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 $d\mathfrak{a} \subset \mathcal{O}$.

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 $\varphi : K^{\times} \to I(\mathcal{O})$ be defined by $\varphi(u) = u\mathcal{O}$. Define $P(\mathcal{O}) = \operatorname{Im}\varphi$ 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,

$$1 \longrightarrow P \longrightarrow I \longrightarrow Cl \longrightarrow 1.$$

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 π 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. ($\Longrightarrow$) 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 π 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 $s = r$.

($\Longleftarrow$) For a contradiction, suppose that $\pi = \lambda\pi_1$ with π_1 irreducible. So

$$\pi\mathcal{O} = \prod_{i=1}^{r}\mathfrak{p}_i = (\lambda\mathcal{O})(\pi_1\mathcal{O}).$$

Since $\mathcal{O}$ is a Dedekind domain, we have by Theorem 1,

$$\pi_1\mathcal{O} = \prod_{j=1}^{s}\mathfrak{q}_j$$

where each $\mathfrak{q}_j \in \operatorname{mSpec}\mathcal{O}$. But $\pi_1\mathcal{O}|\pi\mathcal{O}$ and so

$$\prod_{j=1}^{s}\mathfrak{q}_j \mid \prod_{i=1}^{r}\mathfrak{p}_i.$$

By maximality of each $\mathfrak{q}_j$ we have that for each j, $\mathfrak{q}_j = \mathfrak{p}_i$ for some i. Reordering if necessary, we have that $\mathfrak{p}_i = \mathfrak{q}_i$ for each $i \in \{1, \ldots, s\}$. But then $\{\mathfrak{p}_i\}_{i=1}^{s}$ is a proper subfamily whose product is principal, a contradiction. ☐

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

Proposition 4. *Let $\mathcal{O}$ be a Dedekind domain and $\alpha \in \mathcal{O}$ be such that*

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

where each $\mathfrak{p}_i \in \operatorname{mSpec}\mathcal{O}$. Then for every irreducible factorization

$$\alpha = \prod_{j=1}^{n}\pi_i \tag{1}$$

of $\alpha \in \mathcal{O}$, there exist a partition $P = \{P_k\}_{k=1}^{n}$ of $\{1, \ldots, r\}$ such that
(i.) $\pi_k\mathcal{O} = \prod_{j\in P_k}\mathfrak{p}_j$
(ii.) no proper subfamily of $\{\mathfrak{p}_j\}_{j\in P_k}$ has principal product for each k.

Proof. Since $\mathcal{O}$ is a Dedekind domain, we have by Theorem 1 that for each i,

$$\pi_i\mathcal{O} = \prod_{j=1}^{s_i}\mathfrak{q}_{i_j}.$$

Since each $\pi_i|\alpha$, we have that for each i, $\pi_i\mathcal{O} \mid \alpha\mathcal{O}$. Thus for each i, j, $\mathfrak{q}_{i_j} = \mathfrak{p}_l$ for some $l \in \{1, \ldots, r\}$. Let

$$P_k = \left\{ t \in \{1, \ldots, r\} \mid \mathfrak{q}_{k_j} = \mathfrak{p}_t \text{ where } \pi_k\mathcal{O} = \prod_{j=1}^{s_k}\mathfrak{q}_{k_j} \right\}.$$

In particular, we have partition $P = \{P_k\}_{k=1}^{r}$ of $\{1, \ldots, r\}$ with the property that

$$\pi_k\mathcal{O} = \prod_{j\in P_k}\mathfrak{p}_j.$$

Since each π_k is irreducible, we have by Proposition 2 that for each k, no proper subfamily of $\{\mathfrak{p}_j\}_{j\in k}$ has a principal product. ☐

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 π_j in every factorization

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

depends only on α.

Proof. ($\Longrightarrow$) 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

$$\alpha\mathcal{O}_K = \prod_{i=1}^{s} \mathfrak{p}_i \prod_{j=1}^{t} \mathfrak{q}_j$$

where each $\mathfrak{p}_i, \mathfrak{q}_j$ is a prime of $\mathcal{O}_K$ and each $\mathfrak{p}_i \in P(I_K)$ and $\mathfrak{q}_j \notin P(I_K)$.

