Counting problems for number rings

Proefschrift

ter verkrijging van
de graad van Doctor aan de Universiteit Leiden,
op gezag van Rector Magnificus prof. mr. P. F. van der Heijden,
volgens besluit van het College voor Promoties
te verdedigen op dinsdag 22 december 2009
klokke 11.15 uur

door

Johannes Franciscus Brakenhoff

geboren te Heemskerk
in 1980

Samenstelling van de promotiecommissie:

promotor:	prof. dr. H. W. Lenstra
overige leden:	prof. dr. P. Stevenhagen
	prof. dr. M. Bhargava (Princeton University)
	prof. dr. J. Top (Rijksuniversiteit Groningen)
	prof. dr. S. J. Edixhoven
	dr. B. de Smit

Counting problems for number rings

Thomas Stieltjes Institute
for Mathematics

Jos Brakenhoff, Leiden, 2009

Op het omslag staat een representatie van de deelringen van index 9 in de maximale orde van $\mathbb{Q}[X]/(X^3 - X + 3)$.

Contents

1 Number rings and counting problems **7**

2 Conventions and notations **16**

3 Equality of polynomial and field discriminants **19**
3.1 Introduction 19
3.2 Probability 20
3.3 Lenstra's heuristic argument 21
3.4 Squarefreeness of polynomial discriminants 24
3.5 Experimental evidence 24
3.6 Appendix – square-free discriminants 25

4 Cocyclic subrings **34**
4.1 Cocyclic subrings and ideals 34
4.2 Cocyclic rings for p-adic orders 36

5 Subrings of maximal orders **37**
5.1 Articulation of the proof 38
5.2 Vector spaces 46
5.3 Localization 47
5.3.1 Weak approximation 48
5.3.2 Local rings of integers 48
5.3.3 Multiplicativity 49
5.4 Counting submodules 51
5.5 Rounding rings 55

6 Artinian principal ideal rings **60**
6.1 Basic ring theory 62
6.1.1 Products 62
6.1.2 Differentials 63
6.1.3 Hensel 63
6.2 Valuations 64
6.3 Subalgebras 68

6.4 Generalized Eisenstein 71
6.5 Equivalence on artinian ideal rings 76

7 Round rings **81**
7.1 Applicability of chapter 6 82
7.2 Finite étale $\mathbb{Q}_p$-algebras 84
7.3 Maximal subrings 85
7.4 Approximate lifts 90
7.5 Bound on round rings 93

8 Quintic rings **96**

9 Class numbers for general orders **99**
9.1 Articulation of the proofs 102
9.2 Picard groups 105
9.3 Class semigroups 106
9.4 Regulators 107
9.5 The size of the normalization kernel 108
9.6 Examples 110

Samenvatting **114**

Curriculum vitae **116**

Chapter 1

Number rings and counting problems

A *number field* is a field that is finite as a vector space over $\mathbb{Q}$, the field of rational numbers. The dimension of the vector space is called the *degree* of the number field. A *number ring* is a domain such that the field of fractions is a number field. Most of the time, we will only consider number rings that are finitely generated as a group. Another term for a finitely generated number ring is *order*.

To an order, we can assign two integers that measure the size of the order. The first is the *rank*, which is the degree of the field of fractions of the order. The second is the *discriminant*, which measures the density of the elements. A larger discriminant tells us that the elements are farther apart. We can see this most easily in imaginary quadratic orders; for positive integers d, the order $\mathbb{Z}[\sqrt{-d}]$ has discriminant $4d$, and if we embed $\mathbb{Z}[\sqrt{-d}]$ into $\mathbb{C}$, the area of the parallelogram $(0, \sqrt{-d}, 1 + \sqrt{-d}, 1)$ is $\sqrt{d}$. This parallelogram is called a *fundamental domain* of the order. We denote the discriminant of an order R by $\Delta(R)$. Note that what we call the discriminant here is the absolute value of the usual discriminant.

Once we know the rank and the discriminant, we have almost determined the order; for every rank and discriminant there are only finitely many orders with that rank and discriminant. This fact is essential when we want to count orders, but it does not help with creating them.

A way we can obtain an order is to take a monic, irreducible polynomial $f \in \mathbb{Z}[X]$ and divide out the ideal it generates. The resulting ring $\mathbb{Z}[X]/(f)$ has field of fractions $\mathbb{Q}[X]/(f)$ and is therefore a number ring. It can be embedded into $\mathbb{C}$ by fixing a root $\alpha \in \mathbb{C}$ of f and taking the map

$$\begin{aligned} \mathbb{Z}[X]/(f) &\to \mathbb{Z}[\alpha] \\ X &\mapsto \alpha. \end{aligned}$$

Orders of this type are called *monogenic*; we can generate them as $\mathbb{Z}$-algebra by one element. The rank of a monogenic order $\mathbb{Z}[\alpha] \cong \mathbb{Z}[X]/(f)$ is equal to the degree of f,

and the discriminant of this order is equal to the absolute value of the discriminant of f.

Not every order is monogenic, for example, the order $\mathbb{Z}[\sqrt{-2}, \sqrt{-5}]$ is not monogenic. However, in every order R we can find an element α such that $\mathbb{Z}[\alpha]$ is close to R, by which we mean that $\mathbb{Z}[\alpha]$ has finite index in R. For $R = \mathbb{Z}[\sqrt{-2}, \sqrt{-5}]$ we can take for example $\alpha = \sqrt{-2} + \sqrt{-5}$; the subring $\mathbb{Z}[\alpha] \subset R$ has index 12.

In every number field we can order the suborders of that number field by inclusion. Then there is a unique largest order, which contains all other orders. This largest order is called the *maximal order* of that number field. Every order R has finite index in the maximal order of the field of fractions of R. For the example $R = \mathbb{Z}[\sqrt{-2}, \sqrt{-5}]$ the field of fractions is $\mathbb{Q}[\sqrt{-2}, \sqrt{-5}]$. The element $\alpha = \frac{\sqrt{-2}+\sqrt{10}}{2}$ satisfies $\alpha^4 - 4\alpha^2 + 9 = 0$ and is therefore an element of the maximal order. The maximal order of $\mathbb{Q}[\sqrt{-2}, \sqrt{-5}]$ is in fact $\mathcal{O} = \mathbb{Z}\left[\frac{\sqrt{-2}+\sqrt{10}}{2}, \sqrt{-5}\right]$ and R has index 2 in $\mathcal{O}$.

When an order R is contained in a larger order R' of the same rank, then its discriminant $\Delta(R)$ is divisible by the discriminant $\Delta(R')$ of the larger order. The quotient is the square of the index of the R in R'.

More information on number rings and orders can be found in for example the lecture notes 'Number rings' by Peter Stevenhagen [11].

Counting problems

Depending on the way we look at number rings, there are several basic questions that arise.

For the construction that uses polynomials, a first natural question would be whether constructing an order by picking a random polynomial is usable in practice. For example, what is the probability that a random monic polynomial is irreducible? We measure the probability that a polynomial of degree n has a certain property P in the following way.

Let for every positive integer H the set $B_n(H)$ consist of all monic polynomials of degree n with coefficients that are at most H in absolute value. We define the probability that a random monic polynomial of degree n has the property P to be

$$\lim_{H\to\infty} \frac{\#\{f \in B_n(H) : f \text{ has property } P\}}{\#B_n(H)},$$

if that limit exists. A theorem by van der Waerden from 1934 states that for every degree the probability that a monic polynomial is irreducible is 1, see [12].

Since each number field has a unique maximal order, a basic counting problem related to number rings is the question how many number fields there are with discriminant up to a given bound, where the discriminant of a number field is defined as the discriminant of its maximal order.

For degree 2 there is classical result, which classifies the number fields by discriminant. In 1969 and 1971, Davenport and Heilbronn published articles where they

studied number fields of degree 3, see [6]. They gave a classification by providing a bijection between the set of isomorphism classes of cubic number fields and the set of certain classes of integral binary cubic forms. In 2005 Manjul Bhargava handled the case of degree 4 by first counting ring structures and then sieving out all but the maximal orders [2]. The theory in chapter 8 from the present thesis is used by Bhargava for the sieving step for degree 5, see [3].

The ideal structure of a maximal order can be studied via the *class group*, denoted by $\mathrm{Cl}(\mathcal{O})$. It is a finite abelian group that measures for a maximal order $\mathcal{O}$ the difference between the group of fractional $\mathcal{O}$-ideals and the group of principal fractional $\mathcal{O}$-ideals. For example, the order $\mathbb{Z}[i]$ is a principal ideal ring, and its class group is therefore the trivial group.

The size of the class group is called the *class number* and is denoted by $h(\mathcal{O})$. A bound on the size of ideals, the Minkowski bound, proved by Hermann Minkowski in 1889, can be used to bound the class number from above; for a maximal order $\mathcal{O}$ of rank n and discriminant Δ, we can bound the class number by

$$h(\mathcal{O}) \leq \left(\frac{2}{\pi}\right)^{n/2} \Delta^{1/2} \frac{(n-1+\log(\Delta^{1/2}))^{n-1}}{(n-1)!}$$

This bound is shown in [7, theorem 6.5].

As an example, we look at maximal quadratic orders, that is, maximal orders of rank 2. For a square-free integer d with $d \neq 1$, we split these orders into two categories, the imaginary orders, where $d < 0$ and the real orders, where $d > 0$.

In the first case, there are nine orders that have class number 1 like $\mathbb{Z}[i]$. It has been shown that in general there are only finitely many maximal imaginary quadratic orders with class number below a given bound. In fact, the class numbers are close to the bound given above. For the real quadratic orders, the class numbers in general are small. It is believed that there are an infinite number of maximal orders whose class number is 1.

The difference between these two cases comes from the fact that imaginary quadratic orders have only a finite number of units, but real quadratic orders have an infinite number. If we want to give a reasonable lower bound on the size of the class group we need to account for the units. This is done by making use of the regulator $R(\mathcal{O})$ of $\mathcal{O}$. For a maximal real quadratic order $\mathcal{O} \subset \mathbb{Q}(\sqrt{d})$, the regulator is $\log((x+y\sqrt{d})/2)$, where $x+y\sqrt{d} \in \mathcal{O}$ is the smallest element under the condition that x and y are positive integers which are a non-trivial solution to the Pellian equation $x^2 - dy^2 = \pm 4$.

The product $h(\mathcal{O})R(\mathcal{O})$ has a better behaviour than the two factors separately. Upper and lowers bound for this product of class group and regulator are given by the Brauer-Siegel theorem, which can be stated as follows. For a number field K with maximal order $\mathcal{O}_K$, we define ϵ_K through the equation

$$h_K R_K = \Delta(\mathcal{O}_K)^{1/2+\epsilon_K} \text{ when } \Delta(\mathcal{O}_K) \neq 1$$
$$\epsilon_K = 0 \text{ when } \Delta(\mathcal{O}_K) = 1.$$

Then for each degree n and each positive real number ϵ, there are only finitely many number fields K of degree n such that $|\epsilon_K| > \epsilon$.

This bound is ineffective, but there is an effective upper bound similar to the upper bound on the class number.

In this thesis we will discuss three counting problems that are related to the three counting problems described above. The first provides a link between the description of orders in terms of polynomials and the one in terms of maximal orders. The second problem is counting suborders of maximal orders. In the last chapter we will generalize the bounds from the Brauer-Siegel theorem to general orders.

Square-free discriminants

Recall that if two orders R and R' have the same rank and satisfy the inclusion $R \subset R'$, then their discriminants are related by $\Delta(R) = (R' : R)^2 \Delta(R')$.

Let f be a monic polynomial. When the discriminant of f is square-free it is implied that the order $\mathbb{Z}[X]/(f)$ is a maximal order. In chapter 3, we will determine a heuristic for the probability that a polynomial has a square-free discriminant and for the probability that a polynomial f is such that $\mathbb{Z}[X]/(f)$ is a maximal order. It turns out that these probabilities are not equal, so that, heuristically, the converse of the implication fails with positive probability.

For degree 2, we can prove these heuristics. The following two theorems hold. The first is proven in section 3.6; the second has a proof that goes similarly.

Theorem 1.1. *The probability that a random monic polynomial in $\mathbb{Z}[X]$ of degree 2 has square-free discriminant is $4/\pi^2$.*

Theorem 1.2. *The probability that a for a random monic polynomial $f \in \mathbb{Z}[X]$ of degree 2 the order $\mathbb{Z}[X]/(f)$ is maximal is $6/\pi^2$.*

This chapter has been published in Experimental Mathematics in 2007 [1].

Suborders

The second counting problem covers several chapters. The main result is described in chapter 5. We take a number field K and look at the orders that have K as field of fractions. Each of those orders R is contained in the maximal order $\mathcal{O}_K$ and the index $(\mathcal{O}_K : R)$ is finite. Furthermore, for every integer m the number of orders R with index m can be bounded in terms of m and n, the degree of the number field K.

Let $f_K(m)$ be the number of orders $R \subset \mathcal{O}_K$ with index m. For example, when K has degree 2, then for every integer m the only subring of $\mathcal{O}_K$ of index m is $\mathbb{Z} + m\mathcal{O}_K$. So in that case $f_K(m)$ is 1.

For number fields of degree 3, there exist a formula for the Dirichlet series $\eta_K(s) = \sum_{m=1}^{\infty} f_K(m) m^{-s}$ in terms of the Riemann zeta function $\zeta(s)$ and the Dedekind zeta function $\zeta_K(s)$ of K. It is

$$\eta_K(s) = \frac{\zeta_K(s)}{\zeta_K(2s)} \zeta(2s)\zeta(3s-1),$$

see [9, lemma 3.2]. By writing out the Euler factors and applying the following proposition, which is proven in section 5.3, we obtain a bound on $f_K(m)$ that is uniform in K.

Proposition 1.3. *The following equality holds for all number fields K*

$$\limsup_{m\to\infty} \frac{\log f_K(m)}{\log m} = \limsup_{p^k\to\infty} \frac{\log f_K(p^k)}{k\log p},$$

where m ranges over the set of positive integers and p^k over the set of prime powers.

The bound we obtain is that for every real $\epsilon > 0$ there is a constant $c_1(\epsilon)$ such that for all number fields K of degree 3 and all integers m we can bound

$$f_K(m) \leq c_1(\epsilon) m^{1/3+\epsilon}.$$

Furthermore, for each number field K of degree 3 there exist infinitely many m such that $f_K(m) \geq m^{1/3-\epsilon}$ holds as well.

For degree 4, Jin Nakagawa provides a similar, but more involved formula for $\eta_K(s)$ in [8]. His results do not cover all cases, but they seem to indicate that we have, similarly to the degree 3 case, that for every real $\epsilon > 0$ there is a constant $c_2(\epsilon)$ such that for all number fields K of degree 4 and all integers m we can bound

$$f_K(m) \leq c_2(\epsilon) m^{1/2+\epsilon}.$$

For each number field K of degree 4 there exist infinitely many m such that $f_K(m) \geq m^{1/2-\epsilon}$ holds as well.

For degree 5 and higher there are no formulas known for $\eta_K(s)$. In chapter 5, we will study the following function

$$F(n) = \limsup_{m\to\infty} \frac{\log(\max_K\{\#R \subset \mathcal{O}_K : R \text{ is a suborder of index } m\})}{\log m},$$

where K ranges over the collection of number fields of degree n. We saw that $F(2) = 0$ and $F(3) = 1/3$, and $F(4)$ is probably equal to $1/2$.

We will give explicit upper and lower bounds for $F(n)$. For example, we will show that $F(5)$ lies between $2/3$ and $20/11$. The bounds we prove for $F(n)$ are not very sharp. They show that $F(3) = 1/3$, but the value for $F(4)$ already has a gap, it lies somewhere between $1/2$ and 1. For large n, they do have the same behaviour, in the sense that the upper and lower bound for $F(n)$ turn out to be both linear in n.

Hall polynomials, first used by Ernst Steinitz in 1901, but named after Philip Hall who redefined them in 1959, count the number of subgroups of finite abelian groups. This theory can be used to give an upper bound on the number of subgroups of maximal orders as well. The bound on $F(n)$ this gives is already quite reasonable and will be the basis of the theory.

The lower bound follows from the following lemma, which is proven in section 5.1.

Lemma 1.4. *Every additive subgroup G of $\mathcal{O}_K$ that satisfies $\mathbb{Z} + m^2\mathcal{O}_K \subset G \subset \mathbb{Z} + m\mathcal{O}_K$ for some integer m is a subring.*

To improve the upper bound, we consider the *cotype* of the order R, that is, the isomorphism type of the finite abelian group $\mathcal{O}_K/R$. For *cocyclic* subrings, that is, subrings such that the cotype is a cyclic group, we use the following theorem, which is proven in chapter 4.

Theorem 1.5. *Let K be a number field of degree n and let $\mathcal{O}_K$ be its maximal order. Let $p^e > 1$ be a prime power and define the set W to be the set of subrings $R \subset \mathcal{O}_K$ with $\mathcal{O}_K/R \cong \mathbb{Z}/p^e\mathbb{Z}$ as groups, which is a set of certain cocyclic subrings. Let V be the set of $\mathcal{O}_K$-ideals I with $\mathcal{O}_K/I \cong (\mathbb{Z}/p^e\mathbb{Z})^2$ as groups. Then the maps*

$$\begin{aligned} f : W &\to V \\ R &\mapsto \{x \in \mathcal{O}_K : x\mathcal{O}_K \subset R\} \end{aligned}$$

and

$$\begin{aligned} g : V &\to W \\ I &\mapsto \mathbb{Z} + I \end{aligned}$$

are well-defined and each others two-sided inverse.

Furthermore, the set V satisfies $\#V \leq \binom{n}{2}$.

We generalize the notion of cocyclic to *round* rings. These are subrings such that the cotype is of the form $(\mathbb{Z}/p^e\mathbb{Z})^d$ for some integers e and d. The cocyclic rings are the round rings with $d = 1$.

For $d \geq 2$, we can also give bounds for the number of round rings. The reason this works is that these round rings have more structure. For example, we have the following theorem from chapter 6.

Theorem 1.6. *Let p be a prime, n, d and $e \geq 2$ be integers and Z be the ring $\mathbb{Z}/p^e\mathbb{Z}$. Let A be a commutative Z-algebra such that $A \cong Z^n$ as Z-module and suppose A is an artinian principal ideal ring. Let $B \subset A$ be a sub-Z-algebra such that $A/B \cong Z^d$ as Z-module. Then B is an artinian principal ideal ring.*

The condition $e \geq 2$ in this theorem cannot be omitted. For $e = 1$ we use the following, weaker result, which is proven in section 7.3.

Definition 1.7. *Let A be a ring. A subring B of A is called* maximal *if there are precisely two rings B' with $B \subset B' \subset A$, namely $B' = B$ and $B' = A$.*

Proposition 1.8. *Let p be a prime and A be a commutative principal ideal ring of characteristic p, that is, a commutative principal ideal $\mathbb{F}_p$-algebra, of finite dimension n as $\mathbb{F}_p$-module. Then the number of maximal subrings of A is at most $\binom{n}{2}$.*

The other, non-round, subrings can sometimes be rounded to round subrings, and this provides us with a new upper bound for the number of subrings of certain

cotypes. This rounding map is described and studied in section 5.5. Combining all the roundings gives the upper bound for $F(n)$.

Finally, in chapter 8 we take a closer look at suborders of number fields of degree 5. We prove the following bound, which is used by Manjul Bhargava to count the number of number fields of degree 5, see [3]. It plays the same role as the theorem by Jin Nakagawa does for degree 4, namely that it can be used to sieve the maximal orders from all orders.

Theorem 1.9. *Define for a number field K and integer m the number*

$$f_K(m) = \#\{R \subset \mathcal{O}_K : R \text{ is a subring of index } (\mathcal{O}_K : R) = m\}.$$

Then there is a constant c_3 such that for every number field K of degree 5 and every prime p we can bound

$$\sum_{k=1}^{\infty} f_K\left(p^k\right)/p^{2k} \leq \frac{c_3}{p^2}.$$

Class semigroups

For a maximal order $\mathcal{O}_K$ in a number field K, we define the group $\mathrm{Frac}(\mathcal{O}_K)$ to be the semigroup of finitely generated fractional $\mathcal{O}_K$-ideals with ideal multiplication as operation. Since $\mathcal{O}_K$ is a maximal order, every fractional $\mathcal{O}_K$-ideal is invertible. Hence this semigroup is in fact a group. The subgroup $\mathrm{PFrac}(\mathcal{O}_K)$ of principal fractional $\mathcal{O}_K$-ideals has finite index. The quotient group $\mathrm{Cl}(\mathcal{O}_K) = \mathrm{Frac}(\mathcal{O}_K)/\mathrm{PFrac}(\mathcal{O}_K)$ is called the *class group* or *Picard group* of $\mathcal{O}_K$.

In chapter 9 we will generalize this notion of class group to general, not necessarily maximal, orders and prove bounds similar to the bounds from Minkowski and Brauer-Siegel. Since for general orders not every fractional ideal is invertible, we can generalize the class group in two ways. For an order A, we let $\mathrm{Frac}(A)$ be the semigroup of fractional A-ideals, $\mathrm{Inv}(A)$ the group of invertible fractional A-ideals and $\mathrm{PFrac}(A)$ the subgroup of principal fractional A-ideals. We define the *Picard group* of A to be

$$\mathrm{Pic}(A) = \mathrm{Inv}(A)/\mathrm{PFrac}(A)$$

and the *class semigroup* of A is

$$\mathrm{Cl}(A) = \mathrm{Frac}(A)/\mathrm{PFrac}(A).$$

Note the the first quotient is dividing out a subgroup, while the quotient in the second formula is dividing out by the action of $\mathrm{PFrac}(A)$ on $\mathrm{Frac}(A)$.

The upper bound from the Brauer-Siegel theorem has been generalized for the Picard group by Jonathan Sands in 1991 [10]. The upper bound he gives is effective.

We prove upper and lower bounds on the size of the Picard group and class semigroup of an order A by relating them to the class group of the maximal order $\mathcal{O}_K$, where K is the field of fractions of A. The difference can be expressed in terms of the *normalization kernel* of A. This is the finite subsemigroup S_A of $\mathrm{Frac}(A)$ consisting

of the fractional A-ideals I that satisfy $I\mathcal{O}_K = \mathcal{O}_K$. In other words, it is the kernel of the normalization map

$$\begin{aligned} \mathrm{Frac}(A) &\to \mathrm{Frac}(\mathcal{O}_K) \\ I &\mapsto I\mathcal{O}_K. \end{aligned}$$

This normalization kernel has been described by Dade-Taussky and Zassenhaus in [5].

For example, let K be a number field and let n be its degree. Let p be an inert prime and define the order $A = \mathbb{Z} + p\mathcal{O}_K$ in K. The set S_A consists of all fractional A-ideals I that satisfy $I\mathcal{O}_K = \mathcal{O}_K$. This implies that every $I \in S_A$ satisfies $p\mathcal{O}_K \subsetneq I \subset \mathcal{O}_K$. On the other hand, for this A every subgroup $N \subset \mathcal{O}_K$ with $p\mathcal{O}_K \subsetneq N$ is a fractional A-ideal and since $p\mathcal{O}_K$ is a maximal $\mathcal{O}_K$-ideal, such a subgroup also satisfies $N\mathcal{O}_K = \mathcal{O}_K$. So S_A consists of all subgroups $N \subset \mathcal{O}_K$ that satisfy $p\mathcal{O}_K \subsetneq N$.

By providing bounds on the normalization kernel, we can use the known bounds for the class group of $\mathcal{O}_K$ to give bounds on the Picard group and class semigroup of A. We can, for example, bound the class semigroup in the following way.

Theorem 1.10. *For all integers n and real numbers $\epsilon > 0$, there exist constants $c_4(n, \epsilon)$ such that for all orders A of rank n we can bound*

$$\#\mathrm{Cl}(A) \leq c_4(n, \epsilon)\Delta(\mathcal{O}_K)^{1/2+\epsilon} m^{2n},$$

where K is the field of fractions of A and m is the index of A in $\mathcal{O}_K$.

Another example of a bound we will prove is the following theorem. It is the Brauer-Siegel theorem for the Picard group of general orders.

Theorem 1.11. *For all integers n and real numbers $\epsilon > 0$, there exist constants $c_5(n, \epsilon) > 0$ and $c_6(n, \epsilon)$ such that for all orders A of rank n we can bound*

$$\frac{\#\mathrm{Pic}(A) \cdot R(A)}{w(A)} \geq c_5(n, \epsilon)\Delta(A)^{1/2-\epsilon}$$

and

$$\frac{\#\mathrm{Pic}(A) \cdot R(A)}{w(A)} \leq c_6(n, \epsilon)\Delta(A)^{1/2+\epsilon},$$

where K is the field of fractions, $R(A)$ the regulator and $w(A)$ the number of roots of unity of A and m is the index of A in $\mathcal{O}_K$.

The upper bound of this theorem also follows immediately from the bound proven by Sands.

Since the proofs of the bounds in chapter 9 use the Brauer-Siegel theorem, they are ineffective. The upper bounds can be made effective by using the effective upper bounds for maximal orders.

Bibliography

[1] A. Ash, J. Brakenhoff, Th. Zarrabi, *Equality of Polynomial and Field Discriminants*, Experiment. Math. **16** (2007) no. 3, 367–374.

[2] M. Bhargava, *The density of discriminants of quartic rings and fields*, Ann. of Math., Princeton, **162** (2005), 1031–1063.

[3] M. Bhargava, *The density of discriminants of quintic rings and fields*, Ann. of Math., Princeton, to appear.

[4] R. Brauer, *On the zeta-function of algebraic number fields*, Amer. J. Math. **69** (1947), 243–250.

[5] E. C. Dade, O. Taussky, H. Zassenhaus, *On the theory of orders, in particular on the semi-group of ideal classes and genera of an order in an algebraic number field*, Math. Ann. **148** (1962), 31–64.

[6] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields*, Bull. London Math. Soc. **1** (1969), 345–348.
H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields. II*, Proc. Roy. Soc. Lond. A. **322** (1971), 405–420.

[7] H. W. Lenstra, Jr., *Algorithms in algebraic number theory*, Bull. Amer. Math. Soc. (N.S.) **26** (1992), 211–244.

[8] J. Nakagawa, *Orders of a quartic field*, Mem. Amer. Math. Soc. **122**, no. 583, 1996.

[9] J. Nakagawa, *On the relations among the class numbers of binary cubic forms*, Invent. Math. **134** (1998), 101–138.

[10] J. W. Sands, *Generalization of a theorem of Siegel*, Acta Arith. **58** (1991), 47–57.

[11] P. Stevenhagen, *Number rings*, `http://websites.math.leidenuniv.nl/algebra/ant.pdf`

[12] B. L. van der Waerden, *Die Seltenheit der Gleichungen mit Affekt*, Math. Ann. **109** (1934), 13–16.

Chapter 2

Conventions and notations

In this chapter we introduce some notation and standard notions that are used throughout the rest of the chapters.

Number fields
A *number field* K is a finite field extension of $\mathbb{Q}$, the field of rationals. We denote the degree of K by $\deg(K)$ and the integral closure of $\mathbb{Z}$ in K by $\mathcal{O}_K$.

p-adic numbers
For a prime number p we denote the ring of p-adic integers by $\mathbb{Z}_p$ and the ring of p-adic rationals by $\mathbb{Q}_p$.

Finite étale algebras
For a field L, a finite étale L-algebra E is a finite product $\prod_i E_i$ of finite separable field extensions E_i of L. The *degree* of E is its dimension over L; we denote the degree of E by $\deg(E)$. We will in particular be interested in finite étale $\mathbb{Q}_p$-algebras.

For a finite étale $\mathbb{Q}_p$-algebra E we denote by $\mathcal{O}_E$ the integral closure of $\mathbb{Z}_p$ in E.

Order notation
Let V and X be collections, and $f_1 : V \to \mathbb{R}$, $f_2 : V \to X$ and $f_3 : V \to \mathbb{R}_{\geq 0}$ maps. By $f_1 = O_{f_2}(f_3)$ we mean that for every $x \in X$ there exists $c(x) \in \mathbb{R}_{\geq 0}$ such that for all $v \in V$ with $f_2(v) = x$ we have $|f_1(v)| \leq c(x) f_3(v)$.

Similarly, let V and X be collections, $f_1 : V \to \mathbb{R}$, $f_2 : V \to X$ and $f_3 : V \to \mathbb{R}_{\geq 1}$ maps and $\alpha \in \mathbb{R}$ a constant. By $f_1 \leq f_3^{\alpha + o_{f_2}(1)}$ we mean that for each $x \in X$ and each $\epsilon \in \mathbb{R}_{>0}$ there is a constant $c(x, \epsilon)$ such that for all $v \in V$ with $f_2(v) = x$ we have $|f_1(v)| \leq c(f_2(v), \epsilon)(f_3(v))^{\alpha + \epsilon}$. Similarly, by $f_1 \geq f_3^{\alpha + o_{f_2}(1)}$ we mean that for each $x \in X$ and each $\epsilon \in \mathbb{R}_{>0}$ there is a constant $c(x, \epsilon) > 0$ such that for all $v \in V$ with $f_2(v) = x$ we have $|f_1(v)| \geq c(f_2(v), \epsilon)(f_3(v))^{\alpha - \epsilon}$.

By $f_1 = f_3^{\alpha + o_{f_2}(1)}$ we mean that both $f_1 \leq f_3^{\alpha + o_{f_2}(1)}$ and $f_1 \geq f_3^{\alpha + o_{f_2}(1)}$ are satisfied.

We usually will not explicitly name the collections and the maps. They should be clear to the reader from the context they are in. For example, one of the results of chapter 7 is stated as follows.

Let E be a finite étale $\mathbb{Q}_p$-algebra and let n be its degree. For integers $e \geq 1$ and $1 \leq d \leq n-1$, let $W_{e,d}(E)$ be the set

$$\big\{R \subset \mathcal{O}_E : R \text{ is a sub-}\mathbb{Z}_p\text{-algebra with } \mathcal{O}_E/R \cong (\mathbb{Z}/p^e\mathbb{Z})^d \text{ as groups}\big\}.$$

Define for positive integers n the constants $c_{10}(n,1) = 0$ and $c_{10}(n,2) = 1$. Furthermore, define for integers n and d with $3 \leq d \leq n-1$ the constant $c_{10}(n,d) = (d-1)(n-d-1)$. Then we can bound

$$\#W_{e,d}(E) = O_n\big(p^{c_{10}(n,d)}\big),$$

where p ranges over the set of primes, E over the collection of finite étale $\mathbb{Q}_p$-algebras, e over the set of positive integers, d over $\{1, \ldots, \deg(E)-1\}$, and n is the degree of E.

For this example the set V consists of the quadruples (p, E, d, e), where p ranges over the set of primes, E over the collection of finite étale $\mathbb{Q}_p$-algebras, e over the set of positive integers and d ranges over $\{1, \ldots, \deg(E)-1\}$. The set X is the set of integers, and the maps are

$$\begin{aligned} f_1 : V &\to \mathbb{R} \\ (p, E, d, e) &\mapsto \#W_{e,d}(E), \end{aligned}$$

$$\begin{aligned} f_2 : V &\to X \\ (p, E, d, e) &\mapsto \deg(E) \end{aligned}$$

and

$$\begin{aligned} f_3 : V &\to \mathbb{R}_{\geq 0} \\ (p, E, d, e) &\mapsto p^{c_{10}(\deg(E),d)}. \end{aligned}$$

Tensors
We denote the tensor product over a commutative ring R of R-modules M and N by $M \otimes_R N$.

Index
For groups M and subgroups $N \subset M$, we write $(M : N)$ for the index of N in M.

Minimal polynomial
Let R be a commutative ring, A a commutative R-algebra and $a \in A$ an element. A polynomial $g \in R[X]$ is called the *minimal polynomial* of a over R if g is monic

and there is an isomorphism

$$\begin{aligned} R[X]/(g) &\to R[a] \\ X &\mapsto a \end{aligned}$$

of R-algebras.

