

Counting subrings of maximal orders

Jos Brakenhoff
Universiteit Leiden

1 June 2007

Maximal orders

Let K a number field of degree n ,
i.e., a field extension $\mathbb{Q} \subset K$ with $K \cong \mathbb{Q}^n$ as groups.

An *order* \mathcal{O} in K is a ring such that

- ▶ $\mathbb{Z} \subset \mathcal{O} \subset K$
- ▶ $\mathcal{O} \cong \mathbb{Z}^n$ as groups.

The *maximal order* \mathcal{O}_K of K is the largest order inside K .
It is equal to the integral closure of \mathbb{Z} in K .

Counting subrings

Only consider subrings $R \subset \mathcal{O}_K$ of finite index $[\mathcal{O}_K : R] = h$.
Define

$$f_K(G) = \#\{R \subset \mathcal{O}_K \mid [\mathcal{O}_K : R] = h\}.$$

Example

$K = \mathbb{Q}(i)$ a quadratic extension,
then $\mathcal{O}_K = \mathbb{Z}[i]$.

If $h \in \mathbb{Z}_{\geq 0}$, then $\mathbb{Z} + h\mathcal{O}_K$ is the only subring of index h .

So $f_{\mathbb{Q}(i)}(h) = 1$.

Previous results

- ▶ If $n = 2$, then $f_K(h) = 1$.
- ▶ If $n = 3$, then $f_K(h) \sim ch^{1/3}$ as $h \rightarrow \infty$.
- ▶ Jin Nakagawa looked at the case $n = 4$.
Under mild conditions on K he proved $f_K(h) \sim ch^{1/2}(\log h)$.

Question (Manjul Bhargava)

Let K have degree 5, does $f_K(h) = o(h^2)$ hold uniformly in K ?

Uniformizing

Define the function $f(n, h) = \max_{K: \deg K = n} f_K(h)$.

Lemma

For all n, h the number $f(n, h)$ is finite.

Proof

- ▶ If $R \subset \mathcal{O}_K$ of index h , then $h\mathcal{O}_K \subset R$.
- ▶ So $R/h\mathcal{O}_K \subset \mathcal{O}_K/h\mathcal{O}_K$ determines R .
- ▶ $\#\mathcal{O}_K/h\mathcal{O}_K = h^n$.
- ▶ Therefore, $f_K(h) \leq 2^{(h^n)}$.
- ▶ This bound only depends on n , not on the specific K .
Hence $f(n, h) \leq 2^{(h^n)}$.

Goal

Give upper and lower bounds for

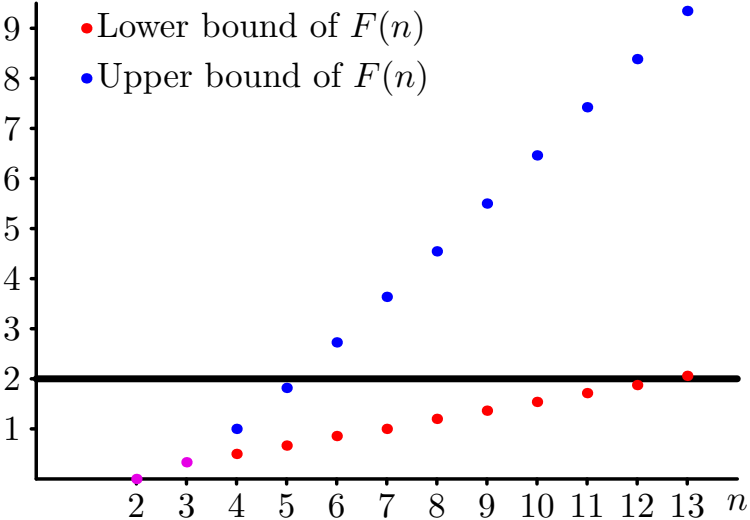
$$F(n) = \limsup_{h \rightarrow \infty} \frac{\log f(n, h)}{\log h}.$$

The question of Manjul Bhargava translates to:

Is $F(5) < 2$?

More generally, for which n is $F(n) < 2$?

Results



Multiplicativity

A function $g : \mathbb{N} \rightarrow \mathbb{Z}$ is called *multiplicative* if for all $h_1, h_2 \in \mathbb{N}$ with $\gcd(h_1, h_2) = 1$ we have $g(h_1 h_2) = g(h_1)g(h_2)$.

$f(n, h)$ is multiplicative in h .

It suffices to know $f(n, p^k)$ for prime powers p^k .

Subgroups

Definition

If $G \subset \mathbb{Z}^N$ is a subgroup of index p^k , then $\mathbb{Z}^N/G = \bigoplus_{i=1}^N (\mathbb{Z}/p^{\lambda_i}\mathbb{Z})$ with $k = \sum_{i=1}^N \lambda_i$.
Order the λ_i such that $\lambda_1 \leq \lambda_2 \leq \dots \leq \lambda_N$.
 $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_N)$ is called the *type* of G .

Counting subgroups

Theorem (Hall polynomials)

Given a type $\lambda = (\lambda_1, \dots, \lambda_N)$, with $\sum_i \lambda_i = k$
there is a monic polynomial $g_\lambda(X) \in \mathbb{Z}[X]$ such that for all $p \in \mathbb{Z}$
prime

$$\#\{G \subset \mathbb{Z}^N \text{ subgroup of index } p^k \text{ and type } \lambda\} = g_\lambda(p).$$

The degree of g_λ is $\sum_{i=1}^N (\lambda_i(2i - N - 1))$.