Since each $\mathfrak{p}_i$ is principal, we have that

$$\mathfrak{p}_i = \pi_i \mathcal{O}_K$$

where each $\pi_i \in \mathcal{O}_K$ is irreducible. Since $h = 2$, we have that $\mathfrak{q}_i\mathfrak{q}_j \in P(I_K)$ for each i, j. In particular, since $\alpha\mathcal{O}_K$ is principal and $\prod_{i=1}^{s} \mathfrak{p}_i$ is principal, we have that $\prod_{j=1}^{t} \mathfrak{q}_j$ is principal. By the above we have that $\prod_{j=1}^{t} \mathfrak{q}_j$ is principal if and only if t is even. So suppose $t = 2u$. Let $\mathfrak{q}_j\mathfrak{q}_{j+1} = \tau_{\frac{j+1}{2}} = \tau_k\mathcal{O}_K$ 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 α factors into $s + u$ irreducibles.

($\Longleftarrow$) 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 $\mathfrak{p}$ and $\mathfrak{p}'$ representing g and g^{-1} in Cl. By Proposition 2 and Corollary 3,

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

with π, π', and π_1 being irreducible in $\mathcal{O}_K$. In particular, $(\mathfrak{p}\mathfrak{p}')^m = \pi_1^m\mathcal{O}_K = \pi\pi'\mathcal{O}_K$ 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 $g_1g_2 = g_3 \neq e$. Now let $\mathfrak{p}_1, \mathfrak{p}_2$, and $\mathfrak{p}_3$ be prime ideals of $\mathcal{O}_K$ representing the ideal classes g_1, g_2, and g_3, respectively. Then we have

$$\mathfrak{p}_j^2 = \pi_j\mathcal{O}_K \quad \text{for } j \in \{1,2,3\} \quad \text{and} \quad \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3 = \pi\mathcal{O}_K$$

[1]Let $\iota(K_{\mathfrak{m},1}) \subset \mathbf{H}^{\mathfrak{m}} \subset \mathbf{I}_K^{\mathfrak{m}}$ be a chain of subgroups. Then any coset of $\mathbf{H}^{\mathfrak{m}}$ in $\mathbf{I}_K^{\mathfrak{m}}$ contains infinitely many primes. The density of this set is $\left[\mathbf{I}_K^{\mathfrak{m}} : \mathbf{H}^{\mathfrak{m}}\right]^{-1}$.

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, $\pi^2 \mathcal{O}_K = (\mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3)^2 = \pi_1 \pi_2 \pi_3 \mathcal{O}_K$ 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 $K = \mathbb{Q}\left(\sqrt{-5}\right)$. It is known that Cl_K has class number 2 and

$$2 \cdot 3 = 6 = \left(1 + \sqrt{-5}\right)\left(1 - \sqrt{-5}\right)$$

and so 6 factorizations consisting of the product of two irreducible, 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

$$Y = \left\{ r \in \mathbb{N} \mid \text{there exists sequence } \{s_i\}_{i=1}^r \subset G \text{ such that } \prod_{j \in J} s_j \neq e \text{ with } J \subsetneq \{1, \ldots, r\} \right\}.$$

Set $\sigma(G) = 1 + \sup(Y)$. We call $\sigma(G)$ the **sequential depth** of G.

In practice, we will consider G to be 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

$$\begin{aligned}
G^{(0)} &= \{e\} \\
G^{(1)} &= \{g_1, \ldots, g_n\} = G \\
G^{(2)} &= \{g_i g_j \mid g_i, g_j \in G\} \\
&\vdots \\
G^{(k)} &= \left\{ g_{i_1} \cdots g_{i_k} \mid g_{i_j} \in G \right\}.
\end{aligned}$$

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 terms, 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 $\sigma(G) \leq |G|$. ☐

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, $\{s\}_{i=1}^{n-1}$ 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. ☐