Semigroups

A set H together with an operation $\cdot : H \times H \to H$ such that $\cdot$ is associative and commutative, and H contains a unit element with respect to this operation, is called a *semigroup*.

A *morphism $\phi : H_1 \to H_2$ of semigroups* is a map that sends the unit element of H_1 to the unit element of H_2 and respects the operation.

For a semigroup H, we define H^* to be the group of invertible elements, that is, the elements $h \in H$ such that there exists $h' \in H$ with $h \cdot h'$ equal to the unit element.

Fractional ideals

Let A be a domain with field of fractions K. A *fractional A-ideal* is a non-zero finitely generated A-module I with $I \subset K$. Two fractional ideals I and J can be multiplied; the result is the fractional ideal $I \cdot J$ generated by the products ij of elements $i \in I$ and $j \in J$. We can restrict the generating set of $I \cdot J$ to products of generators of I and J. Hence $I \cdot J$ is also finitely generated. With this multiplication, the set $\mathrm{Frac}(A)$ of fractional A-ideals becomes a semigroup.

We denote the group of invertible fractional ideals $\mathrm{Frac}(A)^*$ by $\mathrm{Inv}(A)$. The principal fractional ideals, that is, the fractional ideals generated by a single element of K^*, form a subgroup of the group of invertible fractional ideals. We denote the group of principal fractional ideals by $\mathrm{PFrac}(A)$.

Chapter 3

Equality of polynomial and field discriminants

This chapter has been published as: Avner Ash, Jos Brakenhoff, and Theodore Zarrabi, "Equality of polynomial and field discriminants", Experimental mathematics, volume 16, number 3 (2007), 367–374. Some minor corrections have been made.

Abstract. We give a conjecture concerning when the discriminant of an irreducible monic integral polynomial equals the discriminant of the field defined by adjoining one of its roots to $\mathbb{Q}$. We discuss computational evidence for it. An appendix by the second author gives a conjecture concerning when the discriminant of an irreducible monic integral polynomial is square-free and some computational evidence for it.

3.1 Introduction

This paper arose out of a search for S_5-extensions of $\mathbb{Q}$ with small discriminant, performed by the first and third authors. Using PARI, they made lists of irreducible monic integral quintic polynomials f and computed both the polynomial discriminant $D_{\mathrm{pol}}(f)$ and the absolute discriminant of the splitting field $D_{\mathrm{field}}(f)$. They noticed that these two discriminants were equal far more often than expected.

Call an irreducible monic integral polynomial f *essential* if $D_{\mathrm{pol}}(f) = D_{\mathrm{field}}(f)$. It is well known that this implies that the ring of integers of the splitting field of f is monogenic.

In reply to an inquiry, Hendrik Lenstra suggested the following:

Conjecture 3.1. *Let $n \geq 2$. The probability that a random irreducible monic integral polynomial of degree n and height $\leq X$ is essential should tend to $6/\pi^2$ as $X \to \infty$.*

For any irreducible monic integral polynomial f, $D_{\mathrm{pol}}(f)/D_{\mathrm{field}}(f)$ is a square integer. Hence, f is essential if $D_{\mathrm{pol}}(f)$ is square-free. However, this square-freeness

does not account for 100% of essential polynomials, probabilistically speaking.

In section 3.3, we present a heuristic argument for conjecture 3.1, due to Lenstra who kindly communicated it to us via email in October 2004. In section 3.4, we ask when does a random polynomial have square-free discriminant? A conjecture of Bjorn Poonen suggests that for a fixed degree, there should be an asymptotic probability for this. In the appendix (section 3.6), the second author gives a precise conjecture for the value of this probability. Unlike conjecture 3.1, this probability depends on the degree of the polynomial.

In section 3.5 and the appendix we present our experimental evidence, gathered using PARI and Magma, where we studied polynomials whose degrees ranged from 2 to 10. This evidence supports our conjectures.

3.2 Probability

In this paper we deal with two kinds of probability that are easily related. First, let n, N be positive integers and let $\mathbb{Z}/N\mathbb{Z}[x]_n$ denote the set of all monic polynomials in $\mathbb{Z}/N\mathbb{Z}[x]$ of degree n.

Suppose $Q(f)$ is a predicate of a monic polynomial f of degree n in $\mathbb{Z}/N\mathbb{Z}[x]$. For example, Q might be the property that f is irreducible.

Define the probability that f possesses Q to be

$$\frac{\#\{f \in \mathbb{Z}/N\mathbb{Z}[x]_n \mid f \text{ has } Q\}}{\#\mathbb{Z}/N\mathbb{Z}[x]_n}.$$

Now let $R(T)$ be a predicate of an irreducible monic polynomial T of degree n in $\mathbb{Z}[x]$. Define the height $h(T)$ to be the maximum of the absolute value of the coefficients of T. Let $B_n(X)$ be the set of all monic, irreducible T of degree n with $h(T) \leq X$. Then we define the probability that T has R to be

$$\lim_{X \to \infty} \frac{\#\{T \in B_n(X) \mid T \text{ has } R\}}{\#B_n(X)}.$$

We make a similar definition for all polynomials (not necessarily irreducible) in a similar way.

We have the following lemma:

Lemma 3.2. *Let n, N be positive integers and Q, R predicates as above. Suppose $R(T) = Q(T \bmod N)$. Then the probability that $T \bmod N$ has Q equals the probability that T has R.*

Proof. Easy, given the fact that the probability that a monic integral polynomial of degree n is irreducible equals 1 [7]. □

3.3 Lenstra's heuristic argument

Let p be a prime number, K a number field and A a sublattice of finite index of the ring of integers $\mathcal{O}_K$ of K. We say that A is *p-maximal* if p does not divide the index of A in $\mathcal{O}_K$.

Let $T \in \mathbb{Z}[x]$ be a monic, irreducible polynomial with root θ and $K = \mathbb{Q}[\theta]$. It is well known that the polynomial discriminant of T equals the field discriminant of K if and only if $\mathbb{Z}[\theta]$ is p-maximal for every prime p. (See for example [3, proposition 16 and remark 1, section 3.3].) We call such a T *essential*. Of course, if T is essential, $\mathcal{O}_K$ is monogenic, that is, $\mathcal{O}_K$ is generated as a ring over $\mathbb{Z}$ by a single element.

We wish to determine the probability (as defined in section 3.2) that an irreducible, monic T of degree n, is essential. Obviously, if $n = 1$ this probability is 1. It will turn out that for $n \geq 2$, the probability we conjecture is independent of n. Start with Dedekind's criterion, as found, for example, in [1, section 6.1.2], as part (2) of theorem 6.1.4.

Denote reduction modulo p by an overbar.

Lemma 3.3 (Dedekind's criterion)**.** *Let $T \in \mathbb{Z}[x]$ be a monic, irreducible polynomial with root θ and $K = \mathbb{Q}[\theta]$. Let p be a prime number. Let*

$$\bar{T} = \prod \bar{t}_i^{e_i}$$

be the factorization of $\bar{T}$ into monic irreducible polynomials in $\mathbb{F}_p[x]$, where the $t_i \in \mathbb{Z}[x]$ are arbitrary monic lifts of the $\bar{t}_i$. Let

$$g = \prod t_i, \qquad h = \prod t_i^{e_i - 1},$$

so that $h \in \mathbb{Z}[x]$ is a monic lift of $\bar{T}/\bar{g}$. Set $f = (gh - T)/p \in \mathbb{Z}[x]$. Then $\mathbb{Z}[\theta]$ is p-maximal if and only if

$$(\bar{f}, \bar{g}, \bar{h}) = 1$$

in $\mathbb{F}_p[x]$.

From this we can derive the following corollary:

Corollary 3.4. *With notation as above, $\mathbb{Z}[\theta]$ is p-maximal if and only if ($\star$) there does not exist a monic polynomial $u \in \mathbb{Z}[x]$ such that $\bar{u}$ is irreducible in $\mathbb{F}_p[x]$ and $T \in (p^2, pu, u^2) \subset \mathbb{Z}[x]$.*

Proof. First suppose that $\mathbb{Z}[\theta]$ is not p-maximal. Then $\bar{f}, \bar{g}, \bar{h}$ have a common factor, which without loss of generality is $\bar{t}_1$. Therefore $e_1 > 1$. Set $u = t_1$. Then $T = gh - pf = \prod t_i^{e_i} - pf$. Since $\bar{u}$ divides $\bar{f}$, we have $au = f + pb$ for some integral polynomials a, b. Hence $pf \in (p^2, pu)$ and $T \in (p^2, pu, u^2)$. Conversely, let u be as in the statement of the corollary. Then $\bar{T} \in (\bar{u}^2)$. Without loss of generality, $u = t_1$ and $e_1 > 1$. Then $\bar{u}$ divides $\bar{g}$ and $\bar{h}$. Now there are integral polynomials a, b, c such that $T = p^2 a + pub + u^2 c$. Therefore, $f = (gh - T)/p = -pa - ub + u^2 \left(\frac{g}{u}\frac{h}{u} - c\right)/p$. By Gauss's lemma, p must divide $\left(\frac{g}{u}\frac{h}{u} - c\right)$. It follows that $\bar{u}$ also divides $\bar{f}$. $\square$

Continuing with the heuristic, we note that the probability that a monic integral polynomial T satisfies $(\star)$ is independent of whether T is irreducible. This is because the probability that T is irreducible is 1 [7]. We can then compute that probability as follows: First note that $(\star)$ depends on T only modulo p^2. Let $R = (\mathbb{Z}/p^2\mathbb{Z})[x]$. For each positive integer i, let R_i denote the set of polynomials in R of degree $\leq i$ and let R_i^{monic} be the subset of monic polynomials of degree i. For any $g \in R$ denote by I_g the ideal (g^2, pg), $I_{g,n} = I_g \cap R_n$, and $I_{g,n}^{\text{monic}} = I_g \cap R_n^{\text{monic}}$. Note that each of these sets depends only on $\bar{g}$.

Lemma 3.5. *Let g, h be monic polynomials in R of degrees d, e respectively such that $\bar{g}$ and $\bar{h}$ are both square-free and relatively prime. Then $I_{g,n} \cap I_{h,n} = I_{gh,n}$.*

Proof. If $f \in I_{g,n} \cap I_{h,n}$ then $f = ag^2 + pbg$ and $f = Ah^2 + pBh$ for some polynomials a, b, A, B. Then $\bar{f} = \bar{a}\bar{g}^2 = \bar{A}\bar{h}^2$, and hence equal to $\bar{C}\overline{(gh)}^2$ for some polynomial C.

Therefore $f - C(gh)^2 = pk$ for some polynomial k. Then

$$k = \frac{ag^2 + pbg - Cg^2h^2}{p} = \frac{(a - Ch^2)g^2}{p} + bg.$$

Since g is monic, this implies that p divides $a - Ch^2$ and thus that $\bar{k}$ is divisible by $\bar{g}$. Similarly, $\bar{k}$ is divisible by $\bar{h}$. It follows that $f = C(gh)^2 + pD(gh)$ for some polynomial D, and so $f \in I_{gh,n}$. The converse is obvious. □

Proposition 3.6. *Let $g_1, \ldots, g_k$ be monic polynomials in R such that the $\bar{g}_i$ are all irreducible and distinct. Let d be the sum of their degrees. Let $f \in R_n^{\text{monic}}$ be randomly chosen. Then the probability $P(g_1, \ldots, g_k)$ that $f \in I_{g_1,n}^{\text{monic}} \cap \cdots \cap I_{g_k,n}^{\text{monic}}$ is 0 if $2d > n$ and p^{-3d} otherwise.*

Proof. Let $g = g_1 \cdots g_k$. Then $I_{g_1,n}^{\text{monic}} \cap \cdots \cap I_{g_k,n}^{\text{monic}} = I_{g_1,n} \cap \cdots \cap I_{g_k,n} \cap R_n^{\text{monic}} = I_{g,n}^{\text{monic}}$ since by lemma 3.5 we have that $I_{g_1,n} \cap \cdots \cap I_{g_k,n} = I_{g,n}$.

We must show that the cardinality of $I_{g,n}^{\text{monic}}$ is 0 if $2d > n$ and p^{2n-3d} otherwise. If $f = ag^2 + pbg$ for some a, b, since f and g are monic, looking modulo p we see that $2d \leq n$. So we may assume from now on that $2d \leq n$.

Define a map of sets

$$\phi : \bar{R}_{n-2d}^{\text{monic}} \times \bar{R}_{n-d-1} \to I_{g,n}^{\text{monic}}$$

as follows: For each $\alpha \in \bar{R}_{n-2d}^{\text{monic}}$ fix a lift $a(\alpha) \in R_{n-2d}^{\text{monic}}$ and for each $\beta \in \bar{R}_{n-d-1}$ fix a lift $b(\beta) \in R_{n-d-1}$. Set $\phi(\alpha, \beta) = a(\alpha)g^2 + pb(\beta)g$. We will show that ϕ is bijective.

1. ϕ is injective: If $a(\alpha)g^2 + pb(\beta)g = a(\alpha')g^2 + pb(\beta')g$ then $\bar{a}(\alpha) = \bar{a}(\alpha')$, which means $\alpha = \alpha'$. Then $pb(\beta)g = pb(\beta')g$ so $b(\beta)g = b(\beta')g + pk$ for some polynomial k and hence $\bar{b}(\beta) = \bar{b}(\beta')$, which means $\beta = \beta'$.

2. ϕ is surjective: Let $f = ag^2 + pbg$ for some a, b, where f is monic. Since $\bar{a}$ must be monic of degree $n - 2d$, we may write $a = a' + pb'$, where a' is itself monic of degree $n - 2d$. By adding $b'g$ to b we may thus assume that a is already monic of

degree $n-2d$ and (since we can add p times any polynomial we like to b) that the degree of b is $n-d$ or less.

Let b_* be the coefficient of x^{n-d} in b. Then $f = ag^2 + pb_*x^{n-d}g + p(b - b_*x^{n-d})g$. Now $p(b-b_*x^{n-d})g$ has degree less than n, so that $ag^2 + pb_*x^{n-d}g$ must be monic of degree n. Then $\bar{a}$ is monic of degree $n-2d$, so that $a = a(\alpha) + pk$ for some α and some polynomial k of degree $n-2d$ or less. Therefore $f = a(\alpha)g^2 + p(b+kg)g$.

Since $f, g, a(\alpha)$ are all monic, the coefficient of x^{n-d} in $b+kg$ (which has degree $n-d$ or less) must be divisible by p. Therefore $\overline{(b+kg)} = \beta$ for some β in $\bar{R}_{n-d-1}$ and $p(b+kg) = pb(\beta)$. Therefore $f = a(\alpha)g^2 + pb(\beta)g$ is in the image of ϕ. It now follows easily that $P(g_1, \ldots, g_k) = p^{-3d}$ if $2d \leq n$. □

Proposition 3.7. *Let P_n denote the probability that an element of R_n^{monic} is not in $I_{g,n}$ for any $g \in R$ such that $\bar{g}$ is irreducible. Then if $n \geq 2$, $P_n = 1 - p^{-2}$.*

Proof. Let $H(t) = \sum_{n \geq 0} P_n t^n$. To evaluate this using our previous results, consider

$$K(t) = (1-t)^{-1} \prod_{\gamma} \left(1 - \frac{t^{2d(\gamma)}}{p^{3d(\gamma)}}\right),$$

where the product runs over all irreducible monic γ in $\bar{R}$ and $d(\gamma)$ denotes the degree of γ. The coefficient of t^n in $K(t)$ is

$$\sum_{k \geq 0} \sum_{\gamma_1, \ldots, \gamma_k} (-1)^k p^{-3d},$$

where the inner sum runs over k-tuples of γ's such that $2d = 2d(\gamma_1) + \cdots + 2d(\gamma_k) \leq n$.

By proposition 3.6, using the usual inclusion-exclusion rule for independent events, we see that the double sum equals P_n. So $H(t) = K(t)$.

On the other hand let $Z(u) = \frac{1}{1-pu}$ be the zeta function of $Y = \operatorname{Spec} \mathbb{F}_p[x]$. Defining s by the equation $u = p^{-s}$, the Euler product for the zeta function gives

$$Z(u) = \prod_{y} (1 - N(y)^{-s})^{-1},$$

where the product is taken over all the closed points y of Y. If y corresponds to the irreducible polynomial γ of degree $d(\gamma)$, its norm is given by $N(y) = p^{d(\gamma)}$. Thus

$$Z(u) = \prod_{\gamma} \left(1 - p^{-d(\gamma)s}\right)^{-1} = \prod_{\gamma} \left(1 - u^{d(\gamma)}\right)^{-1}.$$

Hence as formal power series, we have

$$1 - pu = \prod_{\gamma} \left(1 - u^{d(\gamma)}\right).$$

Setting $u = t^2/p^3$ we obtain

$$1 - \frac{t^2}{p^2} = \prod_{\gamma} \left(1 - \frac{t^{2d(\gamma)}}{p^{3d(\gamma)}}\right).$$

Thus

$$H(t) = (1-t)^{-1}\left(1 - \frac{t^2}{p^2}\right)$$

and the coefficient P_n of t^n is $1 - p^{-2}$ if $n \geq 2$.

□

Finally, we assume that the probabilities that $\mathbb{Z}[\theta]$ is p-maximal, for varying p's, are independent. Applying this assumption to corollary 3.4 and proposition 3.7, we obtain our conjecture 3.1 which we can restate as follows:

Conjecture. *The probability that an irreducible monic integral polynomial T of degree $n \geq 2$ with root θ has its polynomial discriminant equal to the discriminant of the number field $\mathbb{Q}(\theta)$ exists and equals $\prod_p (1 - p^{-2}) = 6/\pi^2$.*

3.4 Squarefreeness of polynomial discriminants

It might be thought that the reason conjecture 3.1 should be true is that almost all polynomials might have square-free discriminant, since the probability that a random integer is square-free is known to be $6/\pi^2$. For if the irreducible, monic, integral polynomial $T(x)$ has discriminant $D(T)$ and the field discriminant of $\mathbb{Q}[x]/(T)$ is D, then it is well-known that $D(T)/D$ is an integral square. (See, for example, [3, section 3.3].)

Section 3.6 presents a conjecture and numerical evidence for the value of the probability that a random polynomial of fixed degree has square-free discriminant. This result denies the "thought" of the previous paragraph.

We remark that the existence of such a probability is consistent with general results of Bjorn Poonen, where the abc conjecture implies that there is a well-defined density P_n for the set of integral, monic polynomials T of fixed degree n with square-free discriminant. The formula for the density is given by [6, theorem 3.2], applied to the discriminant viewed as a polynomial in the coefficients of T. Of course, there is no easy way to evaluate Poonen's formula directly.

3.5 Experimental evidence

The data in table 3a were generated (using PARI) from random samples of one million polynomials per degree, chosen uniformly from a box of prescribed coefficient height 10,000. The polynomials were first checked for reducibility and then the irreducible polynomials had their field and polynomial discriminants compared.

The last column shows the experimental value minus the expected value $6/\pi^2 \approx 0.6079271$ divided by the standard deviation. (The standard deviation σ is computed in the usual way for a binomial distribution with N trials assuming $p = 6/\pi^2$. That is, $\sigma = \sqrt{p(1-p)/N}$, which in our case is ≈ 0.00049.)

Degree	Percent coincidence	Error/standard deviation
2	0.608356	0.8797
3	0.608551	1.2777
4	0.607761	−0.3391
5	0.607229	−1.4289
6	0.607297	−1.2908
7	0.607995	0.0443

Table 3a

3.6 Appendix – square-free discriminants

Let p be a prime and let I be the set of monic irreducible elements of $\mathbb{Z}/p\mathbb{Z}[X]$. If $f \in \mathbb{Z}_p[X]$ is a monic polynomial, then we can write $f \bmod p = \prod_{g \in I} g^{e_g}$. Using Hensel's lemma [8, 2.2.1] we can write $f = \prod_{g \in I} f_g$, where $f_g \in \mathbb{Z}_p[X]$ is monic and satisfies $f_g = g^{e_g} \bmod p$. Recall that we let D_{pol} denote the polynomial discriminant and we denote reduction modulo p by an overbar.

Denote by $R(f, g)$ the resultant of f and g.

Lemma 3.8. *Let $f, g \in \mathbb{Z}_p[X]$, with f monic. If $\gcd(\bar{f}, \bar{g}) = 1$, then $\mathrm{ord}_p R(f, g) = 0$.*

Proof. Write $\bar{f} = (X - t_1) \cdot \ldots \cdot (X - t_n)$, with the t_i in some algebraic closure of $\mathbb{F}_p$. From the proof of [4, section IV.8, proposition 8.3] we have $R(\bar{f}, \bar{g}) = \prod_{i=1}^{n} \bar{g}(t_i)$. Now $p \mid R(f, g)$ if and only if $R(\bar{f}, \bar{g}) = 0$, so $\bar{g}(t_i) = 0$ for some t_i, that is, if t_i is a zero of $\bar{g}$. □

Corollary 3.9. *Let $f, g \in \mathbb{Z}_p[X]$ be monic. If $\gcd(\bar{f}, \bar{g}) = 1$, then $\mathrm{ord}_p(D_{\mathrm{pol}})(fg)) = \mathrm{ord}_p(D_{\mathrm{pol}})(f)) + \mathrm{ord}_p(D_{\mathrm{pol}}(g))$.*

Proof. This follows from $D_{\mathrm{pol}}(fg) = D_{\mathrm{pol}}(f) D_{\mathrm{pol}}(g) R(f, g)^2$ and lemma 3.8. □

Corollary 3.10. *Let $f \in \mathbb{Z}_p[X]$ be monic. If $\bar{f}$ is irreducible, then $\mathrm{ord}_p(D_{\mathrm{pol}}(f)) = 0$.*

Proof. This follows from using lemma 3.8 with $g = f'$ and [4, section IV.8, proposition 8.5]. □

Proposition 3.11. *Let $P_{n,0}$ denote the probability that a monic polynomial $f \in \mathbb{Z}_p[X]$ of degree n satisfies $\operatorname{ord}_p D_{\mathrm{pol}}(f) = 0$. If $n \leq 1$, then $P_{n,0} = 1$ and if $n \geq 2$, then $P_{n,0} = 1 - p^{-1}$.*

Proof. Let $H(t) = \sum_{n \geq 0} P_{n,0} t^n$. From lemma 3.8 and its corollaries, we see that whether the polynomial f satisfies $\operatorname{ord}_p D_{\mathrm{pol}}(f) = 0$ depends only on f modulo p. We have $\operatorname{ord}_p D_{\mathrm{pol}}(f) = 0$ if and only if for all $g \in I$ we have $e_g = 0$ or 1, that is, if and only if $\bar{f}$ is square-free.

Denote by M the set of monic polynomials in $\mathbb{Z}/p\mathbb{Z}[X]$. From unique factorization in $\mathbb{Z}/p\mathbb{Z}[X]$ we have the following formula.

$$\sum_{f \in M} u^{\deg f} = \prod_{g \in I} \sum_{k \geq 0} u^{k \deg g}$$

Taking square-free parts left and replacing u by t/p, we obtain

$$H(t) = \prod_{g \in I} \left(1 + \left(\frac{t}{p}\right)^{\deg g}\right).$$

Now,

$$\begin{aligned}
\frac{1}{1-t} = \sum t^n &= \prod_g \sum_{i \geq 0} \left(\frac{t}{p}\right)^{i \deg g} \\
&= \prod_g \frac{1}{1 - \left(\frac{t}{p}\right)^{\deg g}} = \prod_g \frac{1 + \left(\frac{t}{p}\right)^{\deg g}}{1 - \left(\frac{t^2}{p^2}\right)^{\deg g}} \\
&= H(t) \frac{1}{1 - \frac{t^2}{p}}.
\end{aligned}$$

So $H(t) = (1-t)^{-1}\left(1 - \frac{t^2}{p}\right)$. The coefficient $P_{n,0}$ of t^n is 1 if $n \leq 1$ and $1 - p^{-1}$ otherwise. □

Lemma 3.12. *Let R be a ring and $r \in R[X]$ be a monic polynomial. Denote by $\Omega_{(R[X]/(r))/R}$ the module of Kähler differentials of $R[X]/r$ over R. Then we have an isomorphism $\Omega_{(R[X]/r)/R} \cong R[X]/(r, r')$.*

Proof. Follows from [5, section 10.26] □

Write $l(L)$ for the length of a finite-length $\mathbb{Z}_p$-module L, and set $e(\psi, L) = l(\operatorname{cok}(\psi)) - l(\ker(\psi))$ for a $\mathbb{Z}_p$-module endomorphism $\psi : L \to L$.

Lemma 3.13. *Let $f \in \mathbb{Z}_p[X]$ be monic and $h \in I$. Then $\operatorname{ord}_p D_{\mathrm{pol}}(f_h) \geq (e_h - 1) \cdot \deg h$. If also $p \mid e_h$, then $\operatorname{ord}_p D_{\mathrm{pol}}(f_h) \geq e_h \deg h$.*

Proof. Let

$$\begin{aligned}\phi : \mathbb{Z}_p[X]/f_h &\to \mathbb{Z}_p[X]/f_h \\ x &\mapsto f_h' x\end{aligned}$$

be multiplication by f_h'. Then $\operatorname{cok}(\phi) = \mathbb{Z}_p[X]/(f_h, f_h') = \Omega_{(Z_p[X]/f_h)/Z_p}$ (lemma 3.12).

From [2, lemma A.2.6] we get that $e(\phi, \mathbb{Z}_p[X]/f_h) = e(\det(\phi), \mathbb{Z}_p)$ and from [2, example A.2.1] we get $\det(\phi) = R(f_h, f_h') = D_{\mathrm{pol}}(f_h)$. We have

$$p^{\operatorname{ord}_p D_{\mathrm{pol}}(f_h)} = p^{e(\det(\phi), \mathbb{Z}_p)} \geq \#\Omega_{(\mathbb{Z}_p[X]/f_h)/\mathbb{Z}_p}.$$

The map

$$\begin{aligned}\Omega_{(\mathbb{Z}_p[X]/(f_h))/\mathbb{Z}_p} &\to \Omega_{(\mathbb{F}_p[X]/(f_h))/\mathbb{F}_p} \\ dg &\mapsto d\bar{g}\end{aligned}$$

is surjective, so

$$\begin{aligned}\#\Omega_{(\mathbb{Z}_p[X]/f_h)/\mathbb{Z}_p} &\geq \#\Omega_{(\mathbb{F}_p[X]/(f_h))/\mathbb{F}_p} = \#\mathbb{F}_p[X]/(f_h, f_h') \\ &= \begin{cases} \#\mathbb{F}_p[X]/(h^{e_h}) = p^{e_h \deg(h)} & \text{if } p \mid e_h \\ \#\mathbb{F}_p[X]/(h^{e_h - 1}) = p^{(e_h - 1)\deg(h)} & \text{otherwise,} \end{cases}\end{aligned}$$

which completes the proof. □

Proposition 3.14. *A monic polynomial $f \in \mathbb{Z}_p[X]$ satisfies $\operatorname{ord}_p D_{\mathrm{pol}}(f) = 1$ if and only if the following conditions are met:*

1. *$p \neq 2$;*
2. *there is a unique $h \in I$ for which $e_h \geq 2$;*
3. *for this h we have $\deg h = 1$ and $e_h = 2$;*
4. *if $h = X - \widetilde{\alpha}$, and α is any lift of $\widetilde{\alpha}$ to $\mathbb{Z}_p$, then $f_h(\alpha) \not\equiv 0 \bmod p^2$.*

Proof. Let I' be the set of all $g \in I$ with $e_g \geq 2$.

From lemma 3.8, its corollaries and lemma 3.13, we see that

$$\operatorname{ord}_p(D_{\mathrm{pol}}(f)) = \sum_{g \in I'} \operatorname{ord}_p(D_{\mathrm{pol}}(f_g)) \geq \sum_{g \in I'} (e_g - 1) \deg g.$$

This can equal 1 only if $\#I' = 1$ and the only $h \in I'$ satisfies $\deg h = 1$ and $e_h = 2$. Furthermore, if $p = 2$, then $\operatorname{ord}_p(D_{\mathrm{pol}}(f)) \geq e_h \deg h = 2$. So $p \neq 2$.

If f satisfies conditions 1.–3., then there are $b, c \in p\mathbb{Z}_p$ such that $f_h = (X - \alpha)^2 + b(X - \alpha) + c$ and $\operatorname{ord}_p(D_{\mathrm{pol}}(f_h)) = \operatorname{ord}_p(b^2 - 4c)$, which is 1 if and only if $\operatorname{ord}_p(c) = 1$, independently of the choice of the lift α. □

Theorem 3.15. *Let $P_{n,1}$ denote the probability that a monic polynomial $f \in \mathbb{Z}_p[X]$ of degree n satisfies $\mathrm{ord}_p(D_{\mathrm{pol}}(f)) = 1$. The following table gives $P_{n,1}$ for various n and p.*

	$p = 2$	$p \neq 2$
$n = 2$	0	$p^{-1} - p^{-2}$
$n = 3$	0	$p^{-1} - 2p^{-2} + p^{-3}$
$n \geq 4$	0	$(p-1)^2(1 - (-p)^{-n+2})/(p^2(p+1))$

Proof. From proposition 3.14 we see that whether f satisfies $\mathrm{ord}_p(D_{\mathrm{pol}}(f)) = 1$ depends only on f modulo p^2. So we have

$$P_{n,1} = \frac{1}{p^{2n}} \#\{f \in \mathbb{Z}/p^2\mathbb{Z}[X] : f \text{ monic}, \deg f = n, \mathrm{ord}_p(D_{\mathrm{pol}}(f)) = 1\}.$$

If $p = 2$, then proposition 3.14 tells us that the discriminant being square-free is the same as it being a unit, so $P_{n,1} = 0$.

Now let $p \neq 2$ and let $H(t) = \sum_{n \geq 0} P_{n,1} t^n$. Let $N = \{f \in \mathbb{Z}/p^2\mathbb{Z}[X] : f \text{ monic}\}$ and $N' = \{f \in N : \mathrm{ord}_p(D_{\mathrm{pol}}(f)) = 1\}$. For $h \in I$ linear, let

$$\begin{aligned} N_h &= \{f \in N : \mathrm{ord}_p D_{\mathrm{pol}}(f_h) = 1\}, \\ N_{h,1} &= \{f \in N : h^2 = \bar{f}, f(\alpha) \neq 0\}, \\ N_{h,2} &= \{f \in N : \mathrm{ord}_p D_{\mathrm{pol}}(f) = 0, h \nmid \bar{f}\}. \end{aligned}$$

Then $N' = \bigcup_{h \in I, \deg h = 1} N_h$ and for all h we have a bijection

$$\begin{aligned} N_h &\to N_{h,1} \times N_{h,2} \\ f &\mapsto (f_h, f/f_h). \end{aligned}$$

So we have the following generating function

$$\begin{aligned} \sum_{n \geq 0} P_{n,1} p^{2n} u^n &= \sum_{f \in N'} u^{\deg f} = \sum_{h \in I, \deg h = 1} \sum_{f \in N_h} u^{\deg f} \\ &= \sum_{h \in I, \deg h = 1} \left(\left(\sum_{f \in N_{h,1}} u^{\deg f} \right) \left(\sum_{f \in N_{h,2}} u^{\deg f} \right) \right) \\ &= \sum_{h \in I, \deg h = 1} p\,(p-1)\,u^2 \prod_{g \in I, g \neq h} \left(1 + (pu)^{\deg g}\right), \end{aligned}$$

where we used proposition 3.14 and the proof of proposition 3.11 for the last step.