Corollary

$$\begin{aligned} \limsup_{p \rightarrow \infty} \frac{\log \#\{G \subset \mathbb{Z}^N \text{ index } p^k, \text{ type } \lambda\}}{\log p^k} \\ = \frac{\sum_{i=1}^N (\lambda_i(2i - N - 1))}{k} = c(\lambda) \end{aligned}$$

Example

Take $\lambda_i = e$ for all i , then $k = eN$ and

$$c(\lambda) = \frac{\sum_{i=1}^N (e(2i - N - 1))}{eN} = 0$$

This is the smallest possible value.

Take $\lambda_i = 0$ for $i < N$ and $\lambda_N = k$, then

$$c(\lambda) = \frac{k(2N - N - 1)}{k} = N - 1.$$

This is the largest possible value.

Subgroups containing 1

A subring $R \subset \mathcal{O}_K$ is a subgroup which contains 1.
So $R/\mathbb{Z} \subset \mathcal{O}_K/\mathbb{Z} \cong \mathbb{Z}^{n-1}$ is a subgroup. ($N = n - 1$)

Suppose R has index p^k , then we see that

$$f_K(p^k) \leq \max_{\lambda: \sum_{i=1}^{n-1} \lambda_i = k} c(\lambda) = N - 1 = n - 2.$$

Therefore $F(n) \leq n - 2$.

We see

$$\limsup_{n \rightarrow \infty} \frac{F(n)}{n} \leq 1.$$

Lower bound

Lemma

If $G \subset \mathcal{O}_K$ is a subgroup such that $1 \in G$ and G is of type $(0, 1, 1, \dots, 1, 2, 2, \dots, 2)$, then G is a subring.

Proof

- ▶ $\mathbb{Z} + p^2\mathcal{O}_K \subset G \subset \mathbb{Z} + p\mathcal{O}_K$
- ▶ Take $x_1, x_2 \in \mathbb{Z}$ and $y_1, y_2 \in \mathcal{O}_K$ such that $x_1 + py_1, x_2 + py_2 \in G$.
- ▶ Then $(x_1 + py_1)(x_2 + py_2) = -x_1x_2 + x_1(x_2 + py_1) + x_1(x_2 + py_2) + p^2y_1y_2 \in G$.

For the lower bound we count subgroups $G/\mathbb{Z} \subset \mathcal{O}_K/\mathbb{Z}$ of type $\lambda = (1, 1, \dots, 1, 2, 2, \dots, 2)$.

Let d be the number of twos, then

$$c(\lambda) = \frac{\sum_{i=1}^{n-1} (\lambda_i(2i - (n-1) - 1))}{\sum_{i=1}^{n-1} \lambda_i} = \frac{d(n-d-1)}{n-1+d}.$$

For $n = 13$ this is maximal when $d = 5$. So $F(n) > \frac{5 \cdot 7}{17}$.

In general, it is maximal when d is close to $(\sqrt{2} - 1)(n - 1)$, hence

$$\limsup_{n \rightarrow \infty} \frac{F(n)}{n} \geq (\sqrt{2} - 1)^2.$$

Co-cyclic

$c(\lambda)$ is maximal when $\lambda_i = 0$ for $i < N$ and $\lambda_N = k$.
In that case $\mathcal{O}_K/R \cong \mathbb{Z}/p^k\mathbb{Z}$ as groups.

We call rings with this property *co-cyclic*.

Counting co-cyclic subrings

Theorem

Let K be a number field, and $k \in \mathbb{Z}_{>0}$,
then there is a bijection between

$$\{R \subset \mathcal{O}_K \text{ subring} \mid \mathcal{O}_K/R \cong \mathbb{Z}/p^k\mathbb{Z} \text{ as groups}\}$$

and

$$\{I \subset \mathcal{O}_K \text{ ideal} \mid \mathcal{O}_K/I \cong (\mathbb{Z}/p^k\mathbb{Z})^2 \text{ as groups}\}.$$

We can estimate $\#\{I \subset \mathcal{O}_K \text{ ideal} \mid \mathcal{O}_K/I \cong (\mathbb{Z}/p^k\mathbb{Z})^2\} \leq \binom{n}{2}$.

Rounding rings

Theorem

If $R \subset \mathcal{O}_K$ is a subgroup of index p^k and type λ with $\lambda_{n-1} > 2\lambda_{n-2}$, then

$$R' = \mathcal{O}_K \cap p^{-2\lambda_{n-2}}(R + p^{\lambda_{n-1}}\mathcal{O}_K)$$

is a co-cyclic subgroup of index $p^{\lambda_{n-1}-2\lambda_{n-2}}$.

We say that R is *rounded* to R' .

If R is a subring, then R' is a subring.

We can count the number of subgroups that get rounded to a particular co-cyclic subgroup.

Using co-cyclic rounding we get an upper bound $F(n) \leq n - \frac{8}{3}$.

Upper bound

More generally, rounding can be done towards rings of type

$$(0, \dots, 0, \underbrace{e, \dots, e}_l)$$

with $1 \leq l \leq n - 1$.

Using ring theory, we can give estimates for the number of these types of rings as well (like in the co-cyclic case).

Using all these roundings we get the upper bound $F(5) \leq \frac{20}{11}$.