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 Cl is nontrivial, then

$$\rho(\mathcal{O}) \leq \frac{\sigma(Cl)}{2} \leq \frac{h}{2}.$$

Proof. By Proposition 6,

$$\frac{\sigma(Cl)}{2} \leq \frac{h}{2}.$$

For the other inequality, let $\alpha \in \mathcal{O} \setminus (\mathcal{O}^\times \cup \{0\})$ and suppose that $\alpha\mathcal{O}$ has prime factorization,

$$\alpha\mathcal{O} = \prod_{i=1}^{s_\alpha} \mathfrak{p}_i.$$

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

$$\rho(\mathcal{O}) = \sup\left\{\rho_\alpha \in \mathbb{Q} \mid \alpha \in \mathcal{O} \setminus \left(\mathcal{O}^\times \cup \{0\}\right)\right\}.$$

By Proposition 4, we have that X_α is equivalent to

$$X_\alpha = \left\{ r \in \mathbb{N} \middle| \begin{array}{c} \text{there exists a partition } P = \{P_k\}_{k=1}^r \text{ of } \{1, \ldots, s_\alpha\} \text{ such that } \prod_{j \in P_k} \mathfrak{p}_j \text{ is} \\ \text{principal, but the product of any proper subfamily is not for } k \in \{1, \ldots, r\}. \end{array} \right\}.$$

Since we are only interested in maximal ρ_α, we observe:

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

(2) The prime factorization of $\alpha\mathcal{O}$ contains only nonprincipal prime ideals. For if we delete the principal ideals, say d of such ideals, then there exist $\beta \in \mathcal{O} \setminus (\mathcal{O}^\times \cup \{0\})$ 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_α satisfies the inequality

$$2 \leq |P_k| \leq \sigma(Cl). \tag{2}$$

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

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

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

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

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

□

Remark The sequential depth of the class group is precisely the supremum of prime factorizations of ideals $\alpha\mathcal{O}_K$ where α varies over the irreducible elements of $\mathcal{O}$.

Proposition 9. *Let $\mathcal{O}$ 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 $n_k \mid n_{k+1}$ for $k \in \{1, \ldots, t-1\}$. Let

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

Then

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

Proof. Let $\mathfrak{p}_k$ 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 $\mathfrak{p}_{t+1}$ such that $\mathfrak{p}_{t+1}$ represents the ideal class inverse to $\prod_{j=1}^{t} \mathfrak{p}_j$ in Cl. By Proposition 2 and Corollary 3,

$$\begin{aligned}
\prod_{j=1}^{t+1} \mathfrak{p}_j &= \pi\mathcal{O} \\
\mathfrak{p}_k^{n_k} &= \pi_k\mathcal{O} \text{ for } k \in \{1, \ldots, t\} \\
\mathfrak{p}_{t+1}^{n_t} &= \pi_{t+1}\mathcal{O}
\end{aligned}$$

with π and each π_k being irreducible. Thus

$$\pi^{n_t}\mathcal{O} = \prod_{j=1}^{t+1} \mathfrak{p}_j^{n_t} \Longrightarrow \pi^{n_t}\mathcal{O} = \pi_1^{n_t/n_1}\pi_2^{n_t/n_2}\cdots\pi_t\pi_{t+1}\mathcal{O}$$

and so

$$\pi^{n_t} = u\pi_1^{n_t/n_1}\pi_2^{n_t/n_2}\cdots\pi_t\pi_{t+1}$$

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

$$\rho(\mathcal{O}) \geq \frac{\frac{n_t}{n_1} + \frac{n_t}{n_2} + \cdots + \frac{n_t}{n_t} + \frac{n_t}{n_t}}{n_t} = \frac{1}{n_t} + \sum_{k=1}^{t} \frac{1}{n_k} = \zeta$$

and

$$\rho(\mathcal{O}) \geq \frac{n_t}{\frac{n_t}{n_1} + \frac{n_t}{n_2} + \cdots + \frac{n_t}{n_t} + \frac{n_t}{n_t}} = \left(\frac{1}{n_t} + \sum_{k=1}^{t} \frac{1}{n_k}\right)^{-1} = \zeta^{-1}.$$