Setting $u = t/p^2$, we obtain

$$H(t) = \sum_{h \in I, deg_h = 1} t^2 \left(\frac{p-1}{p^3}\right) \prod_{g \in I, g \neq h} \left(1 + \left(\frac{t}{p}\right)^{\deg g}\right).$$

By rewriting this formula and using proposition 3.11 we obtain

$$\begin{aligned} H(t) &= pt^2 \left(\frac{p-1}{p^3}\right)\left(1+\frac{t}{p}\right)^{-1} \prod_{g\in I}\left(1+\left(\frac{t}{p}\right)^{\deg g}\right) \\ &= t^2\left(\frac{p-1}{p^2}\right)\left(1+\frac{t}{p}\right)^{-1}(1-t)^{-1}\left(1-\frac{t^2}{p}\right) \\ &= t^2\frac{p-1}{p^2(p+1)}\left(\frac{p-t^2}{1-t}+\frac{1-\frac{t^2}{p}}{1+\frac{t}{p}}\right), \end{aligned}$$

and the coefficient of t^n is given by

$$P_{n,1} = \begin{cases} \frac{p-1}{p^2(p+1)}(p+1), & n=2, \\ \frac{p-1}{p^2(p+1)}(p-\frac{1}{p}), & n=3, \\ \frac{p-1}{p^2(p+1)}(p-1+\left(\frac{-1}{p}\right)^{n-2}+\left(\frac{-1}{p}\right)^{n-3}), & n\geq 4. \end{cases}$$

□

By combining proposition 3.11 and theorem 3.15, we obtain the probability that $\mathrm{ord}_p D_{\mathrm{pol}}(f) \leq 1$.

	$p=2$	$p\neq 2$
$n=2$	$1/2$	$1-1/p^2$
$n=3$	$1/2$	$1-2/p^2+1/p^3$
$n\geq 4$	$1/2$	$(1-1/p)+\frac{(p-1)^2(1-(-p)^{-n+2})}{(p^2(p+1))}$

If we assume that all these probabilities are independent, then we obtain a heuristic for the probability that a polynomial $f \in \mathbb{Z}[X]$ has square-free discriminant, by taking the product over all p.

For $2 \leq n \leq 7$, table 3b gives approximations for the heuristic probability. It is obtained by calculating the product for primes up to 1 million. It also gives experimental values, which were obtained as the fraction of polynomials with square-free discriminant out of a random set of 1 million polynomials of height at most 10,000. In the last column the experimental value is compared to the heuristic value and then divided by the standard deviation.

For $n = 2$ we can calculate the heuristic probability exactly. It is

$$\frac{1}{2}\prod_{p\neq 2}\left(1-\frac{1}{p^2}\right) = \frac{2}{3}\prod_{p}\left(1-\frac{1}{p^2}\right) = \frac{4}{\pi^2}.$$

The following theorem proves that this value is in fact correct.

degree	heuristic value	experimental value	error/standard deviation
2	0.4052847	0.404588	−1.4191
3	0.3425997	0.342442	−0.3323
4	0.2997226	0.299933	0.4593
5	0.3090905	0.309574	1.0463
6	0.3064416	0.305986	−0.9883
7	0.3072498	0.307041	−0.4526

Table 3b

Theorem 3.16. *The probability that a random monic polynomial in $\mathbb{Z}[X]$ of degree 2 has square-free discriminant is $4/\pi^2$. More exactly,*

$$\#\{(b,c) \in ([-x,x] \times [-x,x]) \cap (\mathbb{Z} \times \mathbb{Z}) : D_{\mathrm{pol}}(X^2 + bX + c) \text{ is square-free}\} = \frac{4}{\pi^2}(2x)^2 + O(x^{7/4}).$$

Proof. Write

$$P(x) = \#\{(b,c) \in ([-x,x] \times [-x,x]) \cap (\mathbb{Z} \times \mathbb{Z}) : D_{\mathrm{pol}}(X^2 + bX + c) \text{ is square-free}\}.$$

If b is even, then $D_{\mathrm{pol}}(X^2+bX+c) = b^2-4c = 0 \bmod 4$, so we only need to consider odd b. Since $D_{\mathrm{pol}}(X^2 + bX + c)$ is square-free if and only if $D_{\mathrm{pol}}(X^2 - bX + c)$ is square-free, it suffices to count the case in which $b > 0$ twice. So we have

$$P(x) = 2\#\{(d,c) \in ([0,(x-1)/2] \times [-x,x]) \cap (\mathbb{Z} \times \mathbb{Z}) : (2d+1)^2 - 4c \text{ is square-free}\}.$$

Now we can use inclusion-exclusion. Since $|(2d+1)^2 - 4c| \le x^2 + 4x < (x+2)^2$, it suffices to do the inclusion-exclusion up to $x+2$. We already dealt with the even n, so the inclusion-exclusion only needs to be done over the odd n. Let $\mu(n)$ denote the Moebius function. Then we have

$$P(x) = 2 \sum_{n=1,\ \text{odd}}^{x+2} \mu(n) A(n),$$

where

$$A(n) = \#\{(d,c) \in ([0,(x-1)/2] \times [-x,x]) \cap (\mathbb{Z} \times \mathbb{Z}) : (2d+1)^2 - 4c = 0 \bmod n^2\}.$$

We split this sum into two parts,

$$Q_1(x) = 2 \sum_{n=1,\ \text{odd}}^{x^{3/4}} \mu(n) A(n)$$

and

$$Q_2(x) = 2 \sum_{n=x^{3/4},\ \text{odd}}^{x+2} \mu(n) A(n).$$

For the first part we observe that we have an element in the set only if $c = 4^{-1}(2d+1)^2 \bmod n^2$. So the number of c is $\left\lfloor \frac{2x+1}{n^2} \right\rfloor$ or this number plus 1. Then we sum over all d to get

$$Q_1(x) = 2 \sum_{n=1,\ \text{odd}}^{x^{3/4}} \mu(n) \left\lfloor \frac{x+1}{2} \right\rfloor \left(\frac{2x+1}{n^2} + B(n) \right),$$

where $|B(n)| \le 1$. Now, $\left\lfloor \frac{x+1}{2} \right\rfloor \left(\frac{2x+1}{n^2} \right) = \frac{x^2}{n^2} + O(x)$. Furthermore,

$$\sum_{n=1,\ \text{odd}}^{x^{3/4}} |\mu(n) \left\lfloor \frac{x+1}{2} \right\rfloor B(n)| < \sum_{n=1,\ \text{odd}}^{x^{3/4}} \left\lfloor \frac{x+1}{2} \right\rfloor = O(x^{7/4}).$$

So

$$Q_1(x) = 2 \sum_{n=1,\ \text{odd}}^{x^{3/4}} \mu(n) \frac{x^2}{n^2} + O(x^{7/4}).$$

To count $Q_2(x)$, we observe that since $(2d+1)^2 - 4c \neq 0$, we need $(2d+1)^2 \ge n^2 + 4c \ge x^{6/4} - 4x$, which can only happen if $d \ge \frac{1}{2}x^{3/4} - x^{1/4} - 1$. So when d is large enough to get a solution, the difference between $(2(d+1)+1)^2$ and $(2d+1)^2$ is at least $4x^{3/4} - 8x^{1/4}$, which is greater than $x^{3/4}$, for x sufficiently large. Around every multiple of n^2, we have an interval of length $8x$ in which $(2d+1)^2$ must lie for solutions to occur. The number of d that can lie in such an interval is at most $8x/x^{3/4} + 1 = 8x^{1/4} + 1$ and the number of intervals is at most $x^2/n^2 + 1 \le x^{2/4} + 1$. So per n, the number of solutions is at most $8x^{3/4} + O(x^{2/4})$. So

$$Q_2(x) \le 2 \sum_{n=x^{3/4},\ \text{odd}}^{x+2} (8x^{3/4} + O(x^{2/4})) < 16x^{7/4} + O(x^{6/4}) = O(x^{7/4}).$$

Now we have

$$P(x) = 2 \sum_{n=1,\ \text{odd}}^{x^{3/4}} \mu(n) \frac{x^2}{n^2} + O(x^{7/4}).$$

We use that

$$\sum_{n=x^{3/4},\ \text{odd}}^{\infty} x^2 \mu(n)/n^2 \le \int_{x^{3/4}-1}^{\infty} x^2/t^2 dt = x^2/(x^{3/4}-1) = O(x^{5/4})$$

to conclude that

$$P(x) = 2x^2 \sum_{n=1,\ \text{odd}}^{\infty} \frac{\mu(n)}{n^2} + O(x^{7/4}).$$

Since

$$\sum_{n=1,\ \text{even}}^{\infty} \mu(n)/n^2 = \sum_{m=1}^{\infty} \mu(2m)/(2m)^2 = -\frac{1}{4} \sum_{m=1,\ \text{odd}}^{\infty} \mu(m)/m^2$$

and

$$\sum_{n=1}^{\infty} \mu(n)/n^2 = 6/\pi^2,$$

we obtain

$$P(x) = 4x^2 \frac{4}{\pi^2} + O(x^{7/4}),$$

and the proof is complete. □

We wish to thank the following people whom we consulted when we were at the beginning of this project: Manjul Bhargava, Henri Cohen, Keith Conrad, Darrin Doud, William Duke, Farshid Hajir, Roger Heath-Brown, John Jones, Hugh Montgomery, David Rohrlich, and Jean-Pierre Serre. Special thanks to Hendrik Lenstra for explaining his heuristic argument to us.

Many thanks to the first referee, who noted in an earlier version that some of our experimental results differed from the heuristic results by several standard deviations. This led us to discover a slight error in our formulas and to report the standard deviations, which are now within respectable limits. Thanks also to the second referee for very helpful suggestions.

The first and third authors wish to thank the National Science Foundation for support of this research through NSF grant number DMS-0139287.

Bibliography

[1] H. Cohen, *A course in computational algebraic number theory*, second corrected printing 1995. New York: Springer, 1993.

[2] W. Fulton, *Intersection theory*, Springer, Berlin, 1997.

[3] S. Lang, *Algebraic number theory*, Reading, MA: Addison-Wesley, 1970.

[4] S. Lang, *Algebra*, third edition, Reading, MA: Addison-Wesley, 1993.

[5] H. Matsumura, *Commutative algebra*, New York: Benjamin, 1970.

[6] B. Poonen, *Squarefree values of multivariable polynomials*, Duke Math. J. **118** (2003), 353–373.

[7] B. L. van der Waerden, *Die Seltenheit der Gleichungen mit Affekt*, Math. Ann. **109** (1934), 13–16.

[8] E. Weiss, *Algebraic number theory*, New York: McGraw-Hill, 1963.

Chapter 4

Cocyclic subrings

The next five chapters will all deal with subrings of commutative rings. This first part will deal with cocyclic subrings. A commutative ring can be viewed as $\mathbb{Z}$-algebra; in that case the cocyclic subrings of a commutative ring A are subrings $R \subset A$ such that $A/R \cong \mathbb{Z}/m\mathbb{Z}$ as groups for some positive integer m. In this chapter we will use a more general view. We will look at commutative Z-algebras A, for some commutative ring Z. Then cocyclic subrings are sub-Z-algebras $R \subset A$ such that $A/R \cong Z/J$ as Z-modules for some Z-ideal J.

There is a link between these subrings and a certain class of A-ideals.

Theorem 4.1. *Let Z be a commutative ring, $J \subset Z$ an ideal and A a commutative Z-algebra. Let W be the set of sub-Z-algebras $R \subset A$ with $A/R \cong Z/J$ as Z-modules, which is a set of certain cocyclic subrings. Let V be the set of A-ideals I with $A/I \cong (Z/J)^2$ as Z-modules. Then the maps*

$$\begin{aligned} f : W &\to V \\ R &\mapsto \{x \in A : xA \subset R\} \end{aligned}$$

and

$$\begin{aligned} g : V &\to W \\ I &\mapsto Z + I \end{aligned}$$

are well-defined and each others two-sided inverse.

We will prove this theorem in the next section. After the proof we will apply it to the maximal order $\mathcal{O}_B$ of a finite étale $\mathbb{Q}_p$-algebra B. For these rings we obtain an upper bound on the number of cocyclic subrings in terms of the degree of B.

4.1 Cocyclic subrings and ideals

In this section we will prove theorem 4.1. To show the well-definedness of the map g we will use the following lemma.

Lemma 4.2. *Let Z be a commutative ring and A a commutative quadratic Z-algebra, that is, an algebra that is free of rank 2 as an Z-module. Then there exists a basis of A over Z containing 1.*

Proof. Let (a_1, a_2) be a basis for A. Write $1 = s_1a_1 + s_2a_2$ with $s_1, s_2 \in Z$. The ideal (s_1, s_2) generated by s_1 and s_2 satisfies $(s_1, s_2)A = A$ and therefore $(s_1, s_2) = Z$. Hence, there exist $t_1, t_2 \in Z$ such that the matrix

$$\begin{pmatrix} s_1 & s_2 \\ t_1 & t_2 \end{pmatrix}$$

is invertible. So $(1, t_1a_1 + t_2a_2)$ is a basis for A. □

For a commutative ring T and a T-module M, we denote the annihilator of M in T by $\mathrm{Ann}_T(M)$.

Proof of theorem 4.1. First, we show the correctness of the maps. For every $R \in W$, the set $f(R) = \mathrm{Ann}_R(A/R)$ is clearly an A-ideal. The isomorphism $\mathrm{End}_Z(A/R) \cong \mathrm{End}_Z(Z/J) \cong Z/J$ shows that the map

$$\begin{aligned} \psi : R &\to \mathrm{End}_Z(A/R) \\ r &\mapsto (a \mapsto ra) \end{aligned}$$

is surjective. We obtain the short exact sequence of Z-modules

$$\begin{aligned} 0 \to f(R) \to R \to \mathrm{End}_Z(A/R) \to 0 \\ \psi : r \mapsto (a \mapsto ra). \end{aligned}$$

In fact, the map ψ is already surjective when restricted to Z, so we obtain $R/f(R) \cong Z/J$. Since we required $A/R \cong Z/J$, we have $JA \subset R$. From this we see $JA \subset f(R)$ and therefore we can view $A/f(R)$ as an Z/J-module. The short exact sequence of Z/J-modules

$$0 \to R/f(R) \to A/f(R) \to A/R \to 0$$

splits because $A/R \cong Z/J$ is free. We obtain $A/f(R) \cong (Z/J)^2$, and therefore $f(R)$ is an ideal of the required type.

For the correctness of g, we note that for each $I \in V$ the set $Z+I$ is equal to $\phi^{-1}\phi(Z)$, where $\phi : A \to A/I$ is the canonical ring morphism. So $Z + I$ is a sub-Z-algebra of A.

By definition, A/I is a quadratic Z/J-algebra. By lemma 4.2, there exists a basis $(1, a)$ of A/I over Z/J. Now, the isomorphism

$$A/(Z + I) = (A/I)/\phi(Z) = (1 \cdot Z/J \oplus a \cdot Z/J)/(1 \cdot Z/J) = a \cdot Z/J \cong Z/J$$

shows that $g(I)$ is a ring of the required type.

Let $I \subset A$ be an ideal with $A/I \cong (Z/J)^2$. From $J = \mathrm{Ann}_Z(A/I)$ it follows that $J \subset Z \cap I$. On the other hand, if $x \in Z \cap I$ is an element, then we have an inclusion $xA \subset I$; this implies $x \in \mathrm{Ann}_Z(A/I) = J$, so $Z \cap I = J$ also holds.

We finish the proof by showing f and g are inverses. Since g is well-defined, $A/(Z+I)$ is isomorphic to Z/J. Combining this with the fact that $Z \cap I = J$, we obtain the Z-linear isomorphism $A/(Z+I) \cong Z/J \cong Z/(Z \cap I) \cong (Z+I)/I$. Since I acts trivially on both $A/(Z+I)$ and $(Z+I)/I$, this is in fact a $Z+I$-linear isomorphism. Hence, for an ideal $I \in V$ we have $fg(I) = \mathrm{Ann}_{Z+I}(A/(Z+I)) = \mathrm{Ann}_{Z+I}((Z+I)/I) = I$.

On the other hand, for each subring $R \in W$, we have the inclusion $gf(R) = Z + f(R) \subset R$, and since Z maps via ψ surjectively to $R/f(R)$, the subrings $gf(R)$ and R are equal. □

4.2 Cocyclic rings for p-adic orders

We will apply theorem 4.1 to the case where $A = \mathcal{O}_E$, the ring of integers of a finite étale $\mathbb{Q}_p$-algebra E, for a prime p. We view this ring as a $\mathbb{Z}_p$-algebra. Each non-zero ideal of $\mathbb{Z}_p$ is generated by some power p^e, and for each of those ideals we can bound the number of cocyclic subrings. The result is the following corollary. Note that the bound is independent of e.

Corollary 4.3. *For every integer $n \in \mathbb{Z}_{>0}$, every prime p, every positive integer e and every finite étale $\mathbb{Q}_p$-algebra E of degree n, the number of sub-$\mathbb{Z}_p$-algebras $R \subset \mathcal{O}_E$ such that $\mathcal{O}_E/R \cong \mathbb{Z}/p^e\mathbb{Z}$ as $\mathbb{Z}_p$-modules is bounded from above by $\binom{n}{2}$.*

Proof. Since the subrings we are looking at are cocyclic, the theorem gives us a bijection between the set of subrings $R \subset \mathcal{O}_E$ with $\mathcal{O}_E/R \cong \mathbb{Z}/p^e\mathbb{Z}$ and the set of ideals $I \subset \mathcal{O}_E$ with $\mathcal{O}_E/I \cong (\mathbb{Z}/p^e\mathbb{Z})^2$. Write $E = \prod_{\mathfrak{m} \in \mathrm{Spec}(E)} E_\mathfrak{m}$ as a product of field extensions of $\mathbb{Q}_p$. Every ideal $I \subset \mathcal{O}_E = \prod_\mathfrak{m} \mathcal{O}_{E_\mathfrak{m}}$ can be written as $I = \prod_\mathfrak{m} I_\mathfrak{m}$, where $I_\mathfrak{m} \subset \mathcal{O}_{E_\mathfrak{m}}$ is an ideal. There are only two ways to obtain an ideal $I \subset \mathcal{O}_E$ with $\mathcal{O}_E/I \cong (\mathbb{Z}/p^e\mathbb{Z})^2$. The first is the kernel of the map $\mathcal{O}_E \to \mathcal{O}_{E_\mathfrak{m}} \to \mathcal{O}_{E_\mathfrak{m}}/I_\mathfrak{m}$, where $I_\mathfrak{m} \subset \mathcal{O}_{E_\mathfrak{m}}$ is an ideal such that $\mathcal{O}_{E_\mathfrak{m}}/I_\mathfrak{m} \cong (\mathbb{Z}/p^e\mathbb{Z})^2$. The other is the kernel of the map $\mathcal{O}_E \to \mathcal{O}_{E_\mathfrak{m}} \times \mathcal{O}_{E'_\mathfrak{m}} \to \mathcal{O}_{E_\mathfrak{m}}/I_\mathfrak{m} \times \mathcal{O}_{E_{\mathfrak{m}'}}/I_{\mathfrak{m}'}$, where $\mathfrak{m}$ and $\mathfrak{m}'$ are different and both $I_\mathfrak{m} \subset \mathcal{O}_{E_\mathfrak{m}}$ and $I_{\mathfrak{m}'} \subset \mathcal{O}_{E_{\mathfrak{m}'}}$ are ideals such that $\mathcal{O}_{E_\mathfrak{m}}/I_\mathfrak{m} \cong \mathbb{Z}/p^e\mathbb{Z}$ and $\mathcal{O}_{E_{\mathfrak{m}'}}/I_{\mathfrak{m}'} \cong \mathbb{Z}/p^e\mathbb{Z}$.

For each $\mathfrak{m} \in \mathrm{Spec}(E)$, the ring $\mathcal{O}_{E_\mathfrak{m}}$ is a discrete valuation ring. The set of ideals $I_\mathfrak{m} \subset \mathcal{O}_{E_\mathfrak{m}}$ such that $\mathcal{O}_{E_\mathfrak{m}}/I_\mathfrak{m}$ is as a $\mathbb{Z}_p$-module isomorphic to a given finite p-group, consists of at most one element. Furthermore, if $E_\mathfrak{m}$ is isomorphic to $\mathbb{Q}_p$, then the set $\{I_\mathfrak{m} \subset \mathcal{O}_{E_\mathfrak{m}} : \mathcal{O}_{E_\mathfrak{m}}/I_\mathfrak{m} \cong (\mathbb{Z}/p^e\mathbb{Z})^2\}$ is empty for all k. If $E_\mathfrak{m}$ is not isomorphic to $\mathbb{Q}_p$, then the degree $\deg(E_\mathfrak{m})$ is at least 2.

Denote by s_1 the number $\#\mathrm{Spec}(E)$ and by s_2 the number $\#\{\mathfrak{m} \in \mathrm{Spec}(E) : \deg(E_\mathfrak{m}) \geq 2\}$. From the inequalities $1 \leq s_1 + s_2 \leq n$ and the previous remarks, we obtain the result

$$\{I \subset \mathcal{O}_E : \mathcal{O}_E/I \cong (\mathbb{Z}/p^e\mathbb{Z})^2\} \leq \binom{s_1}{2} + s_2 \leq \binom{s_1+s_2}{2} \leq \binom{n}{2}. \qquad \square$$

Chapter 5

Subrings of maximal orders

In this chapter K is a number field. We will determine bounds for the number of subrings R of $\mathcal{O}_K$ of given finite additive index m. These bounds depend on the degree of K and the index m.

More precisely, for an integer $n \in \mathbb{Z}_{\geq 2}$ define Nf_n to be the collection of number fields of degree n. Define for each $K \in \mathrm{Nf}_n$ the function $f_K : \mathbb{Z}_{\geq 1} \to \mathbb{Z}$ by

$$f_K(m) = \#\{R \subset \mathcal{O}_K : \ R \text{ is a subring of index } m\}.$$

Note that if $K \in \mathrm{Nf}_n$ and R is a subring of index m of $\mathcal{O}_K$, then $m\mathcal{O}_K \subset R$. Since $\mathcal{O}_K/m\mathcal{O}_K$ is as a group isomorphic to $(\mathbb{Z}/m\mathbb{Z})^n$, the number $f_K(m)$ is bounded from above by the number of subsets of $(\mathbb{Z}/m\mathbb{Z})^n$. This bound depends only on n and m. Hence, the function $f : \mathbb{Z}_{\geq 2} \times \mathbb{Z}_{\geq 1} \to \mathbb{Z}$ defined by

$$f(n,m) = \max_{K \in \mathrm{Nf}_n} \#\{R \subset \mathcal{O}_K : \ R \text{ is a subring of index } m\}$$

is well-defined.

We will study the function f. We are in particular interested in the limit behaviour of $f(n,m)$ for fixed n and $m \to \infty$. The main result of this chapter is the following theorem.

Theorem 5.1. *For an integer $n \geq 2$, define $c_7(n) = \max_{0 \leq d \leq n-1} \frac{d(n-1-d)}{n-1+d}$ and define $c_8(n)$ by the following table.*

n	2	3	4	5	6	7	8	9	10	11	12	13	≥ 14
$c_8(n)$	0	$\frac{1}{3}$	1	$\frac{20}{11}$	$\frac{29}{11}$	$\frac{186}{53}$	$\frac{49}{11}$	$\frac{119}{22}$	$\frac{70}{11}$	$\frac{388}{53}$	$\frac{440}{53}$	$\frac{492}{53}$	$n - \frac{8}{3}$

Then for each integer $n \geq 2$ the inequalities

$$c_7(n) \leq \limsup_{m \to \infty} \frac{\log f(n,m)}{\log m} \leq c_8(n)$$

hold. Furthermore, we have

$$\liminf_{n\to\infty} \frac{1}{n} \limsup_{m\to\infty} \frac{\log f(n,m)}{\log m} \geq 3 - 2\sqrt{2}$$

and

$$\limsup_{n\to\infty} \frac{1}{n} \limsup_{m\to\infty} \frac{\log f(n,m)}{\log m} \leq 1.$$

For $n = 2$ the bounds $c_7(n)$ and $c_8(n)$ are equal. This is a classical result. Indeed, the only subring of $\mathcal{O}_K$ of index m is $\mathbb{Z}+m\mathcal{O}_K$. In [5] Nakagawa studies the Dirichlet series

$$\eta_K(s) = \sum_R (\mathcal{O}_K : R)^{-s}$$

where R runs over all subrings of finite index $(\mathcal{O}_K : R)$. In his introduction, Nakagawa gives a formula for $\eta_K(s)$ in the case where K has degree 3. From the formula we can deduce that the lower bound, $1/3$, is the correct value the case $n = 3$. Nakagawa also gives a hypothesis for a formula in the case where $n = 4$. If this formula is true, we can deduce that $\limsup_{m\to\infty} \frac{\log f(4,m)}{\log m}$ should be $1/2$, equal to $c_7(4)$.

The fact that $c_8(5) < 2$ will be used in chapter 8 to prove a theorem on quintic rings requested by Manjul Bhargava.

In section 5.1, we will prove theorem 5.1 using some auxiliary results. In the rest of this chapter and chapters 6 and 7 we will prove those results.

For $n \geq 3$, the upper bound of theorem 5.1 is different from the lower bound. This can be seen by comparing the following table with the table of upper bounds.

n	2	3	4	5	6	7	8	9	10	11	12	13
$c_7(n)$	0	$\frac{1}{3}$	$\frac{1}{2}$	$\frac{2}{3}$	$\frac{6}{7}$	1	$\frac{6}{5}$	$\frac{15}{11}$	$\frac{20}{13}$	$\frac{12}{7}$	$\frac{15}{8}$	$\frac{35}{17}$

Also $3 - 2\sqrt{2} \approx 0.1716$, the lower bound of the final statement, is smaller than 1, the upper bound. There clearly is room for improvement.

5.1 Articulation of the proof

In this section, we will prove theorem 5.1 from a few results we will prove in later sections.

Vector spaces
For the lower bound, we construct a large set of subrings. We will count that set using the following lemma.

Lemma 5.2. *Let p be a prime and let n and d be integers such that $0 \leq d \leq n$. Then the number of $\mathbb{F}_p$-linear subspaces $V \subset \mathbb{F}_p^n$ of dimension d is*

$$\prod_{i=1}^{d} \frac{p^n - p^{i-1}}{p^d - p^{i-1}}.$$

Furthermore, there exists a constant $c_9 > 0$ such that for all prime numbers p and all integers n and d with $0 \leq d \leq n$, the number $\prod_{i=1}^{d} \frac{p^n - p^{i-1}}{p^d - p^{i-1}}$ is between $p^{d(n-d)}$ and $p^{d(n-d)} + c_9 p^{d(n-d)-1}$.

This lemma will be proven in section 5.2.

Localization

For a prime p and an integer $n \in \mathbb{Z}_{\geq 2}$ define $\mathrm{Et}_{p,n}$ to be the collection of finite étale $\mathbb{Q}_p$-algebras that have degree n.

For a prime p, an algebra $E \in \mathrm{Et}_{p,n}$ and an integer $k \in \mathbb{Z}_{\geq 0}$ define

$$f_E(k) = \#\{R \subset \mathcal{O}_E : R \text{ is a sub-}\mathbb{Z}_p\text{-algebra of index } p^k\}$$

and $f_{\mathrm{Et}}(n, p, k) = \max_{E \in \mathrm{Et}_{p,n}} f_E(k)$.

To prove the upper bounds, we will prove bounds on $f_{\mathrm{Et}}(n, p, k)$, the localized version of $f(n, m)$. The result we obtain locally, immediately gives a similar result globally by the next proposition, which we will prove in section 5.3.

Proposition 5.3. *The following equality holds for all integers $n \geq 2$.*

$$\limsup_{m \to \infty} \frac{\log f(n, m)}{\log m} = \limsup_{p^k \to \infty} \frac{\log f_{\mathrm{Et}}(n, p, k)}{k \log p},$$

where m ranges over the set of positive integers and p^k over the set of prime powers.

Cotype

For a finite étale algebra E, the ring of integers $\mathcal{O}_E$ is free as a $\mathbb{Z}_p$-module. Every subring of $\mathcal{O}_E$ contains $1 \cdot \mathbb{Z}_p$, so there is a natural inclusion of the set of subrings of $\mathcal{O}_E$ to the set of subgroups of $\mathcal{O}_E/\mathbb{Z}_p$. We split the set of subgroups of $\mathcal{O}_E/\mathbb{Z}_p$ of finite index up according to the so-called cotype. For each cotype we will bound the number of subgroups of that cotype, and hence the number of subrings of that cotype.

Definition 5.4. *A* partition λ *is a sequence $(\lambda_i)_{i \in \mathbb{Z}_{>0}}$ of non-negative integers such that $\lambda_i \geq \lambda_{i+1}$ holds for all $i \in \mathbb{Z}_{>0}$ and $\lambda_i \neq 0$ for only finitely many i. Define the* length *of λ to be the number of non-zero coordinates of λ.*

Whenever we write a partition as a finite vector $(\lambda_1, \lambda_2, \ldots, \lambda_n)$, then we mean that $\lambda_i = 0$ for all $i > n$.

For partitions, we will sometimes use a parenthesis notation. The product of two parentheses is concatenation. For example, $(2)^2(1)^3$ denotes the partition $(2, 2, 1, 1, 1)$.

Definition 5.5. *For a prime p and a finite abelian p-group G, define the* type *of G to be the unique partition $(\lambda_1, \ldots, \lambda_d)$ such that G is isomorphic to the group $\bigoplus_{i=1}^{d} \mathbb{Z}/p^{\lambda_i}\mathbb{Z}$.*

Definition 5.6. *Let M be a finitely generated $\mathbb{Z}_p$-module. For a submodule $N \subset M$ of finite index, we define the* cotype *of N to be the type of M/N.*

Note that this is an extension of the definition of cotype in Macdonald [3, chapter II (1.3)–(1.4)]. If μ is the cotype of $N \subset M$, then μ is also the cotype of $N/p^a M \subset M/p^a M$ for any integer $a \geq \mu_1$.

Let M be a free $\mathbb{Z}_p$-module of rank n and let $N \subset M$ be a submodule of finite index. Then the cotype of $N \subset M$ has length at most n. For a partition μ of length at most n, we define

$$S(M, \mu) = \{N \subset M : N \text{ is a submodule of cotype } \mu\}$$

and $u(\mu, n) = \sum_{i=1}^{n}((n + 1 - 2i)\mu_i)$.

The following proposition gives a bound on the number of subgroups, and hence on the number of subrings.

Proposition 5.7. *The set $S(M, \mu)$ satisfies*

$$\#S(M, \mu) = O_n\big(p^{u(\mu,n)}\big),$$

where p ranges over the set of primes, M over the collection of free $\mathbb{Z}_p$-modules of finite rank and μ over the set of partitions of length at most n, the rank of M.

For example, for a cotype $\mu = (e)$, the corresponding submodules are cocyclic. We have the bound $\#S(M, (e)) = O_n\big(p^{u((e),n)}\big) = O_n\big(p^{(n-1)e}\big)$.

We will prove the bound from this proposition, as well as a lower bound for $\#S(M, \mu)$, in section 5.4.

Bound for round rings

The $\mathbb{Z}_p$-module $\mathcal{O}_E/\mathbb{Z}_p$ has rank $n-1$, so every subring of $\mathcal{O}_E$ has a cotype of length at most $n - 1$.

In chapter 4, we have seen that the number of subrings of $\mathcal{O}_E$ of cotype (e) is at most $\binom{n}{2}$. This bound is better than the bound from proposition 5.7. In general, we can obtain better bounds for subrings of cotype $(e)^d$, so called *round* subrings. For integers $e \geq 1$ and $1 \leq d \leq n - 1$, define $W_{e,d}(E)$ to be the set

$$\{R \subset \mathcal{O}_E : R \text{ is a sub-}\mathbb{Z}_p\text{-algebra of cotype } (e)^d\}.$$

Proposition 5.8. *Define for positive integers n the constants $c_{10}(n, 1) = 0$ and $c_{10}(n, 2) = 1$. Furthermore, define for integers n and d with $3 \leq d \leq n - 1$ the constant $c_{10}(n, d) = (d - 1)(n - d - 1)$. Then we can bound*

$$\#W_{e,d}(E) = O_n\big(p^{c_{10}(n,d)}\big),$$

where p ranges over the set of primes, E over the collection of finite étale $\mathbb{Q}_p$-algebras, e over the set of positive integers, d ranges over $\{1, \ldots, \deg(E) - 1\}$ and n is the degree of E.

