with \( n > 1 \). By Corollary 10,

\[
\rho(\mathcal{O}) \geq \max \left\{ \frac{n}{2}, \frac{2}{n} \right\} = \frac{n}{2}.
\]

If \( \text{Cl} = Z_{n} \) with \( n > 1 \), then by Corollary 7, \( \sigma(Z_{n}) = n \) and by Proposition 8,

\[
\frac{n}{2} \leq \rho(\mathcal{O}) \leq \frac{\sigma(Z_{n})}{2} = \frac{n}{2}
\]

and so \( \rho(\mathcal{O}) = \frac{n}{2} \), as desired.

**Corollary 12** (Carlitz, 1959). Given a number field \( K \), \( \rho(\mathcal{O}_{K}) = 1 \) if and only if \( h(\mathcal{O}_{K}) \leq 2 \).

**Proof.** If \( h = 1 \), then \( \mathcal{O}_{K} \) is a UFD and so \( \rho(\mathcal{O}_{K}) = 1 \).

Suppose \( \rho(\mathcal{O}_{K}) = 1 \), then

\[
\frac{n}{2} \leq 1 \leq \frac{\sigma(Z_{n})}{2} \leq \frac{h}{2}.
\]

Since \( n > 1 \), we must have that \( n = 2 \) and so \( \text{Cl} \) contains exactly one nontrivial subgroup and so \( \text{Cl} = Z_{2} \).

Thus \( h = 2 \). If \( h \leq 2 \), then \( \rho(\mathcal{O}_{K}) \leq 1 \) and so \( \rho(\mathcal{O}_{K}) = 1 \).
Example Let $K = \mathbb{Q}(\sqrt{-23})$. Then $h = 3$ and $\mathcal{O}_K = \mathbb{Z}\left[\frac{1 + \sqrt{-23}}{2}\right]$. Then

$$3 \cdot 3 \cdot 3 = (2 + \sqrt{-23})(2 - \sqrt{-23}).$$

One may show that $3\mathcal{O}_K$ has prime factorization

$$3\mathcal{O}_K = pq$$

with $p \neq q$. Since 3 is irreducible in $\mathcal{O}_K$, we have that $p$ and $q$ are not principal by Proposition 2. In particular, they represent inverse elements of $Cl$, since $Cl = \mathbb{Z}_3$. Moreover, both are of order 3. By Corollary 3,

$$(3\mathcal{O}_K)^3 = (pq)^3 = p^3 q^3 = (\pi_1\mathcal{O}_K)(\pi_2\mathcal{O}_K) = \pi_1\pi_2\mathcal{O}_K.$$ 

Since we know $3^3 = (2 + \sqrt{-23})(2 - \sqrt{-23})$, we conclude that up to reordering, $\pi_1 = (2 - \sqrt{-23})$ and $\pi_2 = (2 + \sqrt{-23})$.

By Corollary 11 we have that $\rho(\mathcal{O}_K) = \frac{3}{2}$.

Example Consider the number field $K = \mathbb{Q}(\sqrt{-21})$. Then $\mathcal{O}_K = \mathbb{Z}\left[\sqrt{-21}\right]$ and $Cl(\mathcal{O}_K) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Let

$$p_2 = (2, 1 + \sqrt{-21})$$

$$p_3 = (3, \sqrt{-21})$$

$$p_5 = (5, 2 + \sqrt{-21})$$

$$p_0 = (30).$$

Then $p_i$ correspond to distinct elements in $Cl(\mathcal{O}_K)$ and we have

$$p_2^3 + p_3^2 + p_5^2 \equiv p_0 \mod P(\mathcal{O}_K) \quad \text{and} \quad p_2p_3p_5 \equiv p_0 \mod P(\mathcal{O}_K).$$

In particular we have,

$$2 \cdot 3 \cdot 5 = 30 = (3 + \sqrt{-21})(3 - \sqrt{-21})$$

and so $\rho(\mathcal{O}_K) \geq \frac{3}{2}$. But for which $K$, is $\rho(\mathcal{O}_K) > \frac{3}{2}$?

Lemma 13. Let $G$ be a finite abelian group, and suppose that $|G| > S^T$ for some $S > 1$, $T > 1$. Then either,

(i.) $G$ contains a subgroup of type $\mathbb{Z}_n$ for some $n > S$.

(ii.) $G$ contains a subgroup of type $\mathbb{Z}_t^S$ for some $t > T$, $S \geq n > 1$.

Proof. Let $G$ have elementary divisor decomposition,

$$G = \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_t}$$

where $n_k | n_{k+1}$ for $k \in \{1, \ldots, t - 1\}$ and in particular $n_1 \leq n_t$. Since $|G| = n_1 \cdots n_t$ we have that $\mathbb{Z}_{n_1}^t \subset G$. So if (ii.) fails, then $n_1 > S$ and so $\mathbb{Z}_{n_1} \subset G$.

On the other hand, if (i.) fails, then $n_t \leq S$ and so

$$S^T < |G| \leq n_t \leq S^T$$

and so $t > T$ and (ii.) holds. 

\[ \square \]

Theorem 14 (Valenza, 1980). Let $K$ be a number field. Then

$$\rho(\mathcal{O}_K) \to \infty \text{ as } h \to \infty.$$
Proof. Fix $M > 1$ and choose $N > (2M)^{2M^2}$. It suffices to show that $\rho(\mathcal{O}_K) > M$ whenever $h = |\text{Cl}| > N$. Since as $h$ gets large, we can choose $h > N > (2M)^{2M^2} > M > 1$. Thus as $h \to \infty$ we have that $M \to \infty$.

For if $|\text{Cl}| > N$, by Lemma 13, one of the following alternatives holds:

(i.) $\text{Cl}$ contains a subgroup of type $\mathbb{Z}_n$ for some $n > 2M$.
(ii.) $\text{Cl}$ contains a subgroup of type $\mathbb{Z}_t^{\ell}$ for some $t > 2M^2$, $2M \geq n > 1$.

If (i.) holds, then by Corollary 11,

$$\rho(\mathcal{O}_K) \geq \frac{n}{2} > M.$$ 

If (ii.) holds, then by Corollary 10,

$$\rho(\mathcal{O}_K) \geq \frac{t + 1}{n} > \frac{2M^2}{2M} = M$$

and so $\rho(\mathcal{O}_K) > M$ whenever $h > N$, as desired. \qed
References