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

Corollary 10. *Suppose that Cl contains a subgroup of type Z_n^t where $n > 1$ and $t \geq 1$. Then*

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

Proof. Take $N = \prod_{i=1}^{t} Z_n$ in Proposition 9. Then

$$\zeta = \frac{1}{n} + \sum_{i=1}^{t} \frac{1}{n} = \frac{1}{n} + \frac{t}{n} = \frac{t+1}{n} \text{ and } \zeta^{-1} = \frac{n}{t+1},$$

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

Corollary 11. *If 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 $Cl = Z_n$, $n > 1$, then $\rho(\mathcal{O}) = \frac{n}{2}$.*

Proof. Let $Z_n \subset Cl$ with $n > 1$. By Corollary 10,

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

If $Cl = Z_n$ 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. $\square$

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 Cl contains exactly one nontrivial subgroup and so $Cl = Z_2$. Thus $h = 2$. If $h \leq 2$, then $\rho(\mathcal{O}_K) \leq 1$ and so $\rho(\mathcal{O}_K) = 1$. $\square$

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

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

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

$$3\mathcal{O}_K = \mathfrak{p}\mathfrak{q}$$

with $\mathfrak{p} \neq \mathfrak{q}$. Since 3 is irreducible in $\mathcal{O}_K$, we have that $\mathfrak{p}$ and $\mathfrak{q}$ are not principal by Proposition 2. In particular, they represent inverse elements of Cl, since $Cl = Z_3$. Moreover, both are of order 3. By Corollary 3,

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

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

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

Example Consider the number field $K = \mathbb{Q}\left(\sqrt{-21}\right)$. Then $\mathcal{O}_K = \mathbb{Z}\left[\sqrt{-21}\right]$ and $Cl\left(\mathcal{O}_K\right) \cong Z_2 \times Z_2$. Let

$$\begin{aligned}
\mathfrak{p}_2 &= \left(2, 1+\sqrt{-21}\right)\\
\mathfrak{p}_3 &= \left(3, \sqrt{-21}\right)\\
\mathfrak{p}_5 &= \left(5, 2+\sqrt{-21}\right)\\
\mathfrak{p}_0 &= (30).
\end{aligned}$$

Then $\mathfrak{p}_i$ correspond to distinct elements in $Cl\left(\mathcal{O}_K\right)$ and we have

$$\mathfrak{p}_2^2 + \mathfrak{p}_3^2 + \mathfrak{p}_5^2 \equiv \mathfrak{p}_0 \mod P\left(\mathcal{O}_K\right) \text{ and } \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5 \equiv \mathfrak{p}_0 \mod P\left(\mathcal{O}_K\right).$$

In particular we have,

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

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

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 Z_n for some $n > S$.

$(ii.)$ G contains a subgroup of type Z_n^t for some $t > T$, $S \geq n > 1$.

Proof. Let G have elementary divisor decomposition,

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

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 $Z_{n_1}^t \subset G$. So if $(ii.)$ fails, then $n_1 > S$ and so $Z_{n_1} \subset G$.

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

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

and so $t > T$ and $(ii.)$ holds. □

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

$$\rho\left(\mathcal{O}_K\right) \longrightarrow \infty \text{ as } h \longrightarrow \infty.$$

Proof. Fix $M > 1$ and choose $N > (2M)^{2M^2}$. It suffices to show that $\rho(\mathcal{O}_K) > M$ whenever $h = |Cl| > N$. 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 $|Cl| > N$, by Lemma 13, one of the following alternatives holds:

(i.) Cl contains a subgroup of type Z_n for some $n > 2M$.

(ii.) Cl contains a subgroup of type Z_n^t 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. □

References

[Car60] L. Carlitz. A characterization of algebraic number fields with class number two. *Proc. Amer. Math. Soc.*, 11:391–392, 1960.

[Jan96] Gerald J. Janusz. *Algebraic number fields*, volume 7 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, second edition, 1996.

[Val90] R. J. Valenza. Elasticity of factorization in number fields. *J. Number Theory*, 36(2):212–218, 1990.