In chapter 6 we look at extensions of commutative artinian principal ideal rings. In chapter 7 we will apply the theory from chapter 6 to the ring $\mathcal{O}_E/(p^e\mathcal{O}_E)$ and derive the proposition.

Rounding rings

For other, non-round cotypes, we can get bounds for the number of rings of that cotype from the result on round subrings. This is done through a process called *rounding*.

Let E be a finite étale $\mathbb{Q}_p$-algebra and let n be its degree. For a partition λ of length at most $n-1$ define $\tilde{S}(E,\lambda)$ to be the set of sub-$\mathbb{Z}_p$-modules $N \subset \mathcal{O}_E$ of cotype λ with $1 \in N$. Note that $\{R \subset \mathcal{O}_E : R \text{ is a subring of cotype } \lambda\}$ is a subset of $\tilde{S}(E,\lambda)$.

Proposition 5.9. *For each prime p, each integer $n \geq 2$, each finite étale $\mathbb{Q}_p$-algebra E of degree n, each partition λ of length at most $n-1$ and each integer d with $\lambda_d > 2\lambda_{d+1}$, there exists a map*

$$\rho_d : \tilde{S}(E,\lambda) \to \tilde{S}\big(E, (\lambda_d - 2\lambda_{d+1})^d\big)$$

with the following properties:

1. *every fibre of ρ_d has the same cardinality; the number*

$$c_{11}(n,d,\lambda) = -d(n-d-1)(\lambda_d - 2\lambda_{d+1}) + \sum_{i=1}^{n-1}\big((n-2i)\lambda_i\big)$$

   is such that $\#\rho_d^{-1}(N) = O_n\big(p^{c_{11}(n,d,\lambda)}\big)$, where p ranges over the set of primes, E over the collection of finite étale $\mathbb{Q}_p$-algebras, λ over the set of partitions of length at most n, the degree of E, the integer d over integers such that $\lambda_d > 2\lambda_{d+1}$ and N over $\tilde{S}\big(E, (\lambda_d - 2\lambda_{d+1})^d\big)$;

2. *the image under ρ_d of a subring of $\mathcal{O}_E$ is a subring.*

The map ρ_d is the *rounding map*. In section 5.5 we will describe this map and show it has the required properties.

Lower bounds of main theorem

First, we prove the lower bounds of theorem 5.1. Let K be a number field and let n be its degree.

Lemma 5.10. *Every additive subgroup G of $\mathcal{O}_K$ that satisfies $\mathbb{Z} + m^2\mathcal{O}_K \subset G \subset \mathbb{Z} + m\mathcal{O}_K$ for some integer m is a subring.*

Proof. Clearly, 1 is an element of G. Since $G \subset \mathbb{Z}+m\mathcal{O}_K$, we can write any element of G as $x+my$ with $x \in \mathbb{Z}$ and $y \in \mathcal{O}_K$. Let x_1+my_1 and x_2+my_2 be two such elements. Then their product $(x_1+my_1)(x_2+my_2) = x_1x_2 + (mx_1y_2 + mx_2y_1) + m^2y_1y_2$ lies in $\mathbb{Z} + G + m^2\mathcal{O}_K = G$. □

For any number field $K \in \mathrm{Nf}_n$, any prime p and any integer d with $0 \leq d \leq n-1$ we can use the above lemma to bound

$$\#\{R \subset \mathcal{O}_K : R \text{ is a subring of index } p^{n-1+d}\}$$

from below by

$$\begin{aligned}\#\{G \subset \mathcal{O}_K : G \text{ is a subgroup,} \\ \mathbb{Z} + p^2\mathcal{O}_K \subset G \subset \mathbb{Z} + p\mathcal{O}_K, \\ \dim_{\mathbb{F}_p}(G/(\mathbb{Z} + p\mathcal{O}_K)) = d\}.\end{aligned}$$

For a prime p, the vector space $(\mathbb{Z}+p\mathcal{O}_K)/(\mathbb{Z}+p^2\mathcal{O}_K)$ has dimension $n-1$ over $\mathbb{F}_p$. Hence, for each integer d with $0 \leq d \leq n-1$ there exists a bijection between this set of subgroups and the set of $\mathbb{F}_p$-linear subspaces $V \subset \mathbb{F}_p^{n-1}$ of dimension d. By lemma 5.2, this set of subspaces has cardinality at least $p^{d(n-1-d)}$.

Hence, for all n and $0 \leq d \leq n-1$ we have

$$\limsup_{m\to\infty} \frac{\log f(n,m)}{\log m} \geq \limsup_{p\to\infty} \frac{d(n-1-d)\log p}{(n-1+d)\log p}.$$

We obtain $c_7(n)$ as a lower bound by taking the maximum over all d.

The lower bound of the final statement of the theorem is proven by

$$\begin{aligned}\lim_{n\to\infty} \frac{1}{n} \max_{0\leq d\leq n-1} \frac{d(n-1-d)}{n-1+d} &= \lim_{n\to\infty} \frac{n-1}{n} \max_{0\leq d\leq n-1} \frac{\frac{d}{n-1}(1-\frac{d}{n-1})}{1+\frac{d}{n-1}} \\ &= \max_{x\in[0,1]} \frac{x(1-x)}{1+x} \\ &= 3-2\sqrt{2}.\end{aligned}$$

Upper bounds of main theorem

Now, we will prove the upper bounds of theorem 5.1. By proposition 5.3, it suffices to show the upper bounds for $f_{\mathrm{Et}}(n,p,k)$. For this local version, we set up an integer linear program.

For an integer $n \geq 1$ and a vector $\lambda \in \mathbb{Z}^{n-1}$, define the constant

$$c_{12}(n,0,\lambda) = \sum_{i=1}^{n-1}((n-2i)\lambda_i).$$

For an integer n with $n \geq 1$, a vector $\lambda \in \mathbb{Z}^{n-1}$ and an integer d with $1 \leq d \leq n-2$ define the constant

$$c_{12}(n,d,\lambda) = c_{10}(n,d) - d(n-d-1)(\lambda_d - 2\lambda_{d+1}) + \sum_{i=1}^{n-1}((n-2i)\lambda_i),$$

with $c_{10}(n,d)$ as defined in proposition 5.8.

Theorem 5.11. *Let $n \geq 1$ be an integer. Suppose $r \in \mathbb{R}$ is such that there is no integral solution $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_{n-1})$ to the following system of linear inequalities.*

$$\begin{aligned} c_{12}(n,d,\lambda) &\geq r \sum_{i=1}^{n-1} \lambda_i && \text{for } d = 0, \ldots, n-2 \\ \lambda_d &\geq \lambda_{d+1} && \text{for } d = 1, \ldots, n-2 \\ \lambda_{n-1} &\geq 0 \\ \sum_{i=1}^{n-1} \lambda_i &\geq 1 \end{aligned} \tag{5.12}$$

Then we can bound

$$\limsup_{p^k \to \infty} \frac{\log f_{\mathrm{Et}}(n,p,k)}{k \log p} \leq r.$$

To prove the previous theorem, we will first combine all the bounds from the auxiliary results.

Lemma 5.13. *We can bound*

$$f_E(\lambda) = \#\{R \subset \mathcal{O}_E : \ R \text{ is a subring of cotype } \lambda\} = O_n\big(p^{c_{12}(n,d,\lambda)}\big),$$

where p ranges over the set of primes, E over the collection of finite étale $\mathbb{Q}_p$-algebras, λ over the set of all partitions of length at most $\deg(E) - 1$ and d over $\{0, \ldots, \deg(E) - 2\}$, and where n is the degree of E.

Proof. By proposition 5.7, we have $f_E(\lambda) \leq \#S(\mathcal{O}_E/\mathbb{Z}_p, \lambda) = O_n\big(p^{u(\lambda, n-1)}\big)$. Noting that $u(\lambda, n-1) = c_{12}(n, 0, \lambda)$ proves the case $d = 0$.

If $d > 0$ and $\lambda_d - 2\lambda_{d+1} \leq 0$, then the inequality $c_{12}(n,d,\lambda) \geq c_{12}(n,0,\lambda)$ holds. Hence, we are done in that case as well.

In the final case $d > 0$ and $e = \lambda_d - 2\lambda_{d+1} > 0$. Define the partition $\mu = (e)^d$. By the second property of the rounding map (see proposition 5.9) every ring $R \subset \mathcal{O}_E$ of cotype λ can be rounded to a ring of cotype μ.

If there exists no ring of cotype μ, then there are also no rings of cotype λ. We obtain $f_E(\lambda) = 0 = O_n\big(p^{c_{12}(n,d,\lambda)}\big)$

If there exists a ring of cotype μ, denote by R_μ such a ring. By the first property of the rounding map and proposition 5.8, we can bound

$$\begin{aligned} f_E(\lambda) &\leq \#W_{e,d}(E) \cdot \#\rho_d^{-1}(R_\mu) \\ &\leq O_n\big(p^{c_{10}(n,d)}\big) O_n\big(p^{c_{11}(n,d,\lambda)}\big) \\ &= O_n\big(p^{c_{12}(n,d,\lambda)}\big), \end{aligned}$$

which proves the last case. □

Proof of theorem 5.11. By lemma 5.13, there exists for each integer n a constant $c_{13}(n)$ such that for all primes p, all finite étale $\mathbb{Q}_p$-algebras E of degree n, all partitions λ of length at most $n-1$ and all integers d with $0 \leq d \leq n-2$, we have $f_E(\lambda) \leq c_{13}(n)p^{c_{12}(n,d,\lambda)}$. We can combine this to the bound $f_E(\lambda) \leq \min_{0\leq d\leq n-2} c_{13}(n)p^{c_{12}(n,d,\lambda)}$.

We denote the set of partitions λ of size k and length $n-1$ by $\Lambda_n(k)$. We see that

$$\begin{aligned} f_{\mathrm{Et}}(n,p,k) &= \max_{E\in \mathrm{Et}_{p,n}} \max_{\lambda\in\Lambda_n(k)} f_E(\lambda) \\ &\leq \max_{\lambda\in\Lambda_n(k)} \min_{0\leq d\leq n-2} (c_{13}(n)p^{c_{12}(n,d,\lambda)}) \\ &\leq c_{13}(n) \max_{\lambda\in\Lambda_n(k)} \min_{0\leq d\leq n-2} p^{c_{12}(n,d,\lambda)}. \end{aligned}$$

We obtain the bound

$$\begin{aligned} \limsup_{p^k\to\infty} \frac{\log f_{\mathrm{Et}}(n,p,k)}{k\log p} &\leq \limsup_{p^k\to\infty} \left(\frac{\log c_{13}(n)}{k\log p} + \max_{\lambda\in\Lambda_n(k)} \min_{0\leq d\leq n-2} \frac{c_{12}(n,d,\lambda)}{k} \right) \\ &= \limsup_{p^k\to\infty} \max_{\lambda\in\Lambda_n(k)} \min_{0\leq d\leq n-2} \frac{c_{12}(n,d,\lambda)}{\sum_{i=1}^{n-1}\lambda_i} \\ &= \sup_{\lambda\in\bigcup_{k=1}^{\infty}\Lambda_n(k)} \min_{0\leq d\leq n-2} \frac{c_{12}(n,d,\lambda)}{\sum_{i=1}^{n-1}\lambda_i}. \end{aligned}$$

Suppose $\limsup_{p^k\to\infty} \frac{\log f_{\mathrm{Et}}(n,p,k)}{k\log p} = r+\epsilon > r$ holds. Then there exists a non-zero partition λ of length at most $n-1$ such that $\min_{0\leq d\leq n-2} \frac{c_{12}(n,d,\lambda)}{\sum_{i=1}^{n-1}\lambda_i} > r+\frac{\epsilon}{2}$. Clearly, $(\lambda_i)_{i=1}^{n-1}$ is a solution of system (5.12). □

If r is as in theorem 5.11, then we obtain $\limsup_{m\to\infty} \frac{\log f(n,m)}{\log m} \leq r$ by proposition 5.3. For $n=2$ every partition gives the same bound, namely $r=0$. For $n=3$ and $n=4$ system (5.12) is analysed in the following lemma.

Lemma 5.14. *For $n=3$ system (5.12) has no solutions for r with $r>1/3$. It does have solutions for $r=1/3$.*

For $n=4$ system (5.12) has no solutions for r with $r>1$. It does have solutions for $r=1$.

Proof. Suppose that for $n=3$ the partition λ is a solution with r for $r>1/3$. The first inequality for $d=0$ is $\lambda_1-\lambda_2 \geq r(\lambda_1+\lambda_2) > 1/3(\lambda_1+\lambda_2)$. This can be rewritten as $\lambda_1 > 2\lambda_2$. The first inequality for $d=1$ is $-(\lambda_1-2\lambda_2)+\lambda_1-\lambda_2 \geq r(\lambda_1+\lambda_2) > 1/3(\lambda_1+\lambda_2)$. This can be rewritten as $2\lambda_2 > \lambda_1$. This contradicts $\lambda_1 > 2\lambda_2$ and therefore proves the first claim.

As can be seen from this, for $r=1/3$, the only possible solutions are of the form $(2\lambda_2, \lambda_2)$. Indeed, all these partitions are solutions for system (5.12).

n	$c_8(n)$	$\lambda(n)$
2	0	(1)
3	1/3	(2,1)
4	1	(2,1,0)
5	20/11	(7,3,1,0)
6	29/11	(7,3,1,0,0)
7	186/53	(31,14,6,2,0,0)
8	49/11	(12,6,3,1,0,0,0)
9	119/22	(12,6,3,1,0,0,0,0)
10	70/11	(12,6,3,1,0,0,0,0,0)
11	388/53	(28,14,7,3,1,0,0,0,0,0)
12	440/53	(28,14,7,3,1,0,0,0,0,0,0)
13	492/53	(28,14,7,3,1,0,0,0,0,0,0,0)

Table 5a. Optimal solutions to system (5.12) for small n.

Suppose that for $n = 4$ the partition λ is a solution with r for $r > 1$. The first inequality for $d = 1$ is $-2(\lambda_1 - 2\lambda_2) + 2\lambda_1 - 2\lambda_3 \geq r(\lambda_1 + \lambda_2 + \lambda_3) > \lambda_1 + \lambda_2 + \lambda_3$. This can be rewritten as $3\lambda_2 > \lambda_1 + 3\lambda_3$. The first inequality for $d = 2$ is $1 - 2(\lambda_2 - 2\lambda_3) + 2\lambda_1 - 2\lambda_3 \geq r(\lambda_1 + \lambda_2 + \lambda_3) > \lambda_1 + \lambda_2 + \lambda_3$. This can be rewritten as $1 + \lambda_1 + \lambda_3 > 3\lambda_2$. Since every λ_i is an integer, we can conclude $\lambda_1 + \lambda_3 \geq 3\lambda_2$.

Combining these inequalities, we get $\lambda_1 + \lambda_3 \geq 3\lambda_2 > \lambda_1 + 3\lambda_3$. This can only happen when λ_3 is negative, contradicting the third inequality of the system. This shows the third claim of the lemma.

For $r = 1$, we obtain the inequality $1 + \lambda_1 + \lambda_3 \geq 3\lambda_2 \geq \lambda_1 + 3\lambda_3$. This can only occur when $\lambda_3 = 0$ and either $\lambda_1 = 3\lambda_2$ or $\lambda_1 = 3\lambda_2 - 1$. Indeed, the partitions $(3\lambda_2, \lambda_2, 0)$ and $(3\lambda_2 - 1, \lambda_2, 0)$ are solutions to the system for $r = 1$. □

For a fixed n and r, system (5.12) is an integer linear program without objective. If we add an objective, a computer program can check whether there is a solution for that r, and, by varying the objective, can check whether the solution is unique. When a partition is a solution for the linear program with a fixed r_0, it is also a solution for $r < r_0$. Hence, when we find a unique solution λ for a number r, we can use that solution to find the maximum r for with system (5.12) has a solution, namely the largest r for which λ is a solution.

For $5 \leq n \leq 13$, it turns out that there exists a number r for which system (5.12) has a unique solution. In table 5a the column $c_8(n)$ states the largest value for r for which system (5.12) has an integral solution. These values are the upper bounds from theorem 5.1. The partition $\lambda(n)$ is a solution for the system with $r = c_8(n)$; it is unique for $5 \leq n \leq 13$.

The upper bound for $n \geq 14$, as well as the upper bound for the final statement of theorem 5.1 follow from the following proposition.

Proposition 5.15. *Let $n \geq 5$ be an integer. Then system* (5.12) *does not have any solutions for $r > n - \frac{8}{3}$.*

Proof. For ease of notation, write $\alpha = \frac{4}{3}$. Suppose $\lambda = (\lambda_1, \ldots, \lambda_{n-1})$ is a solution for system (5.12) for some $r > n - 4 + \alpha$. Write $A = \sum_{i=1}^{n-1} \lambda_i$.

In case $\lambda_1 \leq \frac{\alpha}{2} A$ we obtain

$$c_{12}(n, 0, \lambda) = \sum_{i=1}^{n-1} \big((n-2i)\lambda_i\big) \leq 2\lambda_1 + \sum_{i=1}^{n-1} \big((n-4)\lambda_i\big) \leq \alpha A + (n-4)A < rA,$$

which is a contradiction with the first equation of the system for $d = 0$. If $\lambda_1 > \frac{\alpha}{2} A$ and $\lambda_2 \leq \frac{\alpha}{4} A$ hold, then we have the inequality

$$\begin{aligned} c_{12}(n, 1, \lambda) &= -(\lambda_1 - 2\lambda_2)(n-2) + \sum_{i=1}^{n-1} \big((n-2i)\lambda_i\big) \\ &\leq -(n-4)\lambda_1 + 2(n-2)\lambda_2 + \sum_{i=1}^{n-1} \big((n-4)\lambda_i\big) \\ &\leq -(n-4)\frac{\alpha}{2} A + 2(n-2)\frac{\alpha}{4} A + (n-4)A \\ &= (\alpha + n - 4)A \\ &< rA. \end{aligned}$$

This is a contradiction with the first equation of the system for $d = 1$. For the final case where $\lambda_1 > \frac{\alpha}{2} A$ and $\lambda_2 > \frac{\alpha}{4} A$, the inequality $\lambda_1 + \lambda_2 > \frac{\alpha}{2} A + \frac{\alpha}{4} A = A$ contradicts the λ_i being non-negative. □

Since $\lim_{n \to \infty} \frac{n - 8/3}{n} = 1$ holds, this finishes the proof of theorem 5.1.

5.2 Vector spaces

In this section we will prove lemma 5.2, restated below for convenience.

Lemma 5.2. *Let p be a prime and let n and d be integers such that $0 \leq d \leq n$. Then the number of $\mathbb{F}_p$-linear subspaces $V \subset \mathbb{F}_p^n$ of dimension d is*

$$\prod_{i=1}^{d} \frac{p^n - p^{i-1}}{p^d - p^{i-1}}.$$

Furthermore, there exists a number $c_9 > 0$ such that for all prime numbers p and all integers n and d with $0 \leq d \leq n$, the number $\prod_{i=1}^{d} \frac{p^n - p^{i-1}}{p^d - p^{i-1}}$ is between $p^{d(n-d)}$ and $p^{d(n-d)} + c_9 p^{d(n-d)-1}$.

Proof. The number of ordered independent sets in $\mathbb{F}_p^n$ of cardinality d is equal to $\prod_{i=1}^{d}(p^n - p^{i-1})$. Each subspace V of dimension d is generated by $\prod_{i=1}^{d}(p^d - p^{i-1})$ of those sets. So the number of $\mathbb{F}_p$-linear subspaces $V \subset \mathbb{F}_p^n$ of dimension d is

$$\prod_{i=1}^{d} \frac{p^n - p^{i-1}}{p^d - p^{i-1}}.$$

Taking the logarithm and using the Taylor expansion $\log(1-y) = -\sum_{j=1}^{\infty} \frac{y^j}{j}$, which converges for $|y| < 1$, we get

$$\begin{aligned}
\log\left(\prod_{i=1}^{d} \frac{p^n - p^{i-1}}{p^d - p^{i-1}}\right) &= \log\left(p^{d(n-d)} \prod_{i=0}^{d-1} \frac{1-p^{i-n}}{1-p^{i-d}}\right) \\
&= \log(p^{d(n-d)}) + \sum_{i=0}^{d-1} \left(\log(1-p^{i-n}) - \log(1-p^{i-d})\right) \\
&= \log(p^{d(n-d)}) + \sum_{i=0}^{d-1} \sum_{j=1}^{\infty} \frac{-p^{(i-n)j} + p^{(i-d)j}}{j} \\
&= \log(p^{d(n-d)}) + \sum_{j=1}^{\infty} \frac{\sum_{i=0}^{d-1} p^{ij}(p^{-dj} - p^{-nj})}{j} \\
&= \log(p^{d(n-d)}) + \sum_{j=1}^{\infty} \frac{\frac{p^{dj}-1}{p^j-1}(p^{-dj} - p^{-nj})}{j}.
\end{aligned}$$

Using the bounds $1 \leq \frac{p^{dj}-1}{p^j-1} < p^{dj}\frac{1}{p^j-1} \leq p^{dj}2p^{-j}$ and $0 \leq p^{-dj} - p^{-nj} < p^{-dj}$, we can bound this from below by $\log(p^{d(n-d)})$ and from above by $\log(p^{d(n-d)}) + \sum_{j=1}^{\infty} \frac{2p^{-j}}{j} = \log(p^{d(n-d)}) + \log((1-p^{-1})^{-2}) \leq \log(p^{d(n-d)}) + \log(1+6p^{-1})$. □

5.3 Localization

In this section, we will show that the function f, defined in the introduction of this chapter, is multiplicative in m and that it therefore suffices to determine only $f(n, p^k)$ for prime powers p^k. Furthermore, the number of subrings of $\mathcal{O}_K$ of prime power index p^k can be determined from the localization $K \otimes \mathbb{Q}_p$.

The goal of this section is to prove proposition 5.3, which was stated in section 5.1. A tool we will use is a weak approximation theorem for the field $\mathbb{Q}$. This theorem is useful in proving the results for all number fields and finite étale $\mathbb{Q}_p$-algebras, from the results on specific ones. That is, we use it to link the functions f and f_K, from the introduction to the functions f_{Et} and f_E, defined in section 5.1.

5.3.1 Weak approximation

In this section we state and prove a weak approximation theorem for the field $\mathbb{Q}$. We will use the following lemma, which is a variant of Krasner's lemma.

Let L be a field with a discrete valuation $v : L^* \to \mathbb{Z}$. Let $|.|$ be an absolute value corresponding to this valuation. For polynomials $g, h \in L[X]$, we define the distance between g and h as $|g - h| = \max_i |g_i - h_i|$, where $g = \sum_i g_i X^i$ and $h = \sum_i h_i X^i$.

Lemma 5.16. *Let L be a field with a discrete valuation. Suppose L is complete with respect to this valuation. Let $g \in L[X]$ be a separable, monic polynomial. Then there exists $\delta(g) > 0$ such that for any monic polynomial $h \in L[X]$ of the same degree as g with $|g - h| < \delta(g)$, the polynomial h is also separable and $L[X]/(g)$ and $L[X]/(h)$ are isomorphic as L-algebras.*

Proof. [6, lemma 5.5]. □

Now we state and prove a weak approximation theorem for the field $\mathbb{Q}$.

Lemma 5.17. *Let $n \geq 1$ be an integer and let P be a finite set of prime numbers. For $p \in P$, let E_p be a finite étale $\mathbb{Q}_p$-algebra of degree n. Then there exists a number field K of degree n such that for all $p \in P$ the $\mathbb{Q}_p$-algebra $K \otimes \mathbb{Q}_p$ is isomorphic to E_p.*

Proof. Let p be a prime in P. If E_p is a finite étale $\mathbb{Q}_p$-algebra, then we can write $E_p = \prod_{i \in I(p)} E_{p,i}$, where each $E_{p,i}$ is a finite field extension of $\mathbb{Q}_p$ and $I(p)$ is a finite set. For each of the fields $E_{p,i}$ there exists a separable, irreducible, monic polynomial $g_{p,i} \in \mathbb{Z}_p[X]$ such that $E_{p,i} \cong \mathbb{Q}_p[X]/(g_{p,i})$. When some $g_{p,i}$ are equal, we can, by lemma 5.16, modify them slightly such that they are different but still satisfy $E_{p,i} \cong \mathbb{Q}_p[X]/(g_{p,i})$. Then the product $g_p = \prod_{i \in I(p)} g_{p,i}$ is also separable. Note that E_p is isomorphic to $\mathbb{Q}_p[X]/(g_p)$ and hence g_p has degree n.

Next, we take a prime q not in P and let $\tilde{g}_q \in \mathbb{F}_q[X]$ be a monic irreducible polynomial of degree n. Let $g_q \in \mathbb{Q}_q[X]$ be a lift of $\tilde{g}_q$. Define the algebra $E_q = \mathbb{Q}_q[X]/(g_q)$. Since g_q is irreducible, E_q is a field extension of $\mathbb{Q}_q$ of degree n.

The set P is finite, so by the Chinese remainder theorem we can choose a monic polynomial $h \in \mathbb{Z}[X]$ such that for all $p \in P \cup \{q\}$ we have $|g_p - h| \leq \delta(g_p)$ in $\mathbb{Q}_p[X]$. Applying lemma 5.16 for each $p \in P \cup \{q\}$ to g_p and h, we see $(\mathbb{Q}[X]/(h)) \otimes \mathbb{Q}_p \cong E_p$. The polynomial h is irreducible, since it is irreducible over $\mathbb{Q}_q$. Hence, $K = \mathbb{Q}[X]/(h)$ satisfies the requirements. □

5.3.2 Local rings of integers

In this section, we will establish the connection between $f_K(p^k)$ and the corresponding function $f_{K \otimes_{\mathbb{Q}} \mathbb{Q}_p}(k)$. From this and the weak approximation, we will deduce that for all n, p and k, the equality $f(n, p^k) = f_{\mathrm{Et}}(n, p, k)$ holds.

Lemma 5.18. *Let K be a number field. Then there exists a ring isomorphism $\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong \mathcal{O}_{K \otimes_{\mathbb{Q}} \mathbb{Q}_p}$.*

Proof. Since $\mathbb{Z}_p$ is torsion-free over $\mathbb{Z}$, the ring morphism $\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p \to K \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is injective. Furthermore, there exists a ring isomorphism $K \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong K \otimes_{\mathbb{Q}} \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong K \otimes_{\mathbb{Z}} \mathbb{Z}_p$. Hence, we have a natural injective ring morphism $\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p \to K \otimes_{\mathbb{Q}} \mathbb{Q}_p$. Every element of $\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is integral over $\mathbb{Z}_p$, so the image of this map lies in $\mathcal{O}_{K \otimes_{\mathbb{Q}} \mathbb{Q}_p}$.

Next, we can write $K \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong \prod_{\mathfrak{p}|p} K_{\mathfrak{p}}$, where $K_{\mathfrak{p}}$ is the completion of K at $\mathfrak{p}$. Hence, the ring of integers of $K \otimes_{\mathbb{Q}} \mathbb{Q}_p$ is $\prod \mathcal{O}_{K_{\mathfrak{p}}}$. From [7, 4-8-13] we see that the discriminant of $\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p$ over $\mathbb{Z}_p$ is equal to the product over all $\mathfrak{p}$ that extend p of the discriminant of $\mathcal{O}_{K_{\mathfrak{p}}}$ over $\mathbb{Z}_p$. Hence the injection $\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p \hookrightarrow \prod \mathcal{O}_{K_{\mathfrak{p}}}$ is a bijection. □

Proposition 5.19. *For all number fields $K \in \mathrm{Nf}_n$ and prime powers p^k we have the equality $f_K(p^k) = f_{K \otimes \mathbb{Q}_p}(k)$.*

Proof. An easy verification shows that the map from the set of subrings $R \subset \mathcal{O}_K$ of index $(\mathcal{O}_K : R) = p^k$ to the set of sub-$\mathbb{Z}_p$-algebras $S \subset \mathcal{O}_K \otimes \mathbb{Z}_p$ of index $(\mathcal{O}_K \otimes \mathbb{Z}_p : S) = p^k$ that sends a subring R to the subalgebra $R \otimes \mathbb{Z}_p$, is a well-defined bijection. Lemma 5.18 gives the isomorphism $\mathcal{O}_K \otimes \mathbb{Z}_p \cong \mathcal{O}_{K \otimes \mathbb{Q}_p}$. Counting these sets gives the result $f_K(p^k) = f_{K \otimes \mathbb{Q}_p}(k)$. □

Proposition 5.20. *For all n, p and k, we have $f(n, p^k) = f_{\mathrm{Et}}(n, p, k)$.*

Proof. Let $K \in \mathrm{Nf}_n$ be such that $f(n, p^k) = f_K(p^k)$. Then by proposition 5.19, we can bound

$$f(n, p^k) = f_K(p^k) = f_{K \otimes \mathbb{Q}_p}(k) \leq f_{\mathrm{Et}}(n, p, k).$$

On the other hand, let $E \in \mathrm{Et}_{p,n}$ be such that $f_{\mathrm{Et}}(n, p, k) = f_E(k)$. From lemma 5.17, we know there exists a number field K such that $K \otimes \mathbb{Q}_p \cong E$. Hence, we also have the bound

$$f_{\mathrm{Et}}(n, p, k) = f_E(k) = f_{K \otimes \mathbb{Q}_p}(k) = f_K(p^k) \leq f(n, p^k).$$

□

5.3.3 Multiplicativity

In this section, we will prove the multiplicativity of f and proposition 5.3. We start by showing that f_K is multiplicative.

Lemma 5.21. *Let K be a number field. The function $f_K : \mathbb{Z}_{>0} \to \mathbb{Z}_{\geq 0}$ defined by*

$$f_K(m) = \#\{R \subset \mathcal{O}_K \text{ subring} : (\mathcal{O}_K : R) = m\}$$

is multiplicative.

Proof. For each integer m, define the set $V_m = \{R \subset \mathcal{O}_K \text{ subring} : (\mathcal{O}_K : R) = m\}$. For relatively prime, positive integers m_1 and m_2, define the map

$$\begin{aligned} \phi : V_{m_1} \times V_{m_2} &\to V_{m_1 m_2} \\ (R_1, R_2) &\mapsto R_1 \cap R_2. \end{aligned}$$

The reader can easily verify that this map is well-defined and that it is a bijection. Therefore we have $f_K(m_1 m_2) = f_K(m_1) f_K(m_2)$. □

Proposition 5.22. *The function $f(n, m)$ is multiplicative in m.*

Proof. Let m_1 and m_2 be relatively prime positive integers and let P be the set of all prime divisors of $m_1 m_2$. For $i = 1, 2$, let K_i be a number field that attains the maximum value for $f_K(m_i)$.

For each prime p in P with $p \mid m_i$, define $E_p = K_i \otimes \mathbb{Q}_p$. According to lemma 5.17, there exists a number field K such that $K \otimes \mathbb{Q}_p \cong E_p$ for all $p \in P$. For $i = 1, 2$ and $p^k \mid m_i$, we have $f_K(p^k) = f_{K \otimes \mathbb{Q}_p}(k) = f_{K_i \otimes \mathbb{Q}_p}(k) = f_{K_i}(p^k)$ by proposition 5.19. By lemma 5.21, we get $f_K(m_i) = f_{K_i}(m_i) = f(n, m_i)$ and therefore $f(n, m_1 m_2) \geq f_K(m_1 m_2) = f(n, m_1) f(n, m_2)$.

On the other hand let K' be a number field of degree n that attains the maximum value for $f_K(m_1 m_2)$. Then we also have the bound

$$f(n, m_1 m_2) = f_{K'}(m_1 m_2) = f_{K'}(m_1) f_{K'}(m_2) \leq f(n, m_1) f(n, m_2).$$

□

Now we prove proposition 5.3, restated here for convenience.

Proposition 5.3. *The following equality holds for all n.*

$$\limsup_{m \to \infty} \frac{\log f(n, m)}{\log m} = \limsup_{p^k \to \infty} \frac{\log f_{\mathrm{Et}}(n, p, k)}{k \log p}$$

Proof. From proposition 5.20 we know

$$\limsup_{p^k \to \infty} \frac{\log f_{\mathrm{Et}}(n, p, k)}{k \log p} = \limsup_{p^k \to \infty} \frac{\log f(n, p^k)}{\log p^k} = x.$$

The set of prime powers is a subset of the integers, so we can bound

$$x \leq \limsup_{m \to \infty} \frac{\log f(n, m)}{\log m}.$$

Hence, if x is infinite, we are done.

Assume x is finite. Then for all $\epsilon > 0$ we have $\lim_{p^k \to \infty} \frac{f(n,p^k)}{p^{k(x+\epsilon)}} = 0$. Since f is multiplicative, we can use [1, theorem 316] to obtain $\lim_{m\to\infty} \frac{f(n,m)}{m^{x+\epsilon}} = 0$. This implies $\limsup_{m\to\infty} \frac{\log f(n,m)}{\log m} < x + \epsilon$ for all $\epsilon > 0$. Hence, we also have the bound

$$\limsup_{m\to\infty} \frac{\log f(n,m)}{\log m} \leq x.$$

□

5.4 Counting submodules

In this section, we will prove proposition 5.7, stated in section 5.1. We start by stating a more general version of the proposition. We will use the extra statement in section 5.5.

Recall the definition of $u(\mu, n) = \sum_{i=1}^{n}((n+1-2i)\mu_i)$.

Proposition 5.23. *The set $S(M,\mu)$ defined in section 5.1, satisfies*

$$\#S(M,\mu) = O_n\left(p^{u(\mu,n)}\right)$$

and

$$\frac{1}{\#S(M,\mu)} = O_n\left(p^{-u(\mu,n)}\right),$$

where p ranges over the set of primes, M over the free $\mathbb{Z}_p$-modules of finite rank and μ over the partitions of length at most n, the rank of M.

One could use the theory of Hall polynomials to show that there exists a monic polynomial $g_{\mu,n} \in \mathbb{Z}[X]$, depending on the partition μ and the rank n, of degree $u(\mu,n)$ such that for all primes p we have $\#S(M,\mu) = g_{\mu,n}(p)$. The existence of such a polynomial would prove the first part of the proposition. For example, a book by Macdonald [3, chapter I–II] states the theory necessary for such an approach. The second statement follows from the fact that the polynomials $g_{\mu,n}(p)$ have non-negative coefficients when expanded in powers of $p-1$, see [4]. It follows that for every prime p and every partition μ of length at most n the inequality $g_{\mu,n}(p) > 0$ holds.

Note that we could explicitly find the exact polynomials as indicated after the proof of [3, chapter II (4.1)]. One could, in theory, use these explicit polynomials through this entire chapter to derive more precise statements. This would, however, involve a lot of calculations.

We will give a different proof using the following observation.

For a prime p and a partition μ, let $A_{\mu,p}$ be a finite abelian p-group of type μ, see definition 5.5. Then for free $\mathbb{Z}_p$-modules M of rank at least the length of μ, there exists a bijection

$$S(M,\mu) \cong \frac{\{\phi : M \to A_{\mu,p} \text{ surjective}\}}{\mathrm{Aut}(A_{\mu,p})}.$$

This follows from the fact that every $N \in S(M,\mu)$ is the kernel of such a surjective map. Two kernels are the same if and only if the maps differ by an automorphism of $A_{\mu,p}$. We will use this fact to bound $\#S(M,\mu)$ by giving upper and lower bounds for both $\#\{\phi : M \to A_{\mu,p} \text{ surjective}\}$ and $\#\mathrm{Aut}(A_{\mu,p})$.

Lemma 5.24. *For every prime p, every positive integer n, every free $\mathbb{Z}_p$-module M of rank n and every partition μ of length at most n, the following inequalities hold.*

$$1 - \frac{p^n - 1}{p^n(p-1)} \leq \frac{\#\{\phi : M \twoheadrightarrow A_{\mu,p}\}}{(\#A_{\mu,p})^n} \leq 1$$

Proof. To give a morphism $\phi : M \to A_{\mu,p}$, it suffices to give the map on a set of generators. Therefore, the number of such maps is $(\#A_{\mu,p})^n$, which is an upper bound for the number of surjective maps.

For the lower bound, we first note that a surjective map $M \to A_{\mu,p}$ exists, since the number of generators of $A_{\mu,p}$ is at most n. Let ψ be such a surjective map.

If a morphism $\phi : M \to A_{\mu,p}$ is not surjective, its image lies in a maximal subgroup of $A_{\mu,p}$, that is, one of index p. Let $\mathrm{Subgr}_p(A)$ and $\mathrm{Subgr}_p(M)$ be the set of subgroups of index p of A and M respectively. We see that

$$\#\{\phi : M \to A_{\mu,p} \text{ not surjective}\} \leq \# \coprod_{B \in \mathrm{Subgr}_p(A)} \{\phi : M \to B\} = \sum_{B \in \mathrm{Subgr}_p(A)} (\#B)^n.$$

If $B \in \mathrm{Subgr}_p(A)$ is a subgroup, then $\psi^{-1}(B) \subset M$ is a subgroup of index p. Furthermore, since ψ is surjective, the map

$$\begin{aligned} \mathrm{Subgr}_p(A) &\to \mathrm{Subgr}_p(M) \\ B &\mapsto \psi^{-1}(B) \end{aligned}$$

is injective. Hence, we can bound $\#\mathrm{Subgr}_p(A)$ from above by $\#\mathrm{Subgr}_p(M)$. Since $\mathrm{Subgr}_p(M) = S(M,(1))$, we can use the bijection

$$S(M,(1)) \cong \frac{\{M \to \mathbb{Z}/p\mathbb{Z} \text{ surjective}\}}{\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})}$$

to obtain $\#\mathrm{Subgr}_p(M) = \frac{p^n-1}{p-1}$.

Combining this yields

$$\begin{aligned} \#\{\phi : M \to A_{\mu,p} \text{ surjective}\} &\geq (\#A_{\mu,p})^n - \sum_{B \in \mathrm{Subgr}_p(A)} (\#B)^n \\ &\geq (\#A_{\mu,p})^n - \frac{p^n-1}{p-1} \left(\frac{\#A_{\mu,p}}{p}\right)^n \\ &= (\#A_{\mu,p})^n \left(1 - \frac{p^n-1}{p^n(p-1)}\right), \end{aligned}$$

the lower bound. □

For the bounds on $\mathrm{Aut}(A_{\mu,p})$, we use the following lemma.

Lemma 5.25. *Let $d \geq 0$ and $h \geq 1$ be integers and $P \in \mathbb{F}_p[X_1, \ldots, X_h]$ be a non-zero homogeneous polynomial of total degree d. Then the number of zeroes of P in $\mathbb{F}_p^h$ is at most dp^{h-1}.*

Proof. We will do induction on h. If $h = 1$, then $P = aX_1^d$ for some non-zero constant a. When $d = 0$ the polynomial P has no zeroes, and when $d \geq 1$ it has one zero. In either case, the number of zeroes is at most dp^{h-1}.

Suppose the statement is true for all polynomials in less than h variables and let P be a polynomial in h variables. If X_h does not occur in P, then we can view it as a polynomial in $h-1$ variables. By the induction hypothesis, the number of zeroes is at most $p \cdot dp^{h-2} = dp^{h-1}$. If X_h does occur, let d' denote the maximal degree of X_h in P. View P as a polynomial in X_h and let $P_{d'}$ be the coefficient of $X_h^{d'}$. Note that $P_{d'}$ is a non-zero homogeneous polynomial in $h-1$ variables of degree $d - d'$.

Let $(x_i)_{i=1}^{h-1}$ run over $\mathbb{F}_p^{h-1}$. If $P(x_1, x_2, \ldots, x_{h-1}, X_h) \in \mathbb{F}_p[X_h]$ is zero, then it has p zeroes. Since in this case $P_{d'}(x_1, x_2, \ldots, x_{h-1})$ is zero, the number of times this occurs is at most $(d - d')p^{h-2}$, the maximal number of zeroes of $P_{d'}$. On the other hand, if $P(x_1, x_2, \ldots, x_{h-1}, X_h)$ is non-zero, then it has at most d' zeroes. Combining these results, we obtain that the number of zeroes of P is at most $p \cdot (d - d')p^{h-2} + d' \cdot p^{h-1} = dp^{h-1}$.

□

Lemma 5.26. *For every prime p, every positive integer n and every partition μ of length at most n, we have*

$$1 \leq \frac{\#\mathrm{End}(A_{\mu,p})}{\#\mathrm{Aut}(A_{\mu,p})} \leq \frac{p}{p-n}$$

when $p > n$ and

$$1 \leq \frac{\#\mathrm{End}(A_{\mu,p})}{\#\mathrm{Aut}(A_{\mu,p})} \leq p^{n^2}$$

when $p \leq n$.

Proof. The lower bounds are clear, since every automorphism is an endomorphism.

For the upper bounds, we define the map

$$\begin{aligned}\psi : \mathrm{End}(A_{\mu,p}) &\to \mathrm{End}(A_{\mu,p}/pA_{\mu,p}) \\ \phi &\mapsto \phi/pA_{\mu,p} = \{a + pA_{\mu,p} \mapsto \phi(a) + pA_{\mu,p}\}.\end{aligned}$$

This is well-defined, since $pA_{\mu,p}$ is mapped into itself by any endomorphism of $A_{\mu,p}$. The set $\psi(\mathrm{End}(A_{\mu,p}))$ is an $\mathbb{F}_p$-linear subspace of $\mathrm{End}(A_{\mu,p}/pA_{\mu,p})$. Let h be its dimension.

If $\phi \in \mathrm{End}(A_{\mu,p})$ is invertible, then $\phi^{-1}/pA_{\mu,p}$ is the inverse of $\phi/pA_{\mu,p}$. On the other hand, if $\phi \in \mathrm{End}(A_{\mu,p})$ is such that $\phi/pA_{\mu,p}$ is invertible, then we can

write $A = pA + \mathrm{im}(\phi)$. By Nakayama's lemma [2, X§4, lemma 4.1], we obtain that $A = \mathrm{im}(\phi)$, that is, ϕ is surjective. Since $A_{\mu,p}$ is a finite set, ϕ is invertible. We see $\psi(\mathrm{Aut}(A_{\mu,p})) = \psi(\mathrm{End}(A_{\mu,p})) \cap \mathrm{Aut}(A_{\mu,p}/pA_{\mu,p})$.

Since an endomorphism $\phi \in \mathrm{End}(A_{\mu,p}/pA_{\mu,p})$ is an automorphism if and only if $\det(\phi) \neq 0$, we look at the determinant map $\det : \psi(\mathrm{End}(A_{\mu,p})) \to \mathbb{F}_p$. It is given by a non-zero homogeneous polynomial in h variables of degree equal to the length of μ. Since μ has length at most n, by lemma 5.25, the number of zeroes of the determinant is at most np^{h-1}. Hence, we can bound

$$\frac{\#\mathrm{Aut}(A_{\mu,p})}{\#\mathrm{End}(A_{\mu,p})} = \frac{\#\psi(\mathrm{Aut}(A_{\mu,p}))}{\#\psi(\mathrm{End}(A_{\mu,p}))} \geq \frac{p^h - np^{h-1}}{p^h} = \frac{p-n}{p}.$$

When p is greater than n, then $\frac{p-n}{p} > 0$ implies that we can invert this. We obtain the first upper bound.

If p is at most n, we can improve this bound to

$$\frac{\#\psi(\mathrm{Aut}(A_{\mu,p}))}{\#\psi(\mathrm{End}(A_{\mu,p}))} \geq \frac{1}{p^{n^2}}$$

by noting that $\#\psi(\mathrm{Aut}(A_{\mu,p})) \geq 1$ and $h \leq n^2$. Inverting this fraction gives the second upper bound. □

Now we combine lemmas 5.24 and 5.26 to prove proposition 5.23.

Proof of proposition 5.23. First, we will determine $\#\mathrm{End}(A_{\mu,p})$. For positive integers a and b, a morphism $\phi \in \mathrm{Hom}(\mathbb{Z}/p^a\mathbb{Z}, \mathbb{Z}/p^b\mathbb{Z})$ is determined by the image of 1 in $\mathbb{Z}/p^b\mathbb{Z}$. This element should be such that $\phi(1)p^a = 0$. It follows that the number $\#\mathrm{Hom}(\mathbb{Z}/p^a\mathbb{Z}, \mathbb{Z}/p^b\mathbb{Z})$ is equal to $\min(p^a, p^b)$. Furthermore, for all groups A_1, A_2, B_1 and B_2, there exist group isomorphisms $\mathrm{Hom}(A_1 \times A_2, B_1) \to \mathrm{Hom}(A_1, B_1) \times \mathrm{Hom}(A_2, B_1)$ and $\mathrm{Hom}(A_1, B_1 \times B_2) \to \mathrm{Hom}(A_1, B_1) \times \mathrm{Hom}(A_1, B_2)$. Using these facts for $\mathrm{End}(A_{\mu,p})$, we obtain

$$\begin{aligned}\#\mathrm{End}(A_{\mu,p}) &= \prod_{i,j=1}^{n} \mathrm{Hom}(\mathbb{Z}/p^{\mu_i}\mathbb{Z}, \mathbb{Z}/p^{\mu_j}\mathbb{Z}) \\ &= p^{\sum_{i,j=1}^{n} \min(\mu_i, \mu_j)} = p^{\sum_{i=1}^{n}(2i-1)\mu_i}.\end{aligned}$$

Hence, the equality $p^{u(\mu,n)} = \frac{(\#A_{\mu,p})^n}{\#\mathrm{End}(A_{\mu,p})}$ follows from the definition of $u(\mu, n)$.

We obtain the equality

$$\begin{aligned}\frac{\#S(M,\mu)}{p^{u(\mu,n)}} &= \frac{\#\{\phi : M \twoheadrightarrow A_{\mu,p}\}/\#\mathrm{Aut}(A_{\mu,p})}{(\#A_{\mu,p})^n/\#\mathrm{End}(A_{\mu,p})} \\ &= \frac{\#\{\phi : M \twoheadrightarrow A_{\mu,p}\}}{(\#A_{\mu,p})^n} \cdot \frac{\#\mathrm{End}(A_{\mu,p})}{\#\mathrm{Aut}(A_{\mu,p})}.\end{aligned}$$

By lemmas 5.24 and 5.26, for $p > n$ this is bounded from above by $\frac{p}{p-n} = 1 + \frac{n}{p-n} \leq 1 + n$, and for $p \leq n$ this is bounded from above by $p^{n^2} \leq n^{n^2}$.

The second statement follows similarly. By the lemmas, $\frac{\#S(M,\mu)}{p^{u(\mu,n)}}$ is bounded from below by $1 - \frac{p^n-1}{p^n(p-1)}$. For $p = 2$ this is $1 - \frac{p^n-1}{p^n(p-1)} = \frac{1}{2^n}$ and for $p \geq 3$ this is bounded by $1 - \frac{p^n-1}{p^n(p-1)} \geq 1 - \frac{1}{p-1} \geq \frac{1}{2}$. □

5.5 Rounding rings

In this section we will prove proposition 5.9. For each prime p, each integer $n \geq 2$, each finite étale $\mathbb{Q}_p$-algebra E of degree n, each partition λ of length at most $n-1$ and each integer d with $\lambda_d > 2\lambda_{d+1}$, we will define the rounding map ρ_d on $\tilde{S}(E,\lambda)$, a set defined in section 5.1. The map ρ_d associates with a sub-$\mathbb{Z}_p$-module of a given cotype λ a submodule of a round cotype μ, that is, a cotype of the form $\mu = (e)^d$ for some positive integers e and d. We will show that ρ_d maps subrings to subrings and give a bound for the size of the fibres of ρ_d.

After that we will investigate the situation where two roundings satisfy an inclusion relation.

We will start by defining roundings on the sets $S(M,\lambda)$ for free $\mathbb{Z}_p$-modules M and partitions λ of length at most the rank of M. The sets $S(M,\lambda)$ were defined in section 5.1 for use in section 5.4. Since for each partition λ there exists a natural bijection between $\tilde{S}(E,\lambda)$ and $S(\mathcal{O}_E/1{\cdot}\mathbb{Z}_p,\lambda)$, this will give us a rounding on $\tilde{S}(E,\lambda)$.

Let M be a free $\mathbb{Z}_p$-module, let r be its rank. Let $N \in S(M,\lambda)$ be a sub-$\mathbb{Z}_p$-module of cotype λ. Let d be an integer with $1 \leq d \leq r-1$ and suppose that $\lambda_d > 2\lambda_{d+1}$ holds. Define the sub-$\mathbb{Z}_p$-module

$$\rho_d(N) = M \cap p^{-2\lambda_{d+1}}(N + p^{\lambda_d}M) \subset M \otimes_{\mathbb{Z}_p} \mathbb{Q}_p.$$

Proposition 5.27. *The module $\rho_d(N)$ is a submodule of M of cotype $(\lambda_d - 2\lambda_{d+1})^d$.*

Proof. Taking a basis $\langle \omega_1, \ldots, \omega_r \rangle$ of M such that $\langle p^{\lambda_1}\omega_1, \ldots, p^{\lambda_r}\omega_r \rangle$ is a basis of N, we see that $\rho_d(N)$ has a basis $\langle p^{\mu_1}\omega_1, \ldots, p^{\mu_r}\omega_r \rangle$, where the numbers μ_j are such that $p^{\mu_j}\omega_j \cdot \mathbb{Z}_p = \omega_j\mathbb{Z}_p \cap p^{-2\lambda_{d+1}}\mathbb{Z}_p(p^{\lambda_j}\omega_j + p^{\lambda_d}\omega_j)$. Hence, we can calculate

$$\begin{aligned}
\mu_j &= \max(0, -2\lambda_{d+1} + \min(\lambda_j, \lambda_d)) \\
&= \begin{cases} 0 & \text{if } \lambda_j \leq 2\lambda_{d+1} \\ -2\lambda_{d+1} + \lambda_j & \text{if } 2\lambda_{d+1} < \lambda_j \text{ and } \lambda_j < \lambda_d \\ -2\lambda_{d+1} + \lambda_d & \text{if } \lambda_d \leq \lambda_j \end{cases} \\
&= \begin{cases} 0 & \text{if } j > d \\ -2\lambda_{d+1} + \lambda_d & \text{if } j \leq d. \end{cases}
\end{aligned}$$

□

Note that from this proof it follows that we can use the same basis of M for N and $\rho_d(N)$.

Recall the definition $c_{11}(n,d,\lambda) = -d(n-d-1)(\lambda_d - 2\lambda_{d+1}) + \sum_{i=1}^{n-1}\big((n-2i)\lambda_i\big)$.

Proposition 5.28. *Let M be a free $\mathbb{Z}_p$-module, let r be its rank. Let λ be a partition of length at most r and let $d \leq r-1$ be an integer with $\lambda_d > 2\lambda_{d+1}$. Write μ for the partition $(\lambda_d - 2\lambda_{d+1})^d$.*

Then the map $\rho_d : S(M,\lambda) \to S(M,\mu)$ that sends a sub-$\mathbb{Z}_p$-module to its rounding is surjective. Furthermore, all fibres have the same cardinality. The fibres of ρ_d satisfy

$$\#\rho_d^{-1}(N) = O_r\big(p^{c_{11}(r+1,d,\lambda)}\big),$$

where p ranges over the set of primes, M over the collection of free $\mathbb{Z}_p$-modules, λ over the set of partitions of length at most the rank of M, the integer d over the integers such that $\lambda_d > 2\lambda_{d+1}$, the module N over $S(M,(\lambda_d - 2\lambda_{d+1})^d)$ and r is the rank of M.

Proof. The surjectivity and the equality of the sizes of the fibres follow from the fact that the group $\mathrm{Aut}_{\mathbb{Z}_p}(M)$ acts transitively on $S(M,\mu)$.

Recall the definition of $u(\lambda,r) = \sum_{i=1}^{r}((r+1-2i)\lambda_i)$. By proposition 5.23, we have $\#S(M,\lambda) = O_r\big(p^{u(\lambda,r)}\big)$ and $\frac{1}{\#S(M,\mu)} = O_r\big(p^{-u(\mu,r)}\big)$. By the first remark of the proof, the number of $\mathbb{Z}_p$-modules in $S(M,\lambda)$ that get rounded to a given $\mathbb{Z}_p$-module in $S(M,\mu)$ is $\frac{\#S(M,\lambda)}{\#S(M,\mu)} = O_r\big(p^{u(\lambda,r)-u(\mu,r)}\big)$. The fact $u(\lambda,r) - u(\mu,r) = c_{11}(r+1,d,\lambda)$ completes the proof. □

Now, we will switch our focus from $S(M,\lambda)$ to $\tilde{S}(E,\lambda)$. The $\mathbb{Z}_p$-module $\mathcal{O}_E/1\cdot\mathbb{Z}_p$ is free of rank $n-1$. The canonical bijection between $S(\mathcal{O}_E/1\cdot\mathbb{Z}_p,\lambda)$ and $\tilde{S}(E,\lambda)$ transports the rounding map ρ_d from the first to the second set. From the previous proposition we know that the fibres of ρ_d are equal in size and satisfy $\#\rho_d^{-1}(N) = O_r\big(p^{c_{11}(n,d,\lambda)}\big)$, as required for proposition 5.9.

It remains to show that ρ_d maps subrings to subrings. This fact is true for all $\mathbb{Z}_p$-algebras R that are free of finite rank as $\mathbb{Z}_p$-module, as we will show in the next proposition.

Let R be a $\mathbb{Z}_p$-algebra that is free as a $\mathbb{Z}_p$-module, suppose $\langle\omega_1,\ldots,\omega_{n-1},1\rangle$ is a basis of R. Consider only sub-$\mathbb{Z}_p$-modules of R with a basis of the form $\langle p^{\lambda_1}\omega_1,\ldots,p^{\lambda_{n-1}}\omega_{n-1},1\rangle$. By the remark after proposition 5.27, we can do this without loss of generality. For ease of notation, we write $\omega_n = 1$.

Since R is a ring, there exist $c_{ij}^k \in \mathbb{Z}_p$ for $i,j,k = 1,\ldots,n$ such that $\omega_i\omega_j = \sum_k c_{ij}^k\omega_k$.

Proposition 5.29. *Let R be a $\mathbb{Z}_p$-algebra that is free as a $\mathbb{Z}_p$-module. Let $T \subset R$ be a subring of cotype λ. Let d be an integer with $1 \leq d \leq n-2$ and suppose that $\lambda_d > 2\lambda_{d+1}$. Then $\rho_d(T)$, the rounding at d of T, is a subring of R.*

In the proof we will use the following lemma.

Lemma 5.30. *Let R be a $\mathbb{Z}_p$-algebra that is free of finite rank as $\mathbb{Z}_p$-module and let $\langle \omega_1, \ldots, \omega_{n-1}, 1\rangle$ be a basis of R. A sub-$\mathbb{Z}_p$-module $N \subset R$ with a basis of the form $\langle p^{\lambda_1}\omega_1, \ldots, p^{\lambda_{n-1}}\omega_{n-1}, 1\rangle$ is a subring if and only if for all i, j, k the equality $c_{ij}^k \equiv 0 \bmod p^{\lambda_k - \lambda_i - \lambda_j}$ holds.*

Proof. The product of two basis elements $p^{\lambda_i}\omega_i$ and $p^{\lambda_j}\omega_j$ is

$$p^{\lambda_i}\omega_i p^{\lambda_j}\omega_j = \sum_k (p^{\lambda_i+\lambda_j-\lambda_k} c_{ij}^k) p^{\lambda_k}\omega_k.$$

This is an element of N if and only if $p^{\lambda_i+\lambda_j-\lambda_k} c_{ij}^k \in \mathbb{Z}_p$ for all k. □

Proof of proposition 5.29. Let μ be the cotype of $\rho_d(N)$. According to lemma 5.30, it suffices to show that $c_{ij}^k \equiv 0 \bmod p^{\mu_k - \mu_i - \mu_j}$ for all i, j, k.

For the case $k > d$, we have $\mu_k - \mu_i - \mu_j \leq 0$ and therefore we are done. The case $k \leq d$ we split up into two subcases. If $i \leq d$ or $j \leq d$ holds, then we have $\mu_k - \mu_i - \mu_j \leq 0$ and we are done. If $i > d$ and $j > d$ both hold, then we can bound $\mu_k - \mu_i - \mu_j = \lambda_d - 2\lambda_{d+1} \leq \lambda_k - \lambda_i - \lambda_j$, and since T is a subring we have $c_{ij}^k \equiv 0 \bmod p^{\lambda_k - \lambda_i - \lambda_j}$, hence $c_{ij}^k \equiv 0 \bmod p^{\mu_k - \mu_i - \mu_j}$ is as required. □

We finish this section by looking into the case where one of the roundings of a subring is contained in a different rounding. These *rounding chains* will be used to improve the bound for degree 5 and cotype $(3, 1, 0, 0)$, an improvement that is used to obtain a result requested by Manjul Bhargava. Chapter 8 will state and prove that result.

Proposition 5.31. *Let M be a free $\mathbb{Z}_p$-module; let r be its rank. Let $N \subset M$ be a sub-$\mathbb{Z}_p$-module of cotype λ. Let d_1 and d_2 be integers with $1 \leq d_1 < d_2 \leq r-1$ and suppose that $0 < \lambda_{d_1} - 2\lambda_{d_1+1} \leq \lambda_{d_2} - 2\lambda_{d_2+1}$ holds. Then the rounding $\rho_{d_1}(N)$ of N at d_1 contains the rounding $\rho_{d_2}(N)$ of N at d_2.*

Proof. Write μ for the cotype of $\rho_{d_1}(N)$ and ν for the cotype of $\rho_{d_2}(N)$. From the proof of proposition 5.27 it follows that there is a basis $\langle \omega_1, \ldots, \omega_r\rangle$ for M such that $\rho_{d_1}(N)$ is generated by $\{p^{\mu_i}\omega_i\}_i$ and $\rho_{d_2}(N)$ by $\{p^{\nu_i}\omega_i\}_i$. The fact that for all i the inequality $\mu_i \leq \nu_i$ holds, shows the inclusion. □

Define for a free $\mathbb{Z}_p$-module M of finite rank r and partitions λ_1 and λ_2 of length at most r the set $S(M, \lambda_1, \lambda_2) = \{(N_1, N_2) \in S(M, \lambda_1) \times S(M, \lambda_2) : N_2 \subset N_1\}$.

Proposition 5.32. *Let M be a free $\mathbb{Z}_p$-module, let r be its rank. Let λ be a partition of length at most r and let d_1, d_2 be integers with $1 \leq d_1 < d_2 \leq r-1$ and $0 < \lambda_{d_1} - 2\lambda_{d_1+1} = \lambda_{d_2} - 2\lambda_{d_2+1}$. Write e for $\lambda_{d_1} - 2\lambda_{d_1+1}$ and write for $i = 1, 2$ the partition $\mu_i = (e)^{d_i}$. Then the map*

$$\begin{aligned} \rho_{d_1,d_2} : S(M, \lambda) &\to S(M, \mu_1, \mu_2) \\ N &\mapsto (\rho_{d_1}(N), \rho_{d_2}(N)) \end{aligned}$$

is surjective.

Furthermore, all fibres of ρ_{d_1,d_2} have the same cardinality. The fibres of ρ_{d_1,d_2} satisfy

$$\#\rho_{d_1,d_2}^{-1}((N_1,N_2)) = O_r\left(p^{(-d_2(r-d_2)-d_1(d_2-d_1))e+\sum_{i=1}^{r}((r+1-2i)\lambda_i)}\right),$$

where p ranges over the set of primes, M over the collection of free $\mathbb{Z}_p$-modules, e over the set of positive integers, λ over the set of partitions of length at most the rank of M, the integer pair (d_1,d_2) over the integers such that $1 \leq d_1 < d_2 \leq \mathrm{rk}(M)-1$ and $0 < \lambda_{d_1} - 2\lambda_{d_1+1} = \lambda_{d_2} - 2\lambda_{d_2+1} = e$, the module pair (N_1,N_2) over $S(M,\mu_1,\mu_2)$ and r is the rank of M.

Proof. The previous proposition shows that the image of the map is contained in $S(M,\mu_1,\mu_2)$.

For any pair $(N_1,N_2) \in S(M,\mu_1,\mu_2)$, let $\langle \omega_1', \dots, \omega_r' \rangle$ be a basis of M such that $\langle p^e\omega_1', \dots, p^e\omega_{d_2}', \omega_{d_2+1}', \dots, \omega_r' \rangle$ is a basis of N_2. Define the submodule $\tilde{N}_2 \subset M$ to be the module generated by $\omega_1', \dots, \omega_{d_2}'$. Let $\langle \omega_1, \dots, \omega_{d_2} \rangle$ be a basis of $\tilde{N}_2$ such that $\langle p^e\omega_1, \dots, p^e\omega_{d_1}, \omega_{d_1+1} \dots, \omega_{d_2}$ is a basis of $N_1 \cap \tilde{N}_2$. It follows that, with $\omega_i = \omega_i'$ for $i > d_2$ that $\langle \omega_1, \dots, \omega_r \rangle$ is a basis of M such that $\langle p^e\omega_1, \dots, p^e\omega_{d_j}, \omega_{d_j+1}, \dots, \omega_r \rangle$ is a basis of N_j for $j = 1, 2$.

This choice of basis shows that $\mathrm{Aut}_{\mathbb{Z}_p}(M)$ acts transitively on $S(M,\mu_1,\mu_2)$, and it therefore follows that ρ_{d_1,d_2} is surjective and that the fibres all have equal size. Hence all the fibres have size $\frac{\#S(M,\lambda)}{\#S(M,\mu_1,\mu_2)}$.

Recall the definition of $u(\lambda,r) = \sum_{i=1}^{r}((r+1-2i)\lambda_i)$. By proposition 5.23, we can bound $\#S(M,\lambda) = O_r\big(p^{u(\lambda,r)}\big)$.

For all $N_2 \in S(M,\mu_2)$, the number of modules $N_1 \in S(M,\mu_1)$ with $N_2 \subset N_1 \subset M$ is equal to $\#S(\tilde{N}_2,\mu_1)$. So we can bound by proposition 5.23,

$$\begin{aligned}\frac{1}{\#S(M,\mu_1,\mu_2)} &= \frac{1}{\#S(M,\mu_1)\#S(\tilde{N}_2,\mu_1)} \\ &= O_r\left(p^{-u(\mu_2,r)-u(\mu_1,d_2)}\right) \\ &= O_r\left(p^{-d_2(r-d_2)e-d_1(d_2-d_1)e}\right).\end{aligned}$$

Combining these two bounds gives the result. □

Bibliography

[1] G. H. Hardy, E. M. Wright, *An introduction to the theory of numbers, fourth edition*, Oxford University Press, New York, 1960.

[2] S. Lang, *Algebra, revised third edition*, Springer-Verlag, New York, 2002.

[3] I. G. Macdonald, *Symmetric functions and Hall polynomials*, Oxford University Press, New York, 1979.

[4] F. Miller Maley, *The Hall polynomial revisited*, J. Alg. **184** (1996), 363–371.

[5] J. Nakagawa, *Orders of a quartic field*, Mem. Amer. Math. Soc. **122**, no. 583, 1996.

[6] D. Saltman, *Generic Galois extensions*, Adv. in Math. **43** (1982), 250–283.

[7] E. Weiss, *Algebraic number theory*, McGraw-Hill, New York, 1963.

Chapter 6

Artinian principal ideal rings

In this chapter, we will study the structure of commutative artinian principal ideal rings. For some background information on artinian rings, we refer to Atiyah-Macdonald [1]. Note especially the following two results.

Lemma 6.1. *A commutative artinian ring can uniquely be written as a finite product of local artinian rings.*

Proof. [1, theorem 8.7]. □

Lemma 6.2. *For a commutative local artinian ring A the following are equivalent:*

1. *A is a principal ideal ring;*
2. *the maximal ideal of A is principal.*

Proof. [1, proposition 8.8]. □

The theory in this chapter will be used in the next chapter to prove proposition 5.8. We first highlight some of the results that will be used in the next chapter.

Throughout this chapter, Z will be a commutative local artinian principal ideal ring and A will be a commutative Z-algebra that is an artinian principal ideal ring. In the next chapter, Z will be the ring $\mathbb{Z}/p^e\mathbb{Z}$ for some prime power p^e and A will be the ring $\mathcal{O}_E/p^e\mathcal{O}_E$ with E a finite étale $\mathbb{Q}_p$-algebra. The rings in the sets $W_{d,e}(E)$ defined in section 5.1, correspond to certain sub-Z-algebras of A.

The first theorem tells us that these subalgebras are artinian principal ideals themselves.

Theorem 6.3. *Let Z be a commutative, local, artinian principal ideal ring, not a field; let $\mathfrak{m}$ be the maximal ideal of Z. Let A be a commutative Z-algebra such that $A/\mathfrak{m}^2A$ is a free $Z/\mathfrak{m}^2$-module of finite rank and A is an artinian principal ideal ring. Let $B \subset A$ be a sub-Z-algebra such that B is a free Z-module. Then B is an artinian principal ideal ring.*

We will show that a commutative, local, artinian principal ideal Z-algebra is generated as a Z-algebra by a single element where the minimal polynomial of that element is generalized Eisenstein.

Definition 6.4. *Let Z be a local ring with maximal ideal $\mathfrak{m}$. A polynomial $g \in Z[X]$ is* generalized Eisenstein *if there exist a monic polynomial $h \in Z[X]$, a positive integer e and for $i = 0, \ldots, e-1$ a polynomial $c_i \in Z[X]$ such that*

h *is irreducible in* $Z/\mathfrak{m}[X]$;

$g = h^e + \sum_{i=0}^{e-1} c_i h^i$;

$\deg(c_i) < \deg h$;

$c_i \in \mathfrak{m}Z[X]$;

$c_0 \notin \mathfrak{m}^2 Z[X]$.

The notion of generalized Eisenstein has been studied for the case where $Z = \mathbb{Z}_p$ by Ford, Pauli and Roblot [3, § 4].

Theorem 6.5. *Let Z be a commutative, local, artinian principal ideal ring, not a field; let $\mathfrak{m}$ be its maximal ideal. Suppose $Z/\mathfrak{m}$ is a perfect field. Then a commutative Z-algebra B that is free of finite rank as a Z-module is a local principal ideal ring if and only if there exists a generalized Eisenstein polynomial $g \in Z[X]$ such that $B \cong Z[X]/(g)$.*

Let Z be a commutative, local, artinian principal ideal ring, not a field; let $\mathfrak{m}$ be the maximal ideal of Z. Suppose $Z/\mathfrak{m}$ is a perfect field. Let A be a commutative Z-algebra such that $A/\mathfrak{m}^2 A$ is a free $Z/\mathfrak{m}^2$-module of finite rank and A is an artinian principal ideal ring.

By theorems 6.3 and 6.5 and lemma 6.1 we can write a sub-Z-algebra $B \subset A$ such that B is a free Z-module, as a finite product $\prod_i B_i$ where each B_i is isomorphic to $Z[X]/(g_i)$ for some polynomial $g_i \in Z[X]$ that is generalized Eisenstein. Let $\beta_i \in B_i$ be the element corresponding to X. Then $B_i = Z[\beta_i]$ and β_i is a zero of g_i. Define the A-ideal

$$I_B = \{a \in A : a(g_i'(\beta_i))_i = 0\}.$$

In section 6.5 we will show that the definition of I_B does not depend on the choice of g_i or β_i. Using the ideals I_B for various B, we can define a relation on the set of sub-Z-algebras $B \subset A$ that are free as a Z-module and satisfy $I_B^2 = 0$.

Definition 6.6. *On the set of artinian principal ideal sub-Z-algebras $B \subset A$ such that B is free as a Z-module and $I_B^2 = 0$, we define the relation $B_1 \approx B_2$ if B_1 and B_2 have the same image in A/I_{B_1}.*

This relation will turn out to be an equivalence relation; we show this in section 6.5 together with the following theorem, which counts the number of rings in an equivalence class.

Definition 6.7. *Let Z be a finite, commutative, local, artinian principal ideal ring, not a field. Write a commutative, finite, local, free, artinian principal ideal Z-algebra B as $B = Z[\beta]$, let g be a minimal polynomial of β and define* the discriminant of B over Z *to be the integer $\Delta_{B/Z} = \#(B/g'(\beta))$.*

In section 6.5 we will show that the definition of $\Delta_{B/Z}$ does not depend on the choice of g or β.

Theorem 6.8. *Let Z be a finite, commutative, local artinian principal ideal ring, not a field; let $\mathfrak{m}$ be the maximal ideal of Z. Let A be a commutative, finite Z-algebra such that A is an artinian principal ideal ring.*

Suppose $B \subset A$ is a local, free, artinian principal ideal sub-Z-algebra satisfying $I_B^2 = 0$. Suppose A is free as a B-module of rank r. Then the number of subalgebras $B' \subset A$ such that $B \approx B'$ is $\Delta_{B/Z}^{r-1}$.

When we can count the number of equivalence classes, we can bound the number of subrings $B \subset A$ such that $I_B^2 = 0$. Part of the next chapter will be to do precisely that in the case where $Z = \mathbb{Z}/p^e\mathbb{Z}$ and $A = \mathcal{O}_E/p^e\mathcal{O}_E$.

In the next section we recall the basic ring theory to be used in the rest of the chapter. In section 6.2 artinian principal ideal rings are given a valuation. In sections 6.3, 6.4 and 6.5 we prove theorems 6.3, 6.5 and 6.8 respectively.

6.1 Basic ring theory

In this section, we state some basic ring theory that will be used in various places in this chapter and the next.

6.1.1 Products

The next lemma will be used in many places to reduce the theory for global rings to that of local rings.

Lemma 6.9. *Let T be a commutative ring and R a commutative T-algebra. Suppose we can write $T = \prod_{i\in I} T_i$ as a finite product of rings. Then $R = \prod_{i\in I} R_i$ is a product of rings where R_i is a T_i-algebra.*

Proof. Let $R_i = R \otimes_T T_i$ for all $i \in I$. Then R_i is a T_i-algebra and as rings we have

$$R = R \otimes_T T = R \otimes_T \prod_{i\in I} T_i = \prod_{i\in I} (R \otimes_T T_i) = \prod_{i\in I} R_i.$$

□

6.1.2 Differentials

The definitions of I_B and $\Delta_{B/Z}$ from the introduction are a bit ad hoc. The more natural way to define this ideal is to look at differentials. We define the differentials here and will show the connection with I_B and $\Delta_{B/Z}$ in section 6.5.

Let T be a commutative ring and R a commutative T-algebra. Denote by $\Omega_{R/T}$ the R-module of relative differentials of R over T, see [6, chapter 10, §26.C] for a definition. Define the different $D_{R/T}$ to be the annihilator of $\Omega_{R/T}$, that is,

$$D_{R/T} = \{r \in R \mid \forall x \in \Omega_{R/T} : rx = 0\}.$$

Note that $D_{R/T}$ is an R-ideal.

Lemma 6.10. *Let T be a commutative ring and R a commutative T-algebra. If $R = T[X]/(f)$ holds for some polynomial f, then $D_{R/T}$ is the ideal generated by f'. Furthermore, we have $\Omega_{R/T} \cong R/D_{R/T}$.*

Proof. From [6, chapter 10, §26, theorem 58], we have the following exact sequence of R-modules.

$$(f)/(f)^2 \to \Omega_{T[X]/T} \otimes_{T[X]} R \to \Omega_{R/T} \to 0$$

From [6, chapter 10, §26.E, example 1], we have $\Omega_{T[X]/T} = T[X]dX \cong T[X]$, so we obtain $\Omega_{T[X]/T} \otimes_{T[X]} R \cong T[X] \otimes_{T[X]} R \cong R$. The first map from the exact sequence becomes the map

$$\begin{array}{ccccc} (f)/(f)^2 & \to \Omega_{T[X]/T} \otimes_{T[X]} R = T[X]dX \otimes_{T[X]} R & \cong R \\ \bar{f} & \mapsto \qquad df \otimes 1 = f'dX \otimes 1 & \mapsto f', \end{array}$$

so $\Omega_{R/T} \cong R/\mathrm{im}((f)/(f)^2) = R/(f')$. The annihilator of the module $R/(f')$ is the ideal generated by f'. □

Lemma 6.11. *Let T be a commutative ring and let R_1 and R_2 be commutative T-algebras. Define $R = R_1 \times R_2$. Then the different of R over T is $D_{R/T} = D_{R_1/T} \times D_{R_2/T}$.*

Proof. Define the multiplicative systems $S_1, S_2 \subset R$ by $S_1 = \{(1,1),(1,0)\}$ and $S_2 = \{(1,1),(0,1)\}$ According to [6, chapter 10, §26.G example 2], we have $\Omega_{S_i^{-1}R/T} \cong S_i^{-1}\Omega_{R/T}$. Since $S_i^{-1}R = R_i$ for $i = 1, 2$ and $S_1^{-1}\Omega_{R/T} \times S_2^{-1}\Omega_{R/T} \cong \Omega_{R/T}$, we have $\Omega_{R_1/T} \times \Omega_{R_2/T} \cong \Omega_{R/T}$. □

6.1.3 Hensel

In the theory of this chapter we will want to construct zeroes of polynomials in certain rings. When we have partial information on those zeroes, for example the residue class modulo some ideal, we can use Hensel theory to find a zero.

The theory in this section is from [2, chapter 7].

Definition 6.12. *Let R be a commutative ring and $\mathfrak{a}$ an ideal of R. Then the ring $\hat{R}_\mathfrak{a} = \varprojlim_i R/\mathfrak{a}^i$ is called the* completion of R with respect to $\mathfrak{a}$.
When the natural map

$$\begin{aligned} R &\to \hat{R}_\mathfrak{a} \\ x &\mapsto (x \bmod \mathfrak{a}^i)_i \end{aligned}$$

is a ring isomorphism, we will say that R is complete with respect to $\mathfrak{a}$.

Lemma 6.13. *Let R be a commutative ring and $\mathfrak{m}$ an ideal of R such that R is complete with respect to $\mathfrak{m}$. Let $f \in R[X]$ be a polynomial.*
If $a \in R$ is such that $f(a) \equiv 0 \bmod (f'(a)^2\mathfrak{m}^k)$ for some $k \in \mathbb{Z}_{\geq 1}$, then there exists an element $b \in R$ such that $f(b) = 0$ and $b \equiv a \bmod (f'(a)\mathfrak{m}^k)$.
Furthermore, if $f'(a)$ is not a zero divisor, then b is unique.

Proof. This follows almost directly from [2, theorem 7.3]. The only thing left to prove is that whenever R is complete with respect to $\mathfrak{m}$, it is also complete with respect to $\mathfrak{m}^k$ for any positive k. This is clear from the fact that

$$\begin{aligned} \hat{R}_\mathfrak{m} &\to \hat{R}_{\mathfrak{m}^k} \\ (x_i)_i &\mapsto (x_{ki})_i \end{aligned}$$

is an isomorphism. □

6.2 Valuations

This section provides us with a way of describing commutative artinian principal ideal rings. We will use this description in the proof of theorem 6.3. For semigroups, see chapter 2.

Definition 6.14. *A* valuation *on a ring Z is a morphism of semigroups from Z with its multiplicative structure to a semigroup H.*

Definition 6.15. *Let $l \geq 0$ and $m > 0$ be integers. Define an equivalence relation $\sim$ on $\frac{1}{m}\mathbb{Z}_{\geq 0} \subset \mathbb{Q}$ by $\frac{i}{m} \sim \frac{j}{m}$ when $i = j$ holds or both i and j are at least l. The set $H_{l/m} = \left(\frac{1}{m}\mathbb{Z}_{\geq 0}\right)/\sim$ is a semigroup where the operation is addition. We write H_l for the semigroup $H_{l/1}$.*

Note that for all l, m and m' the semigroups $H_{l/m}$ and $H_{l/m'}$ are isomorphic. Furthermore, products of these semigroups with componentwise operation are semigroups themselves.

The ordering on $\mathbb{Z}$ gives rise to a total ordering on $H_{l/m}$ and we define a partial ordering on $\prod_i H_{l_i/m_i}$ by saying $(a_i)_i \geq (b_i)_i$ if $a_i \geq b_i$ for all i.

We will sometimes view $H_{l/e}$ as subset of $\mathbb{Q}$ with $l/e \in \mathbb{Q}$ the chosen representative for $[l/e] \in H_{l/e}$. Note that this inclusion respects the ordering, but that addition is only respected as long as the answer is at most l/e.

Proposition 6.16. *Let A be a commutative ring and $t \geq 0$ an integer. Then the following are equivalent:*

1. *A is an artinian principal ideal ring with t maximal ideals;*
2. *there are positive integers $(l_i)_{i=1}^t$ and a surjective valuation $\phi_A : A \to \prod_{i=1}^t H_{l_i}$ such that for $a, b \in A$ the inequality $\phi_A(a) \geq \phi_A(b)$ implies that $a \in bA$.*

We start the proof of this proposition by defining for commutative, artinian principal ideal rings A the valuation ϕ_A.

For a commutative, local, artinian principal ideal ring A, we denote by π_A a generator of the maximal ideal of A. The chain $A \supset \pi_A A \supset \pi_A^2 A \supset \dots$ is finite, say $\pi_A^l A = \pi_A^{l+1} A$. Write $\pi_A^l = \pi_A^{l+1} x$ for some $x \in A$. Then we have $\pi_A^l(1 - \pi_A x) = 0$. Since $1 - \pi_A x$ is not in $\pi_A A$, it is invertible. So the element π_A is nilpotent. Define l_A, the *length of A*, to be the smallest integer l such that $\pi_A^l = 0$ holds. (This length is the length of A as A-module.)

Definition 6.17. *For a commutative, local artinian principal ideal ring A, take $l = l_A$ and define the map $\phi_A : A \to H_l$ in the following way. For an element $a \in A$, with $a \neq 0$, the value $\phi_A(a)$ is the integer such that $a \in \pi_A^{\phi_A(a)} A$ and $a \notin \pi_A^{\phi_A(a)+1} A$. We also set $\phi_A(0) = l_A$.*

Using lemma 6.1*, we write a general commutative, artinian principal ideal ring A as $\prod_i A_i$, a finite product of commutative, local, artinian principal ideal rings. Take $l_i = l_{A_i}$ and define the map*

$$\phi_A : A \to \prod_i H_{l_i}$$
$$a = (a_i)_i \mapsto (\phi_{A_i}(a_i))_i.$$

Next, we show that for local rings A the map ϕ_A has the desired properties.

Lemma 6.18. *Let A be a commutative, local, artinian principal ideal ring with a maximal ideal generated by π_A. Then every ideal of A is generated by π_A^i for some $i \in \mathbb{Z}_{\geq 0}$.*

The map ϕ_A is a surjective valuation such that for $a, b \in A$ the inequality $\phi_A(a) \geq \phi_A(b)$ implies that $a \in bA$.

Furthermore, A is complete with respect to its maximal ideal.

Proof. For an element $a \in A$ with $a \neq 0$, we can write $a = a' \pi_A^{\phi_A(a)}$ for some $a' \notin \pi_A A$, which implies $a' \in A^*$. So the ideal (a) equals $\left(\pi_A^{\phi_A(a)}\right)$. Hence every ideal I of A is generated by π_A^i, with $i = \min_{a \in I}\{\phi_A(a)\}$.

All elements $a, b \in A$ satisfy

$$\left(\pi_A^{\phi_A(ab)}\right) = (ab) = (a)(b) = \left(\pi_A^{\phi_A(a)}\right)\left(\pi_A^{\phi_A(b)}\right) = \left(\pi_A^{\phi_A(a)+\phi_A(b)}\right).$$

Hence ϕ_A is a valuation. Furthermore, if $a, b \in A$ are such that $\phi_A(a) \geq \phi_A(b)$ holds, then we have the inclusion $aA = \pi_A^{\phi(a)} A \subset \pi_A^{\phi(b)} A = bA$.

Since $\pi_A^{l_A} = 0$ implies that we have $\hat{A}_{(\pi_A)} \cong A/(\pi_A^{l_A}) = A$, the ring A is complete with respect to (π_A) □

Proof of proposition 6.16. Let A be a commutative, artinian principal ideal ring. Write $A = \prod_{i=1}^{t} A_i$ as a finite product of local rings and let ϕ_A be the map from definition 6.17. By lemma 6.18 and the properties of the product, this map is a valuation and it satisfies the requirements.

In this case t is equal to the number of maximal ideal of A.

On the other hand, let $\phi : A \to \prod_{i=1}^{t} H_{l_i}$ be a valuation with the required properties. Denote by $\phi_i : A \to H_{l_i}$ the valuation followed by projection on the i-th coordinate.

Let $e_i \in A$ be such that

$$\phi_j(e_i) = \begin{cases} 0 & \text{if } i = j \\ l_j & \text{if } i \neq j \end{cases}.$$

Suppose $1 \leq i \leq t$ and $a, b \in A$ are such that $\phi_i(a) \geq \phi_i(b)$. By definition of e_i, we have $\phi(e_i a) \geq \phi(e_i b)$, so we can write $e_i a = e_i b x$ for some $x \in A$. Hence, the inequality $\phi_i(a+b) = \phi_i(e_i) + \phi_i(a+b) = \phi_i(e_i a + e_i b) = \phi_i(e_i b(x+1)) \geq \phi_i(b)$ holds. Without loss of generality, we can conclude that for all i and $a, b \in A$ the inequality

$$\phi_i(a+b) \geq \min(\phi_i(a), \phi_i(b)) \tag{6.19}$$

holds.

Now, let $I \subset A$ be an ideal, and let for $i = 1, \ldots, t$ the elements $y_i \in I$ be such that $\phi_i(y_i)$ is minimal. Note that the elements $x_i = e_i y_i \in A$ satisfy $\phi_j(x_i) = l_j$ whenever i and j are different. Define $x = \sum_i x_i \in I$ and take an element $a \in A$ that for all i satisfies $\phi_i(a) = \phi_i(x_i)$. Then for all i we have $\phi(x_i) \geq \phi(a)$. Therefore we have $x \in aA$, hence we obtain $\phi_i(x) \geq \phi_i(a) = \phi_i(x_i)$. Using (6.19), we also have $\phi_i(x_i) = \phi_i\left(x - \sum_{j:j\neq i} x_j\right) \geq \min_{j:j\neq i}(\phi_i(x), \phi_i(x_j)) = \phi_i(x)$. We obtain that $\phi_i(x) = \phi_i(x_i)$ holds for all i. By the minimality of $\phi_i(x_i)$, any element $b \in I$ satisfies $\phi(b) \geq \phi(x)$ and is therefore in xA. Hence, the ideal I is generated by x and A is a principal ideal ring.

Let Id_A be the set of A-ideals with a partial order defined by inclusion. Then we have shown that the map

$$\begin{aligned} \mathrm{Id}_A &\to \prod_i H_{l_i} \\ aA &\mapsto \phi_A(a) \end{aligned}$$

is well-defined. The properties of ϕ_A makes it into an anti-isomorphism of partially ordered sets. This shows that A has only finitely many ideals, and hence is artinian. It also gives a bijection between the set of maximal A-ideals and the set of minimal non-zero elements of $\prod_i H_{l_i}$, of which there are exactly t. □

In the next lemma we describe a different set of requirements on a valuation for a commutative, local, artinian principal ideal ring that is equivalent to the requirements from proposition 6.16. These new requirements are easier to check and will be used in the proof of theorem 6.3.

Lemma 6.20. *Let A be a commutative ring, $l \geq 0$ an integer and $\phi : A \to H_l$ a valuation. Then the following are equivalent:*

1. *ϕ is surjective and for $a, b \in A$ the inequality $\phi(a) \geq \phi(b)$ implies $a \in bA$;*

2. *the fibre $\phi^{-1}(0)$ is A^* and the fibre $\phi^{-1}(l)$ is $\{0\}$; there exists $\pi_A \in \phi^{-1}(1)$ that satisfies $\{a \in A : \phi(a) \geq 1\} \subset \pi_A A$.*

Proof. We start by showing that the first set of requirements implies the second. First, let $b \in A$ with $\phi(b) = 0$. Then $1 \in bA$ shows that $b \in A^*$. Also, if $b' \in A^*$ holds, then we have $\phi(b') \leq \phi(b') + \phi(b'^{-1}b) = \phi(b) = 0$. Second, for $a \in \phi^{-1}(l)$ the inequality $\phi(a) \geq \phi(0)$ shows $a \in 0A$, that is, $a = 0$. Finally, take $\pi_A \in \phi^{-1}(1)$. Then all $a \in A$ such that $\phi(a) \geq 1 = \phi(\pi_A)$ satisfy $a \in \pi_A A$.

Now we show that the second set of requirements implies the first. For $1 \leq k \leq l$, we have $\phi(\pi_A^k) = k$, and $\phi(1) = 0$, so ϕ is surjective.

We will prove that the inequality $\phi(a) \geq \phi(b)$ implies $a \in bA$ by induction on $\phi(b)$. For the induction basis where $\phi(b) = 0$, we have $b \in A^*$, so every $a \in A$ is in bA. Next, let k be such that $1 \leq k < l$. Suppose the statement is true for all b' with $\phi(b') < k$. Let $b \in A$ be such that $\phi(b) = k$ and $a \in A$ such that $\phi(a) \geq k$. Since $k \geq 1$, there exist $a', b' \in A$ such that $a = a'\pi_A$ and $b = b'\pi_A$. Now, since $\phi(b) < l$, we have $\phi(a') \geq \phi(a) - 1 \geq \phi(b) - 1 = \phi(b')$. By the induction hypothesis, we have $a' \in b'A$ and so $a = a'\pi_A \in b'\pi_A A = bA$.

If $b \in A$ satisfies $\phi(b) = l$, then any a with $\phi(a) \geq \phi(b)$ equals 0, so $a \in bA$ is true in that case as well. □

We conclude this section with two lemmas on valuations used in sections 6.3 and 6.5 respectively.

Lemma 6.21. *Let Z be a commutative, local, artinian principal ideal ring; let π_Z be a generator of its maximal ideal. Let be A a commutative, local, artinian principal ideal Z-algebra. Denote $\phi_A(\pi_Z)$ by e_A.*

If A is free as a Z-module of finite rank, then its length is $l_A = e_A l_Z$.

Proof. Let π_A be a generator of the maximal ideal of A. We can take a basis of $A/\pi_Z A$ over $Z/\pi_Z Z$ with $\pi_A^{e_A - 1}$ as one of the basis elements. Using Nakayama's lemma, we lift this basis to a basis of A. When A is free, the element $\pi_Z^{l_Z - 1}\pi_A^{e_A - 1}$ is not 0. The length of A is therefore at least $(l_Z - 1)e_A + e_A - 1 + 1 = e_A l_Z$. On the other hand, we have $\left(\pi_A^{e_A l_Z}\right) = \left(\pi_Z^{l_Z}\right) = 0$, so the length of A is at most $e_A l_Z$. □

Lemma 6.22. *Let Z be a commutative, local, artinian principal ideal ring, not a field; let π_Z be a generator of its maximal ideal. Let the Z-algebra A be a commutative, artinian principal ideal ring such that $A/\pi_Z^2 A$ is a free $Z/\pi_Z^2 Z$-module of finite rank.*

Then we have the inclusion $\{x \in A : x^2 = 0\} \subset \pi_Z A$.

Proof. Write $A = \prod_{\mathfrak{m}} A_{\mathfrak{m}}$ as a finite product of local artinian principal ideal rings. To ease notation, we will write $\mathfrak{m}$ as subscript instead of $A_{\mathfrak{m}}$. Denote $\phi_{\mathfrak{m}}(\pi_Z)$ by $e_{\mathfrak{m}}$.

Because $A/\pi_Z^2 A$ is free as a $Z/\pi_Z^2 Z$-module, it follows from lemma 6.21 that for any localization $A_{\mathfrak{m}}$ of A, we have $l_{\mathfrak{m}} \geq l_{A_{\mathfrak{m}}/\pi_Z^2 A_{\mathfrak{m}}} = e_{\mathfrak{m}} l_{Z/\pi_Z^2 Z} = 2e_{\mathfrak{m}}$. Every $x \in A$ with $x^2 = 0$ satisfies for all $\mathfrak{m} \in \mathrm{MaxSpec}(A)$ the inequality $\phi_{\mathfrak{m}}(x) \geq l_{\mathfrak{m}}/2 = e_{\mathfrak{m}} = \phi_{\mathfrak{m}}(\pi_Z)$. This implies $\phi_A(x) \geq \phi_A(\pi_Z)$. Now $x \in \pi_Z A$ follows from proposition 6.16. □

6.3 Subalgebras

In this section, we prove theorem 6.3. We will use the valuation from the previous section. To be able to compare valuations of different algebras over the same base ring, we first define a scaling of the valuations.

Notation 6.23. *Let Z be a commutative, local, artinian principal ideal ring; let π_Z be a generator of its maximal ideal. For a commutative Z-algebra A that is also a local artinian principal ideal ring, we denote $\phi_A(\pi_Z)$ by e_A. Denote by ψ the natural isomorphism $H_{l_A} \to H_{l_A/e_A}$. The scaling of ϕ_A is the valuation $\tilde{\phi}_A = \psi\phi_A$.*

We write a general commutative, artinian principal ideal Z-algebra A as $\prod_i A_i$, a finite product of commutative, local, artinian principal ideal Z-algebras. The scaling of ϕ_A is the valuation $\tilde{\phi}_A = \prod_i \tilde{\phi}_{A_i}$.

The valuation $\tilde{\phi}_A$ is a scaled version of ϕ_A that behaves nicely under inclusions.

Proposition 6.24. *Let Z be a commutative, local, artinian principal ideal ring, not a field; let π_Z be a generator of its maximal ideal. Let the Z-algebra A be a commutative artinian principal ideal ring such that $A/\pi_Z^2 A$ is a free $Z/\pi_Z^2 Z$-module of finite rank. Let $B \subset A$ be a local sub-Z-algebra such that $\pi_Z A \cap B = \pi_Z B$.*

Then there exist an integer l, a valuation $\phi_B : B \to H_l$ and an element $\pi_B \in B$ such that

$$\phi_B^{-1}(0) = B^*,$$

$$\phi_B^{-1}(l) = \{0\},$$

$$\phi_B(\pi_B) = 1 \text{ and}$$

$$\{b \in B : \phi_B(b) \geq 1\} \subset \pi_B B.$$

Proof. Write $A = \prod_{\mathfrak{m}} A_{\mathfrak{m}}$ as a finite product of local artinian principal ideal rings. To ease notation, we will write $\mathfrak{m}$ as subscript instead of $A_{\mathfrak{m}}$. Since $A/\pi_Z^2 A$ is a free $Z/\pi_Z^2 Z$-module, by lemma 6.21 we obtain for all $\mathfrak{m}$ the inequality $l_{\mathfrak{m}} \geq l_{A_{\mathfrak{m}}/\pi_Z^2 A_{\mathfrak{m}}} = e_{\mathfrak{m}} l_{Z/\pi_Z^2 Z} = 2e_{\mathfrak{m}}$.

Since $A/\pi_Z^2 A$ is finite over Z, and therefore A also, the ring B is finite over Z. Since Z is artinian, B is also artinian.

Next, we show that for every ideal $\mathfrak{m} \in \mathrm{MaxSpec}(A)$ the valuation $\tilde{\phi}_{\mathfrak{m}}$ satisfies $B^* = \tilde{\phi}_{\mathfrak{m}}^{-1}(0) \cap B$. Take an element $x \in \tilde{\phi}_{\mathfrak{m}}^{-1}(0) \cap B$. Then x is locally at $\mathfrak{m}$ invertible, hence it is not nilpotent; since B is local and artinian, we obtain $x \in B^*$. On the other hand,

$$B^* \subset A^* \cap B = \left(\bigcap_{\mathfrak{m}} \tilde{\phi}_{\mathfrak{m}}^{-1}(0) \right) \cap B \subset \tilde{\phi}_{\mathfrak{m}}^{-1}(0) \cap B$$

shows that $B^* \subset \tilde{\phi}_{\mathfrak{m}}^{-1}(0) \cap B$ for every maximal ideal $\mathfrak{m}$.

Now we prove the following claim.

Claim. For all elements $x \in B$ and ideals $\mathfrak{n}, \mathfrak{n}' \in \mathrm{MaxSpec}(A)$ we have

$$\min(l_{\mathfrak{n}'}/e_{\mathfrak{n}'}, \tilde{\phi}_{\mathfrak{n}}(x)) = \min(l_{\mathfrak{n}}/e_{\mathfrak{n}}, \tilde{\phi}_{\mathfrak{n}'}(x)).$$

Proof of claim. Suppose there exist $x \in B$ and $\mathfrak{n}, \mathfrak{n}' \in \mathrm{MaxSpec}(A)$ such that the claim is not true. Take x and $\mathfrak{n}$ such that $\tilde{\phi}_{\mathfrak{n}}(x)$ is minimal with this property. We have $\tilde{\phi}_{\mathfrak{n}}(x) \leq \tilde{\phi}_{\mathfrak{n}'}(x) \leq l_{\mathfrak{n}'}/e_{\mathfrak{n}'}$ and $\tilde{\phi}_{\mathfrak{n}}(x) \leq l_{\mathfrak{n}}/e_{\mathfrak{n}}$. The only possible case is $\tilde{\phi}_{\mathfrak{n}}(x) = \min(l_{\mathfrak{n}'}/e_{\mathfrak{n}'}, \tilde{\phi}_{\mathfrak{n}}(x)) < \min(l_{\mathfrak{n}}/e_{\mathfrak{n}}, \tilde{\phi}_{\mathfrak{n}'}(x))$. Note that in particular, $\tilde{\phi}_{\mathfrak{n}}(x) < l_{\mathfrak{n}}/e_{\mathfrak{n}}$ and $\tilde{\phi}_{\mathfrak{n}}(x) < \tilde{\phi}_{\mathfrak{n}'}(x) \leq l_{\mathfrak{n}'}/e_{\mathfrak{n}'}$ hold.

If there exists $\mathfrak{m} \in \mathrm{MaxSpec}(A)$ such that $\tilde{\phi}_{\mathfrak{m}}(x) < \tilde{\phi}_{\mathfrak{n}}(x)$, then, by the minimality of $\tilde{\phi}_{\mathfrak{n}}(x)$, we have $\min(l_{\mathfrak{m}}/e_{\mathfrak{m}}, \tilde{\phi}_{\mathfrak{n}}(x)) = \min(l_{\mathfrak{n}}/e_{\mathfrak{n}}, \tilde{\phi}_{\mathfrak{m}}(x))$, which can only happen if $l_{\mathfrak{m}}/e_{\mathfrak{m}} = \tilde{\phi}_{\mathfrak{m}}(x)$. We see that for all $\mathfrak{m} \in \mathrm{MaxSpec}(A)$ either $\tilde{\phi}_{\mathfrak{n}}(x) \leq \tilde{\phi}_{\mathfrak{m}}(x)$, or $\tilde{\phi}_{\mathfrak{m}}(x) \geq 2$ holds.

Suppose $\tilde{\phi}_{\mathfrak{n}}(x) \geq 1$ holds, then by the previous remark, we have $\tilde{\phi}_A(x) \geq (1, 1, \ldots, 1)$ and $x \in \pi_Z A$. By the assumption on B, we can write $x = \pi_Z x'$ with $x' \in B$. The strict bound $\tilde{\phi}_{\mathfrak{n}}(x') < \tilde{\phi}_{\mathfrak{n}}(x) < l_{\mathfrak{n}'}/e_{\mathfrak{n}'}$ and the minimality of $\tilde{\phi}_{\mathfrak{n}}(x)$ tell us $\tilde{\phi}_{\mathfrak{n}}(x') = \min(l_{\mathfrak{n}'}/e_{\mathfrak{n}'}, \tilde{\phi}_{\mathfrak{n}}(x')) = \min(l_{\mathfrak{n}}/e_{\mathfrak{n}}, \tilde{\phi}_{\mathfrak{n}'}(x'))$. Since we also have the strict bound $\tilde{\phi}_{\mathfrak{n}}(x') < \tilde{\phi}_{\mathfrak{n}}(x) < l_{\mathfrak{n}}/e_{\mathfrak{n}}$, we obtain $\tilde{\phi}_{\mathfrak{n}}(x') = \tilde{\phi}_{\mathfrak{n}'}(x')$. Therefore, we have equality in $\tilde{\phi}_{\mathfrak{n}}(x) = \tilde{\phi}_{\mathfrak{n}}(x') + 1 = \tilde{\phi}_{\mathfrak{n}'}(x') + 1 \geq \tilde{\phi}_{\mathfrak{n}'}(x)$, a contradiction with the inequality $\tilde{\phi}_{\mathfrak{n}}(x) < \tilde{\phi}_{\mathfrak{n}'}(x)$.

If we have $\tilde{\phi}_{\mathfrak{n}}(x) = 0$, then $x \in B^*$ shows that $\tilde{\phi}_{\mathfrak{n}'}(x) = 0$ holds as well.

For the final case where $0 < \tilde{\phi}_{\mathfrak{n}}(x) < 1$, we first note that $\tilde{\phi}_{\mathfrak{n}}(x)$ is the minimum over $\mathfrak{m} \in \mathrm{MaxSpec}(A)$ of $\tilde{\phi}_{\mathfrak{m}}(x)$. Let $k \in \mathbb{Z}$ be such that $(k-1)\tilde{\phi}_{\mathfrak{n}}(x) < 1 \leq k\tilde{\phi}_{\mathfrak{n}}(x)$ holds. By the minimality of $\tilde{\phi}_{\mathfrak{n}}(x)$ and the fact that $l_{\mathfrak{m}}/e_{\mathfrak{m}} \geq 2$ for all $\mathfrak{m} \in \mathrm{MaxSpec}(A)$, we have the inequality $(1, 1, \ldots, 1) \leq k\tilde{\phi}_A(x)$ and $x^k \in \pi_Z A$.

When we write $x^k = \pi_Z x'$ and apply the valuation, we get the strict bound $1 + \tilde{\phi}_{\mathfrak{n}}(x') = k\tilde{\phi}_{\mathfrak{n}}(x) = (k-1)\tilde{\phi}_{\mathfrak{n}}(x) + \tilde{\phi}_{\mathfrak{n}}(x) < 2 \leq l_{\mathfrak{n}}/e_{\mathfrak{n}}$. The structure of $H_{l_{\mathfrak{n}}/e_{\mathfrak{n}}}$ gives $\tilde{\phi}_{\mathfrak{n}}(x') = k\tilde{\phi}_{\mathfrak{n}}(x) - 1 < \tilde{\phi}_{\mathfrak{n}}(x)$. From the minimality of $\tilde{\phi}_{\mathfrak{n}}(x)$ it follows that $\tilde{\phi}_{\mathfrak{n}}(x') = \tilde{\phi}_{\mathfrak{n}'}(x')$. We see $\tilde{\phi}_{\mathfrak{n}}(x^k) = \tilde{\phi}_{\mathfrak{n}}(x') + 1 = \tilde{\phi}_{\mathfrak{n}'}(x') + 1 = \tilde{\phi}_{\mathfrak{n}'}(x^k)$. Since this expression is less than 2 and hence less than $l_{\mathfrak{n}'}/e_{\mathfrak{n}'}$, we obtain $\tilde{\phi}_{\mathfrak{n}}(x) = \tilde{\phi}_{\mathfrak{n}'}(x)$. Hence x, $\mathfrak{n}$ and $\mathfrak{n}'$ do not exist. □

Let $\mathfrak{m} \in \mathrm{MaxSpec}(A)$ be such that $l_{\mathfrak{m}}/e_{\mathfrak{m}}$ is maximal and define $\tilde{\phi}_B = \tilde{\phi}_{\mathfrak{m}}|_B$. This map is a valuation, since $\tilde{\phi}_{\mathfrak{m}}$ is a valuation. We will show that this valuation restricted to its image has the desired properties, including the property that its image is isomorphic to H_l for some integer l.

We already saw that $\phi_B^{-1}(0) = \phi_{\mathfrak{m}}^{-1}(0) \cap B = B^*$.

By the choice of $\mathfrak{m}$, we have for all $x \in A$ and $\mathfrak{n} \in \mathrm{MaxSpec}(A)$ the inequality $\tilde{\phi}_{\mathfrak{n}}(x) \leq l_{\mathfrak{m}}/e_{\mathfrak{m}}$. So, as a direct consequence of the claim, we have for all $x, y \in B$ with $\tilde{\phi}_{\mathfrak{m}}(x) \geq \tilde{\phi}_{\mathfrak{m}}(y)$ and all $\mathfrak{n} \in \mathrm{MaxSpec}(A)$ the inequality

$$\begin{aligned}\tilde{\phi}_{\mathfrak{n}}(x) &= \min(l_{\mathfrak{m}}/e_{\mathfrak{m}}, \tilde{\phi}_{\mathfrak{n}}(x)) = \min(l_{\mathfrak{n}}/e_{\mathfrak{n}}, \tilde{\phi}_{\mathfrak{m}}(x)) \\ &\geq \min(l_{\mathfrak{n}}/e_{\mathfrak{n}}, \tilde{\phi}_{\mathfrak{m}}(y)) = \min(l_{\mathfrak{m}}/e_{\mathfrak{m}}, \tilde{\phi}_{\mathfrak{n}}(y)) = \tilde{\phi}_{\mathfrak{n}}(y).\end{aligned}$$

We see that if $x, y \in B$ satisfy $\tilde{\phi}_B(x) \geq \tilde{\phi}_B(y)$, then we also have $\tilde{\phi}_A(x) \geq \tilde{\phi}_A(y)$.

Take $x \in B$ with $\tilde{\phi}_B(x) \geq \tilde{\phi}_B(0)$. Then by the previous remark, $\tilde{\phi}_A(x) \geq \tilde{\phi}_A(0)$. Hence $x = 0$ follows from the properties of ϕ_A from proposition 6.16.

Next, we will show that the image $\tilde{\phi}_B(B) \subset H_{l_{\mathfrak{m}}/e_{\mathfrak{m}}}$ is equal to H_{l_B/e_B} for some integers $l_B, e_B \in \mathbb{Z}_{>0}$. Let $\pi_B \in B$ be such that $\tilde{\phi}_B(\pi_B)$ is non-zero and minimal with this property. Let $e_B \in \mathbb{Z}_{>0}$ be such that $(e_B - 1)\tilde{\phi}_B(\pi_B) < 1 \leq e_B\tilde{\phi}_B(\pi_B)$. It now follows from the consequence of the claim that $\tilde{\phi}_A(\pi_Z) \leq \tilde{\phi}_A(\pi_B^{e_B})$. From the requirement that $\pi_Z A \cap B = \pi_Z B$ it follows that there exists $x \in B$ such that $\pi_B^{e_B} = \pi_Z x$. The inequality $\tilde{\phi}_B(x) < \tilde{\phi}_B(\pi_B)$ shows that $x \in B^*$. So, we have $e_B\tilde{\phi}_B(\pi_B) = 1$.

Now, let $y \in B$ be an element with $\tilde{\phi}_B(y) < 1$. Let $k \in \mathbb{Z}$ be such that $(k-1)\tilde{\phi}_B(\pi_B) + \tilde{\phi}_B(y) < 1 \leq k\tilde{\phi}_B(\pi_B) + \tilde{\phi}_B(y)$, and write $y\pi_B^k = \pi_Z y'$ with $y' \in B$. Then the inequality $\tilde{\phi}_B(y') < \tilde{\phi}_B(\pi_B)$ shows that $\tilde{\phi}_B(y') = 0$, and $\tilde{\phi}_B(y) = \frac{e_B - k}{e_B} \in \mathbb{Z}\frac{1}{e_B} \cap H_{l_{\mathfrak{m}}/e_{\mathfrak{m}}}$.

For general $x \in B$ with $x \neq 0$, we can write $x = \pi_Z^{\lfloor \tilde{\phi}_B(x) \rfloor} y$, with $y \in B$ such that $\tilde{\phi}_B(y) < 1$. So $\tilde{\phi}_B(x) = e_B\lfloor \tilde{\phi}_B(x) \rfloor + \tilde{\phi}_B(y)$ is in $\mathbb{Z}\frac{1}{e_B} \cap H_{l_{\mathfrak{m}}/e_{\mathfrak{m}}}$ as well.

With $l_B = \lceil (l_{\mathfrak{m}}/e_{\mathfrak{m}})e_B \rceil$, we have $\tilde{\phi}_B(0) = [l_{\mathfrak{m}}/e_{\mathfrak{m}}] = [l_B/e_B]$. Hence we obtain $\tilde{\phi}_B(B) \cong H_{l_B/e_B}$.

It remains to show that every $b \in B$ such that $\tilde{\phi}_B(b) \geq \tilde{\phi}_B(\pi_B)$ satisfies $b \in \pi_B B$. Let $b \in B$ be such an element. We can write $\pi_Z = \pi_B x$ for some $x \in B$. The

inequality $\tilde{\phi}_B(bx) \geq \tilde{\phi}_B(\pi_Z)$ now gives us $bx \in \pi_Z A \cap B = \pi_Z B$. If we write $bx = \pi_Z y = \pi_B xy$, then we see $\pi_Z(b - \pi_B y) = \pi_B x(b - \pi_B y) = 0$. Applying the valuation, we get $\tilde{\phi}_B(\pi_Z) + \tilde{\phi}_B(b - \pi_B y) \geq l_B/e_B \geq 2$. Hence, we obtain $\tilde{\phi}_B(b - \pi_B y) \geq 1$. This implies $b - \pi_B y \in \pi_Z B \subset \pi_B B$. □

Now we can tie everything together to prove theorem 6.3. We restate this theorem below with a slight notational difference.

Theorem 6.3. *Let Z be a commutative, local, artinian principal ideal ring, not a field; let π_Z be a generator of its maximal ideal. Let A be a commutative Z-algebra such that $A/\pi_Z^2 A$ is a free $Z/\pi_Z^2 Z$-module of finite rank and A is an artinian principal ideal ring. Let $B \subset A$ be a sub-Z-algebra such that B is a free Z-module. Then B is an artinian principal ideal ring.*

Proof. First assume B is local. Since B is free, we have the inclusion $\pi_Z B = \mathrm{Ann}_B(\pi_Z^{l_Z - 1}) = \mathrm{Ann}_A(\pi_Z^{l_Z - 1}) \cap B \supset \pi_Z A \cap B$. The reverse inclusion is clear.

Now we use proposition 6.24 to conclude that B has a valuation with the second set of properties from lemma 6.20. Hence, from lemma 6.20 and proposition 6.16, we obtain that B is a local artinian principal ideal ring.

If B is a general ring, write $B = \prod_{\mathfrak{m}} B_{\mathfrak{m}}$ as a finite product of local rings. Kaplansky's theorem [5], which states that over a local ring every projective module is free, shows that each ring $B_{\mathfrak{m}}$ is free as a Z-module and therefore a local artinian principal ideal ring. Hence B is an artinian principal ideal ring. □

6.4 Generalized Eisenstein

We start this section with proving theorem 6.5. The proof is split into two parts. In proposition 6.25 we show the implication from left to right and in proposition 6.26 we show the reverse.

After these two propositions, we will continue with some theory on I_B.

Proposition 6.25. *Let Z be a commutative, local, artinian principal ideal ring, not a field; let π_Z be a generator of its maximal ideal. Suppose $Z/\pi_Z Z$ is a perfect field. Let B be a commutative Z-algebra that is free of finite rank as a Z-module. Suppose B is a local principal ideal ring.*

Then there exists a generalized Eisenstein polynomial $g \in Z[X]$ such that B is isomorphic to $Z[X]/(g)$.

Proof. Write F for the field $Z/\pi_Z Z$. The ring $B/\pi_B B$ is an F-algebra, that is, $B/\pi_B B$ is an extension of F. So we can write $B/\pi_B B = F(\bar{a})$. Let $\bar{h} \in F[X]$ be the monic irreducible minimal polynomial of $\bar{a}$, let h be a monic lift of $\bar{h}$ to $Z[X]$ and let $\tilde{a}$ be a lift of $\bar{a}$ to B.

Since F is perfect, $h'(\tilde{a})$ is not in (π_B), so by Hensel's lemma, there is a unique $a \in B$ such that a is a zero of h and $a = \bar{a}$ holds in F.

The element $\beta = a + \pi_B$ is also a lift of $\bar{a}$. So $Z[\beta]$ maps onto the entire residue class field $B/\pi_B B$ and since we have $h(\beta) = h(a + \pi_B) = h(a) + h'(a)\pi_B + x\pi_B^2 \equiv h'(a)\pi_B \bmod (\pi_B^2)$ and $h'(a) \notin (\pi_B)$, it also contains a generating element of (π_B). If we view $Z[\beta]$ as subset of $B/\pi_B^2 B$, we see it is equal to $B/\pi_B^2 B$. According to [4, II-7.4] the embedding $Z[\beta] \to B$ is surjective and therefore it is an isomorphism.

View multiplication by β as a Z-linear map and let $g \in Z[X]$ be the characteristic polynomial of this map. By Cayley-Hamilton theorem [7] the element β is a zero of g. Furthermore, since the degree of g is exactly the rank of B over Z, we obtain $B \cong Z[X]/(g)$.

Viewing this isomorphism modulo π_Z gives $B/\pi_Z B \cong (Z/\pi_Z Z)[X]/(g)$. Define $e = \phi_B(\pi_Z)$. We obtain $\deg(g) = \mathrm{rk}_F(B/\pi_Z B) = \mathrm{rk}_F(B/\pi_B^e B) = e\,\mathrm{rk}_F(B/\pi_Z B) = e\deg(h)$. The polynomials g and h are monic, so through repeated division with remainder, we can write

$$g = h^e + \sum_{i=0}^{e-1} c_i h^i,$$

where $c_i \in Z[X]$ are such that $\deg(c_i) < \deg(h)$. Hence we have

$$h(\beta)^e = \sum_{i=0}^{e-1} -c_i(\beta)h(\beta)^i.$$

The valuation in B of $h(\beta) = h(a+\pi_B) = h(a)+\pi_B h'(a)+\pi_B^2 x = \pi_B(h'(a)+\pi_B x)$ is 1. Furthermore, for each i we either have $c_i = 0$, or we can write $c_i = \pi_Z^{k_i}\tilde{c}_i$, for some integer k_i and polynomial $\tilde{c}_i \in Z[X] \setminus \pi_Z Z[X]$. In $B/\pi_B B$ we have $\tilde{c}_i(\beta) = \tilde{c}_i(a) \neq 0$, so the valuation of $c_i(\beta)$ is a multiple of e.

From the equality

$$e = \phi_B(h(\beta)^e) = \phi_B\left(\sum_{i=0}^{e-1} -c_i(\beta)h(\beta)^i\right) = \min_{i:c_i\neq 0}(\phi_B(c_i(\beta)+i)),$$

where the last step follows from the fact that all $\phi_B(c_i(\beta)) + i$ are different, we see that $\phi_B(c_i(\beta)) \geq e$ and $\phi_B(c_0(\beta)) = e$. In other words, $c_i \in \pi_Z Z[X]$ and $c_0 \notin \pi_Z^2 Z[X]$. □

Proposition 6.26. *Let Z be a local, artinian principal ideal ring. Let $g \in Z[X]$ be a generalized Eisenstein polynomial. Then $Z[X]/(g)$ is a commutative, local, artinian principal ideal ring that is free as a Z-module.*

Proof. Write $g = h^e + \sum_i c_i h^i$ with h, e and c_i as in the definition of generalized Eisenstein. Write B for $Z[X]/(g)$.

The polynomial g is monic, so B is free of finite rank as a Z-module. This also shows that B is artinian.

Let π_Z be a generator of the maximal ideal of Z. Since π_Z is nilpotent, any maximal ideal of B contains π_Z and is therefore a contraction of a maximal ideal of

$$B/\pi_Z B = (Z/\pi_Z Z)[X]/(g) = (Z/\pi_Z Z)[X]/(h^e).$$

Since h is irreducible in $(Z/\pi_Z Z)[X]$, the only maximal ideal of $B/\pi_Z B$ is generated by h. Hence, the only maximal ideal of B is $(h, \pi_Z)B$.

In B we have $0 = h(h^{e-1} + \sum_{i=1}^{e-1} c_i h^{i-1}) + c_0$, which shows that $c_0 \in hB$. Let $c \in Z[X]$ be a polynomial such that $\pi_Z c = c_0$. Now, from $\deg c = \deg(c_0) < \deg h$ and $c \notin \pi_Z Z[X]$ we deduce that c is invertible in $(Z/\pi_Z Z)[X]/(h) = Z[X]/(\pi_Z, h) = Z[X]/(\pi_Z, h, g) = B/(\pi_Z, h)B$, and hence in B. This shows that c_0 and π_Z generate the same B-ideal. Now, the inclusion $\pi_Z B = c_0 B \subset hB$ shows the maximal ideal $(\pi_Z, h)B = hB$ is a principal ideal. Hence B is a principal ideal ring by lemma 6.2. Since $Z[X]$ is commutative, B is commutative. □

Combining propositions 6.25 and 6.26 completes the proof of theorem 6.5.

To get a handle on the condition $I_B^2 = 0$ from theorem 6.8, we would like to bound $g'(X)$ for generalized Eisenstein polynomials. This is done through the following proposition.

Proposition 6.27. *Let Z be a commutative, local, artinian principal ideal ring and $g \in Z[X]$ a generalized Eisenstein polynomial. Write $B = Z[X]/(g)$ and let ϕ_B the valuation on B from proposition 6.16. Let e be as in the definition of generalized Eisenstein.*

Then we can bound $\phi_B(g'(X)) \leq \phi_B(\deg(g)) + e - 1$. If $\phi_B(e) = 0$, that is, if e is invertible in Z, we have $\phi_B(g'(X)) = e - 1$.

In the proof of this proposition, we use the following lemma.

Lemma 6.28. *Let Z be a commutative, local, artinian principal ideal ring and $g \in Z[X]$ a generalized Eisenstein polynomial. Write $B = Z[X]/(g)$ and let ϕ_B the valuation on B from proposition 6.16. Let $h \in Z[X]$, $e \in \mathbb{Z}$ and $c_i \in Z[X]$ be as in the definition of generalized Eisenstein.*

Then every element $b \in B$ can be written as

$$b = \sum_{i=0}^{e-1} s_i h^i$$

with

$$s_i = \sum_{j=0}^{\deg h - 1} s_{i,j} X^j \in Z[X].$$

Furthermore, the valuation $\phi_B(b)$ is equal to $\min_{i,j} \phi_B(s_{i,j} h^i)$.

Proof. View $b \in B$ as a polynomial in $Z[X]$ of degree less than $\deg(g)$. Since h is monic, we can use repeated division with remainder by h to write $b = \sum_{i=0}^{e-1} s_i h^i$ with $s_i \in Z[X]$ of degree less than $\deg(h)$.

If b is 0, then every s_i is 0 and and for every i and j we have $\phi_B(b) = \phi_B(s_{i,j} h^i)$. Suppose b is non-zero and let i be such that s_i is non-zero. Since $\deg(s_i) < \deg(h)$, we know that $\phi_B(s_i) = \min_j(\phi_Z(s_{i,j})e)$. For every i with $s_i \neq 0$, the value $\phi_B(s_i h^i) =$

$\min_j(\phi_Z(s_{i,j})e) + i$ is unique. In particular, the minimum of $\phi_B(s_i h^i)$ is unique. It follows that

$$\begin{aligned}\phi_B(b) &= \min_i \phi_B(s_i h^i) \\ &= \min_i \min_j (\phi_Z(s_{i,j})e) + i \\ &= \min_{i,j} \phi_B(s_{i,j} h^i).\end{aligned}$$

□

Proof of proposition 6.27. Let $h, c_i \in Z[X]$ be as in the definition of generalized Eisenstein; write $c_e = 1$. The first claim follows from the lemma; we write

$$g'(X) = \sum_{i=0}^{e-1} (d_i h^{i-1})$$

with $d_i \in Z[X]$ of degree less than $\deg(h)$, and see that

$$\begin{aligned}\phi_B(g'(X)) &= \min_{i,j} \phi_B(d_{i,j} h^i) \\ &\leq \phi_B(d_{e-1,\deg(h)-1} h^{e-1}) \\ &= \phi_B(\deg(g)) + e - 1.\end{aligned}$$

The last statement of the proposition follows from the fact that if e is invertible, then eh' is invertible. The term $eh'h^{e-1}$ in $g'(X) = \sum_{i=0}^{e-1} (c_i' + (i+1)c_{i+1}h')\, h^i$ has valuation $e-1$, which is less than the valuation of the other terms; each of those terms is in $\pi_Z Z[X]$ and therefore has valuation at least e. □

Let Z be a commutative, local, artinian principal ideal ring, not a field; let $\mathfrak{m}$ be the maximal ideal of Z. Suppose $Z/\mathfrak{m}$ is a perfect field. Let A be a commutative Z-algebra such that A is a free Z-module of finite rank n and A is an artinian principal ideal ring.

Write a sub-Z-algebra $B \subset A$ such that B is a free Z-module as a finite product $\prod_i B_i$, where each B_i is isomorphic to $Z[X]/(g_i)$ for some polynomial $g_i \in Z[X]$ that is generalized Eisenstein. Let $\beta_i \in B_i$ be the element corresponding to X. Then B_i is equal to $Z[\beta_i]$ and β_i is a zero of g_i. Define the A-ideal

$$J_B = \{a \in A : a(g_i'(\beta_i)^2)_i = 0\}$$

and recall the definition of

$$I_B = \{a \in A : a(g_i'(\beta_i))_i = 0\}.$$

The ideal J_B does not depend on the choice of β_i, which we will show in the next section.

The last proposition of this section tells us that the condition $I_B^2 = 0$ is satisfied for all B, when l_Z is large enough in comparison to n. It also contains some statements that are useful for checking the conditions of lemma 6.13.

Proposition 6.29. *Let Z be a commutative, local, artinian principal ideal ring; let π_Z be a generator of its maximal ideal. Suppose $Z/\pi_Z Z$ is a perfect field. Let A be a commutative Z-algebra such that A is free of finite rank n as Z-module and A is an artinian principal ideal ring. Suppose $2(\max_{j=1,\dots,n}(\phi_Z(j))+1) \leq l_Z$. Then for every Z-algebra $B \subset A$ that is free as a Z-module we have*

$$I_B^2 = 0,$$

the ring A is complete with respect to J_B and

$$I_B = (g_i'(\beta_i))_i J_B.$$

Proof. First we suppose that B is local and we write $B = Z[X]/(g)$ with g generalized Eisenstein. Then by the previous proposition, we can bound

$$\begin{aligned}\tilde{\phi}_B(g'(X)) &= \frac{\phi_B(g'(X))}{e} \\ &\leq \frac{\phi_B(\deg g)+e-1}{e} = \frac{e\phi_Z(\deg g)+e-1}{e} \\ &< \phi_Z(\deg g)+1 \leq \max_{j=1,\dots,n}(\phi_Z(j))+1.\end{aligned}$$

Since A is free, for each $\mathfrak{n} \in \mathrm{Spec}(A)$ we have by lemma 6.21 that $l_\mathfrak{n}/e_\mathfrak{n} = l_Z$. The claim in the proof of proposition 6.24 now gives for each element $x \in B$ and every pair $\mathfrak{n}, \mathfrak{n}' \in \mathrm{Spec}(A)$ the equality $\tilde{\phi}_\mathfrak{n}(x) = \tilde{\phi}_{\mathfrak{n}'}(x)$, in particular, since ϕ_B was defined as the restriction of $\phi_\mathfrak{m}$ for some $\mathfrak{m} \in \mathrm{MaxSpec}(A)$, we have $\phi_B(g'(X)) = \phi_\mathfrak{n}(g'(X))$.

Let $\delta_1, \delta_2 \in I_B$ and $\mathfrak{n} \in \mathrm{MaxSpec}(A)$. Then in $H_{l_\mathfrak{n}/e_\mathfrak{n}}$ we have the inequality

$$\begin{aligned}\tilde{\phi}_\mathfrak{n}(\delta_1\delta_2) &= \tilde{\phi}_\mathfrak{n}(\delta_1)+\tilde{\phi}_\mathfrak{n}(\delta_2) \\ &\geq 2(l_Z - \tilde{\phi}_\mathfrak{n}(g'(X))) \\ &\geq l_Z + l_Z - 2\left(\max_{j=1,\dots,n}(\phi_Z(j))+1\right) \\ &\geq l_Z.\end{aligned}$$

We see that $\delta_1\delta_2 = 0$ and $I_B^2 = 0$.

For the general case, write $B = \prod_i B_i$ as a product of local rings and let $A = \prod_i A_i$ be the corresponding product from lemma 6.9. Each A_i is free as a Z-module of rank at most n, so the condition is satisfied for each local part. Furthermore, since $I_B = \prod_i I_{B_i}$, where each I_{B_i} is a subset of A_i respectively, we can conclude from the local case that $I_B^2 = \prod_i I_{B_i}^2 = 0$.

The inequality $2\tilde{\phi}_B(g'(X)) < l_Z$ is not an equality, hence J_B is contained in every maximal ideal of A and therefore A is complete with respect to J_B.

If $a \in J_B$ is an element, then the equality $((g_i'(\beta_i))_i a)(g_i'(\beta_i))_i = a(g_i'(\beta_i)^2)_i = 0$ shows that $((g_i'(\beta_i))_i a)$ is an element of I_B. On the other hand, write an element

$a = (a_\mathfrak{m})_\mathfrak{m} \in I_B$ locally as $a_\mathfrak{m} = u_\mathfrak{m}\pi_\mathfrak{m}^{\phi_\mathfrak{m}(a_\mathfrak{m})}$, where $u_\mathfrak{m}$ is a unit in $A_\mathfrak{m}$. Also write $(g_i'(\beta_i)) = (b_\mathfrak{m})_\mathfrak{m}$ locally as $b_\mathfrak{m} = v_\mathfrak{m}\pi_\mathfrak{m}^{\phi_\mathfrak{m}(b_\mathfrak{m})}$, where $v_\mathfrak{m}$ is again a unit in $A_\mathfrak{m}$.

Now $a \in I_B$ implies that $\phi_\mathfrak{m}(a_\mathfrak{m}) - \phi_\mathfrak{m}(b_\mathfrak{m}) \geq l_\mathfrak{m} - 2\phi_\mathfrak{m}(b_\mathfrak{m}) > 0$; this shows that $x_\mathfrak{m} = u_\mathfrak{m}v_\mathfrak{m}^{-1}\pi_\mathfrak{m}^{\phi_\mathfrak{m}(a_\mathfrak{m})-\phi_\mathfrak{m}(b_\mathfrak{m})} \in A_\mathfrak{m}$ is well-defined. Furthermore, the element $x = (x_\mathfrak{m})_\mathfrak{m}$ satisfies $xb^2 = ab = 0$, so it is in J_B. Hence we can write $a = bx$ as an element of $(g_i'(\beta_i))_i J_B$. □

6.5 Equivalence on artinian ideal rings

In this section we will show that the definitions of I_B and $\Delta_{B/Z}$ from the introduction and that of J_B from the previous section depend only on B and not on the choices made. Furthermore, we will show that $\approx$ is an equivalence relation. After that we prove theorem 6.8.

In this section, Z is a commutative, local, artinian principal ideal ring such that the length l_Z of Z is at least 2 and $Z/\pi_Z Z$ is a perfect field. Furthermore, A is a commutative Z-algebra such that $A/\pi_Z^2 A$ is free as $Z/\pi_Z^2 Z$-module and A is an artinian principal ideal ring.

Let $B \subset A$ be a principal ideal sub-Z-algebra that is free as a Z-module. By theorems 6.3 and 6.5 and lemma 6.1 we can write a sub-Z-algebra $B \subset A$ such that B is a free Z-module, as a finite product $\prod_i B_i$ where each B_i is isomorphic to $Z[X]/(g_i)$ for some polynomial $g_i \in Z[X]$ that is generalized Eisenstein. Let $\beta_i \in B_i$ be the element corresponding to X.

Locally, the isomorphism $B_i/g_i'(\beta_i) \cong \Omega_{B_i/Z}$ from lemma 6.10 shows that the discriminant in definition 6.7 does not depend on the choice of β_i. By lemma 6.11 we see that the same is true for products of these local rings.

In similar manner, we show that I_B and J_B are independent of the choice of β; they can be defined in terms of $D_{B/Z}$ as well.

Proposition 6.30. *Let $D_{B/Z}$ be the different defined in section 6.1.2. Then the A-ideal I_B is equal to $\{a \in A : aD_{B/Z} = 0\}$ and J_B is equal to $\{a \in A : aD_{B/Z}^2 = 0\}$.*

Proof. If B is local, then lemma 6.10 tells us that $D_{B/Z} = g'(\beta)B$. Hence in that case we are done.

In general, write $B = \prod_\mathfrak{m} B_\mathfrak{m}$ as a product of local rings and write $A = \prod_\mathfrak{m} A_\mathfrak{m}$ for the corresponding product from lemma 6.9. The $A_\mathfrak{m}$-ideals $I_{B_\mathfrak{m}}$ and $J_{B_\mathfrak{m}}$ satisfy $I_B = \prod_\mathfrak{m} I_{B_\mathfrak{m}}$ and $J_B = \prod_\mathfrak{m} J_{B_\mathfrak{m}}$ respectively. By lemma 6.11, we obtain

$$\begin{aligned} I_B &= \prod_\mathfrak{m} I_{B_\mathfrak{m}} = \prod_\mathfrak{m} \{a_\mathfrak{m} \in A_\mathfrak{m} : a_\mathfrak{m} D_{B_\mathfrak{m}/Z} = 0\} \\ &= \{a \in A : a \prod_\mathfrak{m} D_{B_\mathfrak{m}/Z} = 0\} = \{a \in A : aD_{B/Z} = 0\} \end{aligned}$$

and

$$J_B = \prod_{\mathfrak{m}} J_{B_\mathfrak{m}} = \prod_{\mathfrak{m}} \{a_\mathfrak{m} \in A_\mathfrak{m} : a_\mathfrak{m} D^2_{B_\mathfrak{m}/Z} = 0\}$$
$$= \{a \in A : a \prod_{\mathfrak{m}} D^2_{B_\mathfrak{m}/Z} = 0\} = \{a \in A : aD^2_{B/Z} = 0\}.$$

□

The following lemma ensures we can conclude global statements about B, I_B and $\approx$ from the corresponding local statements.

Lemma 6.31. *Let $B \subset A$ be a principal ideal sub-Z-algebra that is free as a Z-module and satisfies $I_B^2 = 0$. Write $B = \prod_\mathfrak{m} B_\mathfrak{m}$ as a product of local rings, and let $A = \prod_\mathfrak{m} A_\mathfrak{m}$ be the corresponding product from lemma 6.9.*

If $B' \subset A$ is a principal ideal sub-Z-algebra such that $B \approx B'$, then there exist sub-Z-algebras $B'_\mathfrak{m} \subset A_\mathfrak{m}$ such that $B' = \prod_\mathfrak{m} B'_\mathfrak{m}$ and $B_\mathfrak{m} \approx B'_\mathfrak{m}$ as sub-Z-algebras of $A_\mathfrak{m}$.

Proof. For each $\mathfrak{m}$, let $e_\mathfrak{m} \in A$ be the unit of $A_\mathfrak{m}$, that is, the element that is 1 when projected to $A_\mathfrak{m}$ and 0 when projected to a different coordinate. Since $B_\mathfrak{m} \subset A_\mathfrak{m}$ is a subring, $e_\mathfrak{m}$ is in B. Let $\delta \in I_B$ be such that $e_\mathfrak{m} + \delta \in B'$. The elements $(e_\mathfrak{m} + \delta)^2 = e_\mathfrak{m} + 2\delta e_\mathfrak{m}$ and $(e_\mathfrak{m} + \delta)^3 = e_\mathfrak{m} + 3\delta e_\mathfrak{m}$ are in B', and therefore $e_\mathfrak{m} = 3(e_\mathfrak{m} + \delta)^2 - 2(e_\mathfrak{m} + \delta)^3$ is an element of B' as well.

Define $B'_\mathfrak{m}$ to be the projection of B' onto $A_\mathfrak{m}$. Then $B' = \prod_\mathfrak{m} B'_\mathfrak{m}$ holds, because for each $b \in B'$ we have $b = \sum_\mathfrak{m} e_\mathfrak{m} b$. Furthermore, since we can write $I_B = \prod_\mathfrak{m} I_{B_\mathfrak{m}}$, we also see that $B_\mathfrak{m} \approx B'_\mathfrak{m}$. □

Next, we show that $\approx$ is an equivalence relation, a corollary to the following proposition.

Proposition 6.32. *If $B_1, B_2 \subset A$ are principal ideal sub-Z-algebras that are free as Z-modules and satisfy $I^2_{B_1} = I^2_{B_2} = 0$ such that $B_1 \approx B_2$ holds, then B_1 and B_2 are isomorphic as Z-algebras and the ideals I_{B_1} and I_{B_2} are equal.*

Proof. First assume B_1 is local. Write $B_1 = Z[\beta] \cong Z[X]/(g)$, where g is the minimal polynomial of β. Let $\alpha \in B_2$ be such that $\delta = \beta - \alpha \in I_{B_1}$. Then we have $g(\alpha) = g(\beta + \delta) = g(\beta) + \delta g'(\beta) + \delta^2 x$ for some $x \in A$. Since δ is in I_{B_1}, we have $\delta g'(\beta) = 0$, and since $I^2_{B_1} = 0$ holds, we also have $\delta^2 = 0$. Hence we obtain $g(\alpha) = g(\beta) = 0$.

From lemma 6.22 we see that $I_{B_1} \subset \pi_Z A$. The images of B_1 and B_2 in $A/\pi_Z A$ are therefore equal. From $\pi_Z A \cap B_1 = \pi_Z B_1$ and $\pi_Z A \cap B_2 = \pi_Z B_2$ it now follows that $B_1/\pi_Z B_1$ and $B_2/\pi_Z B_2$ are isomorphic as $Z/\pi_Z Z$-algebras. The element β generates $B_1/\pi_Z B_1$ as a Z-algebra and therefore α generates the algebra $B_2/\pi_Z B_2$. By Nakayama's lemma, α generates the algebra B_2. Since B_1 and B_2 are both free over Z and $B_1/\pi_Z B_1$ and $B_2/\pi_Z B_2$ have the same rank over $Z/\pi_Z Z$, we see that $B_2 \cong Z[X]/(g)$ is isomorphic to B_1.

For the second claim of the lemma, let β, α and δ be as in the first part of the proof. Let a be an element of I_{B_1}. Then for some $x \in A$, we have $ag'(\alpha) = ag'(\beta)+a\delta x = 0$. This shows that I_{B_1} is a subset of I_{B_2}. In particular, δ is in I_{B_2}. Therefore, for any $a \in I_{B_2}$, we have for some $x \in A$ the equality $ag'(\beta) = ag'(\alpha) - a\delta x = 0$, which shows the reverse inclusion.

The general case follows from the local case by lemma 6.31. □

Corollary 6.33. *The relation $\approx$ is an equivalence relation.*

Proof. The relation is clearly reflexive. The lemma shows that it is symmetric and if $B_1 \approx B_2$ and $B_2 \approx B_3$, then I_{B_1}, I_{B_2} and I_{B_3} are all equal and the relation becomes transitive. □

We conclude this section with the proof of theorem 6.8.

Proposition 6.34. *If $B_1, B_2 \subset A$ are principal ideal sub-Z-algebras that are free as Z-modules and satisfy $I_{B_1}^2 = I_{B_2}^2 = 0$ such that $B_1 \approx B_2$ holds, then the Z-modules $B_1 \cap I_{B_1}$ and $B_2 \cap I_{B_1}$ are isomorphic.*

Proof. For the local case, we write $B_1 = Z[\beta] \cong Z[X]/(g)$ and $B_1 = Z[\alpha] \cong Z[X]/(g)$, where $\beta - \alpha \in I_{B_1}$. Since $\beta - \alpha \in I_{B_1} = I_{B_2}$, the isomorphism from B_1 to B_2 from proposition 6.32, which sends β to α makes the following diagram commutative.

$$\begin{array}{ccc} B_1 & \xrightarrow{\sim} & B_2 \\ & {\scriptstyle\phi_1}\searrow \quad \swarrow{\scriptstyle\phi_2} & \\ & A/I_{B_1} & \end{array}$$

This induces an isomorphism between $\ker(\phi_1) = B_1 \cap I_{B_1}$ and $\ker(\phi_2) = B_2 \cap I_{B_1}$.

The general case follows from the local case by lemma 6.31. □

Proposition 6.35. *If A is finite and $B \subset A$ is a principal ideal sub-Z-algebra that is free as a Z-module and satisfies $I_B^2 = 0$, then the number of $B' \subset A$ such that $B \approx B'$ is*

$$\frac{\#I_B}{\#(B \cap I_B)}.$$

Proof. First we assume B is local. Write $B = Z[\beta] \cong Z[X]/(g)$. For every $\delta \in I_B$, the element $\beta + \delta$ satisfies $g(\beta + \delta) = g(\beta) + \delta g'(\beta) + \delta^2 x = 0$, where x is some element of A. Hence, the Z-algebra morphism

$$\begin{aligned} \psi : Z[X]/(g) &\to Z[\beta + \delta] \\ X &\mapsto \beta + \delta \end{aligned}$$

is well-defined. It is also clearly surjective. We will show that ψ is injective.

Suppose $h \in Z[X]/(g)$ satisfies $\psi(h) = 0$. We will show with induction that for all k we have $\pi_Z^k \mid h$. For $k = 0$ this amounts to $\pi_Z^0 = 1 \mid h$, which is clearly true. Next, suppose that $\pi_Z^{k-1} \mid h$. From $0 = \psi(h) = h(\beta) + \delta h'(\beta)$ it follows that $h(\beta) = -\delta h'(\beta)$. By lemma 6.22 and the fact that $\pi_Z^{k-1} \mid h'$ we see that $h(\beta) = \delta h'(\beta) \in \pi_Z^k A$, hence $\pi_Z^{l_Z - k} h(\beta) = 0$. Since $Z[\beta]$ is isomorphic to $Z[X]/(g)$ as a Z-algebra, we see that $\pi_Z^{l_Z - k} h = 0$, from which it follows that $\pi_Z^k \mid h$. With induction we obtain $\pi_Z^k \mid h$ for all k, hence $h = 0$ and ψ is injective.

From the proof of proposition 6.32, we see that every B' with $B \approx B'$ is equal to $Z[\beta + \delta]$ for some $\delta \in I_B$. On the other hand, every Z-algebra $Z[\beta + \delta]$ is isomorphic to B and is therefore a local artinian principal ideal ring that is free as a Z-module and satisfies $I_{Z[\beta+\delta]} = 0$. From the choice of δ it is clear that $B \approx Z[\beta + \delta]$. We see that $\{B' : B \approx B'\} = \{Z[\beta + \delta] : \delta \in I_B\}$.

A subalgebra $B' = Z[\beta + \delta_1] \subset A$ with $B \approx B'$ is equal to $Z[\beta + \delta_2]$ if and only if $\delta_1 - \delta_2 \in B' \cap I_B$. Hence, the number of $\delta \in I_B$ such that $B' = Z[\beta + \delta]$ is $\#(B' \cap I_B)$. By the previous proposition this is equal to $\#(B \cap I_B)$.

The general case follows again from the local case by lemma 6.31. □

Stated below is theorem 6.8 with a slight notational modification.

Theorem 6.8. *Let Z be a finite, commutative, local, artinian principal ideal ring, not a field; let π_Z be a generator of its maximal ideal. Let A be a commutative, finite Z-algebra such that A is an artinian principal ideal ring.*

Suppose $B \subset A$ is a local, free, artinian principal ideal sub-Z-algebra satisfying $I_B^2 = 0$. Suppose A is free as a B-module of rank r. Then the number of subalgebras $B' \subset A$ such that $B \approx B'$ is $\Delta_{B/Z}^{r-1}$.

Proof. As modules, A is free over B and B is free over Z, so A is free over Z.

We calculate $\frac{\#I_B}{\#(B \cap I_B)}$. Let $(e_i)_{i=1}^r$ be a basis of A over B. Then we can write

$$\begin{aligned} I_B &= \{a \in A : ag'(\beta) = 0\} \\ &\cong \{(b_i)_i \in B^r : \sum_i (e_i b_i) g'(\beta) = 0\} \\ &= \{(b_i)_i \in B^r : b_i g'(\beta) = 0 \text{ for each } i\} \\ &= \{b \in B : bg'(\beta) = 0\}^r \cong (B/g'(\beta))^r \end{aligned}$$

and

$$\begin{aligned} B \cap I_B &= B \cap \{a \in A : ag'(\beta) = 0\} \\ &= \{a \in B : ag'(\beta) = 0\} \cong B/g'(\beta). \end{aligned}$$

Hence, by the previous proposition, the number of B' such that $B \approx B'$ is

$$\frac{\#I_B}{\#(B \cap I_B)} = \frac{\#(B/g'(\beta))^r}{\#(B/g'(\beta))} = \Delta_{B/Z}^{r-1}.$$

□

Bibliography

[1] M. F. Atiyah, I. G. Macdonald, *Introduction to commutative algebra*, Westview Press, Oxford, 1969.

[2] D. Eisenbud, *Commutative algebra with a view towards algebraic geometry*, Springer-Verlag, New York, 1995.

[3] D. Ford, S. Pauli, X.-F. Roblot, *A fast algorithm for polynomial factorization over* $\mathbb{Q}_p$, Journal de théorie des nombres de Bordeaux, **14** no. 1 (2002), 151–169.

[4] R. Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977.

[5] I. Kaplansky, *Projective modules*, Ann. of Math. **68** (1958), 372–377.

[6] H. Matsumura, *Commutative algebra*, W.A. Benjamin Co., New York, 1970.

[7] `http://planetmath.org/encyclopedia/ProofOfCayleyHamiltonTheoremInACommutativeRing.html`

Chapter 7

Round rings

In this chapter we will use the theory from the previous chapter to prove the bound on the number of round rings that was used in chapter 5.

Recall from section 5.1 that for a prime p, a finite étale $\mathbb{Q}_p$-algebra E and integers $e \geq 1$ and $1 \leq d \leq \deg(E) - 1$, the sets

$$W_{e,d}(E) = \{R \subset \mathcal{O}_E : R \text{ is a sub-}\mathbb{Z}_p\text{-algebra with } \mathcal{O}_E/R \cong (\mathbb{Z}/p^e\mathbb{Z})^d \text{ as groups}\}$$

are the sets of round rings. We will prove the following bound on these sets.

Theorem 7.1. *Define for integers n the constants $c_{10}(n,1) = 0$ and $c_{10}(n,2) = 1$. Furthermore, define for integers n and d with $3 \leq d \leq n-1$ the constant $c_{10}(n,d) = (d-1)(n-d-1)$. Then we can bound*

$$\#W_{e,d}(E) = O_n\big(p^{c_{10}(n,d)}\big),$$

where p ranges over the set of primes, E over the collection of finite étale $\mathbb{Q}_p$-algebras, e over the set of positive integers, d over $\{1, \ldots, \deg(E) - 1\}$, and n is the degree of E.

It is remarkable that the bound in this theorem does not depend on e. When e is large enough, we can use the theory from chapter 6 to determine the structure of round rings. This gives us a bound for $\#W_{e,d}(E)$ that does not depend on e. More precisely, define the number $c_{14}(n,p) = 2\left\lfloor \frac{\log n}{\log p} \right\rfloor + 2$. For the cases where $e \geq c_{14}(n,p)$, there is a bound for $\#W_{e,d}(E)$ that is better than the bound given in theorem 7.1. The exponent in this bound is defined by the following combinatorial problem.

Definition 7.2. *For integers $n \geq 2$ and $1 \leq d \leq n-1$, define the integer $c_{15}(n,d)$ to be the maximum of $d - \sum_{j \in J}(r_j - 1)$ under the constraints that J is a finite set, $r_j \in \mathbb{Z}_{>0}$ are integers and there are integers $e_j \in \mathbb{Z}_{>0}$ such that $d = \sum_{j \in J}((r_j - 1)e_j)$ and $n = \sum_{j \in J}(r_j e_j)$.*

Theorem 7.3. *We can bound*

$$\#W_{e,d}(E) = O_n\big(p^{c_{15}(n,d)}\big),$$

where p ranges over the set of primes, E over the collection of finite étale $\mathbb{Q}_p$-algebras, e over the set of integers with $e \geq c_{14}(\deg(E), p)$, the number d ranges over $\{1, \ldots, \deg(E) - 1\}$, and n is the degree of E.

Moreover, for every quadruple of integers n, d, p, e with p prime, $n \geq 2$, $p > n$, $1 \leq d \leq n-1$ and $e \geq c_{14}(n, p)$, there exists a finite étale $\mathbb{Q}_p$-algebra E of degree n such that

$$\#W_{e,d}(E) \geq p^{c_{15}(n,d)}.$$

We will split the proof of theorem 7.1 in two parts:

1. the cases where $e = 1$;
2. the cases where $e \geq c_{14}(n, p)$.

For each n, there are only finitely many pairs (p, e) with $1 < e < c_{14}(n, p)$. Since in those remaining cases $\#W_{e,d}(E)$ is bounded, for example by the module counting argument in proposition 5.7, the above two cases suffice to prove theorem 7.1.

We will handle the first case in section 7.3. The second case follows from theorem 7.3, which we will prove in section 7.4. We will combine these results in section 7.5 to show theorem 7.1.

7.1 Applicability of chapter 6

For a finite étale $\mathbb{Q}_p$-algebra E, let $V_d(E)$ denote the set of sub-$\mathbb{Z}_p$-algebras $T \subset \mathcal{O}_E$ such that $\mathcal{O}_E/T$ is a free $\mathbb{Z}_p$-module of rank d.

In this section we prove the following result. It expresses that many rings encountered in this chapter, especially those in section 7.4, meet the conditions that make the theory of chapter 6 applicable.

Proposition 7.4. *For every prime p, integers $n \geq 1$, $1 \leq d \leq n$ and $e \geq 2$, finite étale $\mathbb{Q}_p$-algebra E of degree n and ring $R \in W_{e,d}(E)$, the ring $Z = \mathbb{Z}/p^e\mathbb{Z}$ is a finite, commutative, local, artinian principal ideal ring with a perfect residue field, the Z-algebra $A = \mathcal{O}_E/p^e\mathcal{O}_E$ is a finite, commutative, artinian principal ideal ring that is free of finite rank as a Z-module and the sub-Z-algebra $B = R/p^e\mathcal{O}_E \subset A$ is free as a Z-module.*

Recall from section 6.4 the definition of J_B. Let J_R be the inverse image of J_B in $\mathcal{O}_E$. If $e \geq c_{14}(n, p)$, then $\mathcal{O}_E$ is complete with respect to every $\mathcal{O}_E$-ideal J_R and every ring $T \in V_d(E)$ is complete with respect to the T-ideal $J_{T+p^e\mathcal{O}_E} \cap T$.

Lemma 7.5. *For every prime p, every finite étale $\mathbb{Q}_p$-algebra E and every positive integer e, the ring $\mathcal{O}_E/p^e\mathcal{O}_E$ is an artinian principal ideal ring.*

Proof. Write $E = \prod_i E_i$ as a product of fields. The ring $\mathcal{O}_E = \prod_i \mathcal{O}_{E_i}$ is a product of discrete valuation rings. A discrete valuation ring is a principal ideal ring, hence $\mathcal{O}_E$ is a principal ideal ring. The ring $\mathcal{O}_E/p^e\mathcal{O}_E$ is therefore also a principal ideal ring. Since it is finite, it is artinian. □

Lemma 7.6. *Let E be a finite étale $\mathbb{Q}_p$-algebra and let $F \subset E$ be a sub-$\mathbb{Q}_p$-algebra. Then $\mathcal{O}_E/\mathcal{O}_F$ is a free $\mathbb{Z}_p$-module.*

Let $e > 0$ be an integer. Then $(\mathcal{O}_E/p^e\mathcal{O}_E)/(\mathcal{O}_F/p^e\mathcal{O}_F)$ is a free $\mathbb{Z}/p^e\mathbb{Z}$-module.

Proof. Since $\mathcal{O}_F = \mathcal{O}_E \cap F$, there is an injective map from $\mathcal{O}_E/\mathcal{O}_F$ into the $\mathbb{Q}_p$-linear space E/F. The finitely generated $\mathbb{Z}_p$-module $\mathcal{O}_E/\mathcal{O}_F$ is therefore torsion-free, hence free.

From the first part of the proof, we know that the exact sequence $0 \to \mathcal{O}_F \to \mathcal{O}_E \to \mathcal{O}_E/\mathcal{O}_F \to 0$ splits. From this it follows that $p^e\mathcal{O}_E \cap \mathcal{O}_F = p^e\mathcal{O}_F$, and hence that $(\mathcal{O}_E/p^e\mathcal{O}_E)/(\mathcal{O}_F/p^e\mathcal{O}_F)$ is a free $\mathbb{Z}/p^e\mathbb{Z}$-module. □

Lemma 7.7. *For a finite étale $\mathbb{Q}_p$-algebra E, the map from the set*

$$\{T \subset \mathcal{O}_E : T \text{ is a sub-}\mathbb{Z}_p\text{-algebra and } \mathcal{O}_E/T \text{ is a free } \mathbb{Z}_p\text{-module}\}$$

to the set

$$\{F \subset E : F \text{ is a finite étale sub-}\mathbb{Q}_p\text{-algebra}\}$$

that sends a sub-$\mathbb{Z}_p$-algebra T to $T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, is bijective. The inverse of this map sends a finite étale sub-$\mathbb{Q}_p$-algebra F to $\mathcal{O}_F$.

Proof. First of all we will show that this map and its claimed inverse are well-defined. From part 1 of lemma 7.6 we see that if F is a finite étale subalgebra of E, then $\mathcal{O}_E/\mathcal{O}_F$ is $\mathbb{Z}_p$-free. On the other hand, if T is a sub-$\mathbb{Z}_p$-algebra of $\mathcal{O}_E$ then $T \otimes \mathbb{Q}_p$ is a sub-$\mathbb{Q}_p$-algebra of E. Every subalgebra of a finite étale algebra is finite étale itself by [1, chapter 5, §6, proposition 3]. (Note that the definition in this reference and our definition of finite étale are the same by [1, chapter 5, §7, theorem 3].)

To show these maps are inverses, let F be a finite étale sub-$\mathbb{Q}_p$-algebra, let x be any element of F and $f \in \mathbb{Z}_p[X]$ a non-zero polynomial that has x as a zero. Let α be the leading coefficient of f. Then αx is integral over $\mathbb{Z}_p$. Hence it follows that $\mathcal{O}_F \otimes \mathbb{Q}_p = F$.

On the other hand, let T be a sub-$\mathbb{Z}_p$-algebra of $\mathcal{O}_E$ such that $\mathcal{O}_E/T$ is a free $\mathbb{Z}_p$-module. We have the inclusions $T \subset \mathcal{O}_{T\otimes\mathbb{Q}_p} \subset \mathcal{O}_E$. We also have the equality $\mathcal{O}_{T\otimes\mathbb{Q}_p} \otimes \mathbb{Q}_p = T \otimes \mathbb{Q}_p$, from which it follows that $(\mathcal{O}_{T\otimes\mathbb{Q}_p}/T) \otimes \mathbb{Q}_p = 0$. This implies $\mathcal{O}_{T\otimes\mathbb{Q}_p}/T$ is torsion. However, $\mathcal{O}_{T\otimes\mathbb{Q}_p}/T$ is a subgroup of $\mathcal{O}_E/T$, which is torsion-free. We conclude that $\mathcal{O}_{T\otimes\mathbb{Q}_p} = T$. □

Proof of proposition 7.4. Since A is a finite ring, all finiteness conditions on Z, A and B are satisfied. The ring Z is clearly a principal ideal ring. The ring A is free over Z by lemma 7.6 and a principal ideal ring by lemma 7.5. The subring B is free over Z by the choice of R and [2, proposition 2.9].

The condition $e \geq c_{14}(n,p)$ is equivalent to $2(\max_{j=1,\ldots,n}(\phi_Z(j)) + 1) \leq l_Z$, with ϕ_Z and l_Z as defined in proposition 6.16 and lemma 6.21 respectively. Hence, by proposition 6.29, the ideal J_R is nowhere equal to $\mathcal{O}_E$, so $\mathcal{O}_E$ is complete with respect to J_R. For $T \in V_d(E)$ there is, by lemma 7.7, a finite étale $\mathbb{Q}_p$-algebra F such that $T = \mathcal{O}_F$, hence T is complete with respect to $J_{T+p^e\mathcal{O}_E} \cap T$. □

7.2 Finite étale $\mathbb{Q}_p$-algebras

In this section, E denotes a finite étale $\mathbb{Q}_p$-algebra, n denotes its degree. The integers d and e satisfy $1 \leq d \leq n$ and $e \geq 2$.

The theory from chapter 6 now gives us an equivalence relation on $W_{e,d}(E)$ and a bound for the size of each class. In section 7.4 we will show that each equivalence class contains exactly one element of the form $T + p^e\mathcal{O}_E$ for some $T \in V_d(E)$. To complete the counting of $W_{e,d}(E)$ we bound the number of elements of $V_d(E)$ and hence the number of equivalence classes.

Proposition 7.8. *We can bound $\#V_d(E) = O_n(1)$, where p ranges over all primes, E over all finite étale $\mathbb{Q}_p$-algebras, n is the degree of E and d ranges over all integers with $1 \leq d \leq n-1$.*

For a finite étale algebra E over a field L, we denote by $Y(E)$ the set of subalgebras of E and by $Y_d(E)$ the subset of algebras of codimension d. Furthermore, we denote the set of equivalence relations on $\mathrm{Spec}(L^n)$ by $C(n)$ and the subset of relations with $n-d$ equivalence classes by $C_d(n)$.

Lemma 7.9. *Let L be a field and n an integer. The map*

$$\begin{aligned}\phi : C(n) &\to Y(L^n)\\ \sim &\mapsto \{x \in L^n : i \sim j \implies x_i = x_j\}\end{aligned}$$

is bijective. For each integer d it maps $C_d(n)$ to $Y_d(L^n)$.

Proof. Let $\sim$ be an equivalence relation and define for each equivalence class c the element $e_c \in L^n$ to be the element that is 1 on coordinates in c and 0 otherwise. The set $\{e_c\}_c$ forms a basis of $\phi(\sim)$ and therefore ϕ is injective and maps equivalence relations to subalgebras of dimension equal to the number of equivalence classes.

To see that ϕ is surjective, we define the map $\psi : Y(L^n) \to C(n)$ that sends an algebra E to the relation $\sim$ that satisfies $i \sim j \iff (\forall x \in E : x_i = x_j)$. Clearly, we have for all $E \in Y(L^n)$ the inclusion $E \subset \phi\psi(E)$. Define for each equivalence class c of $\psi(E)$ the maximal ideal $\mathfrak{m}_c$ to be the kernel of the map

$$\begin{aligned}E &\to L\\ x &\mapsto x_c.\end{aligned}$$

If c' is a different equivalence class, then, by definition of ψ, there is an element $x \in E$ such that $x_c \neq x'_c$. The element $x - x_c$ is in $\mathfrak{m}_c$, but not in $\mathfrak{m}_{c'}$. Hence these ideals are

different. We see that $\dim(E) \geq \#\mathrm{Spec}(E) \geq \#\{c : c \text{ equivalence class of } \psi(E)\} = \dim \phi\psi(E)$, so E and $\phi\psi(E)$ are equal and ϕ is surjective. □

Proof of proposition 7.8. For a finite étale $\mathbb{Q}_p$-algebra E, there exists a field extension L of $\mathbb{Q}_p$ such that $E \otimes L \cong L^n$. Milne [5, chapter I, §3, proposition 3.1] shows this for example for $L = \bar{\mathbb{Q}}_p$. Let L be such a field. Since for every subalgebra $F \subset E$ we have $F = (F \otimes L) \cap E$, the map

$$\begin{aligned} Y_d(E) &\to Y_d(E \otimes L) \\ F &\mapsto F \otimes L \end{aligned}$$

is injective. Hence we can bound

$$\#V_d(E) = Y_d(E) \leq \#Y_d(E \otimes L) = \#Y_d(L^n) = \#C_d(n) = O_n(1),$$

where the first equality follows from lemma 7.7 and the equality $\#Y_d(L^n) = \#C_d(n)$ follows from lemma 7.9. □

7.3 Maximal subrings

In this section, E denotes a finite étale $\mathbb{Q}_p$-algebra, n denotes its degree. The integer d satisfies $1 \leq d \leq n$. We prove theorem 7.1 in the cases where $e = 1$. The result is the following.

Proposition 7.10. *Define for positive integers n the constants $c_{10}(n, 1) = 0$ and $c_{10}(n, 2) = 1$. Furthermore, define for integers n and d with $3 \leq d \leq n - 1$ the constant $c_{10}(n, d) = (d - 1)(n - d - 1)$. Then we can bound*

$$\#W_{1,d}(E) = O_n(p^{c_{10}(n,d)}),$$

where p ranges over the set of primes, E over the collection of finite étale $\mathbb{Q}_p$-algebras, d over the set $\{1, \ldots, \deg(E) - 1\}$, and n is the degree of E.

We start the proof by first describing the ring $\mathcal{O}_E/p\mathcal{O}_E$.

Lemma 7.11. *Let p be a prime and A a commutative ring. Then the following are equivalent:*

1. *there is a finite étale $\mathbb{Q}_p$-algebra E such that $A \cong \mathcal{O}_E/p\mathcal{O}_E$;*
2. *A is a principal ideal ring of characteristic p and has finite dimension as an $\mathbb{F}_p$-module;*
3. *there is a finite index set I and for each $i \in I$ integers $e_i \geq 1$ and $f_i \geq 1$ such that $A \cong \prod_{i \in I} \mathbb{F}_{p^{f_i}}[X_i]/(X_i^{e_i})$.*

Proof. Assuming the first condition is true, we show the second is as well. Let E be a finite étale $\mathbb{Q}_p$-algebra. Lemma 7.5 shows $\mathcal{O}_E/p\mathcal{O}_E$ is a principal ideal ring. It is also clearly of characteristic p and since $\mathcal{O}_E/p\mathcal{O}_E$ is finite, it is of finite dimension as an $\mathbb{F}_p$-module.

Assuming the second condition is true, we show the third is as well. Let A be a commutative principal ideal ring of characteristic p of finite dimension as $\mathbb{F}_p$-module. Since A is finite, it is artinian and we can write $A = \prod_{i\in I} A_i$, where I is a finite set and each A_i is a local artinian principal ideal ring of characteristic p. Let X_i be a generator of the maximal ideal of A_i, then $A_i/(X_i)$ is a finite field of characteristic p; let f_i be its dimension over $\mathbb{F}_p$. Let e_i be the smallest integer such that $X_i^{e_i} = 0$.

Let m_i be an integer such that $p^{m_i} > e_i$. Then the map

$$\begin{aligned} \mathbb{F}_{p^{f_i}} \cong A_i/(X_i) &\to A_i \\ a + (X_i) &\mapsto a^{p^{m_i}} \end{aligned}$$

is a well-defined injective ring morphism. This morphism can be extended to a morphism

$$\begin{aligned} \mathbb{F}_{p^{f_i}}[X_i]/(X_i^{e_i}) &\to A_i \\ X_i &\mapsto X_i, \end{aligned}$$

which is easily seen to be surjective. The kernel of this last morphism is an ideal of $\mathbb{F}_{p^{f_i}}[X_i]/(X_i^{e_i})$ and is therefore generated by X_i^k for some integer $0 \leq k \leq e_i$. By the choice of e_i, the integer k cannot be less than e_i. Hence we have an isomorphism $A_i \cong \mathbb{F}_{p^{f_i}}[X_i]/(X_i^{e_i})$.

Finally, assuming the third condition is true, we show the first is as well. For each i in some finite set I, let e_i and f_i integers. Let $h_i \in \mathbb{Z}_p[X]$ be a monic polynomial of degree f_i that is irreducible in $\mathbb{Z}/p\mathbb{Z}[X]$ and define the field

$$E_i = (\mathbb{Q}_p[X]/(h_i))[Y]/(Y^{e_i} - p).$$

The finite étale $\mathbb{Q}_p$-algebra $E = \prod_i E_i$ satisfies $\mathcal{O}_E/p\mathcal{O}_E = \prod_i \mathbb{F}_{p^{f_i}}[X_i]/(X_i^{e_i})$. □

A ring $R \in W_{1,d}(E)$ corresponds to the subring $R/p\mathcal{O}_E \subset \mathcal{O}_E/p\mathcal{O}_E$. Each subring is contained in some *maximal* subring.

Definition 7.12. *Let A be a ring. A subring B of A is called* maximal *if there are precisely two rings B' with $B \subset B' \subset A$, namely $B' = B$ and $B' = A$.*

By counting the maximal subrings, we will obtain the required bound for $\#W_{1,d}(E)$ when $d \neq 2$.

Proposition 7.13. *The number of maximal subrings of $\mathbb{F}_{p^f}[X]/(X^e)$ equals $\mathrm{pd}(f)$, the number of prime divisors of f, when $e = 1$ and $\mathrm{pd}(f) + 1$ when $e \geq 2$.*

Proof. Write $A = \mathbb{F}_{p^f}[X]/(X^e)$. We start with the case where $e = 1$. In that case A is a field, and any subring will be equal to a subfield. The maximal subfields correspond to the maximal divisors of f. The number of maximal divisors of f equals the number of prime divisors of f. This finishes the proof in the case $e = 1$.

Now let $e \geq 2$ be an integer and R a maximal subring of A. Look at the quotient map $\phi_1 : A \to A/(X)$. If $\phi_1(R)$ is not the entire image of ϕ, then $\phi_1(R)$ is a maximal subring of $A/(X)$ and R is the entire pre-image of this subring under ϕ_1. As seen in the case where $e = 1$, the number of such subrings equals the number of prime divisors of f.

If $\phi_1(R)$ is the entire image, then we look at the quotient map $\phi_2 : A \to A/(X^2)$. For every $c \in \mathbb{F}_{p^f}^*$ there is an element $c + aX \in \phi_2(R)$. So the element $(c + aX)^{p^f} = c^{p^f} + a^{p^f} X^{p^f} = c$ is also in $\phi_2(R)$. Together with the fact that $0 \in R$, this shows that $\mathbb{F}_{p^f} \subset \phi_2(R)$. If $\phi_2(R) \neq \mathbb{F}_{p^f}$ holds, let $c + aX \in \phi_2(R)$ be an element outside $\mathbb{F}_{p^f}$, then $X = a^{-1}((c + aX) - c)$ is in $\phi_2(R)$. This shows that $\phi_2(R)$ is the entire image. In that case, we obtain by [3, II, lemma 7.4] that the inclusion of R in A is surjective, which contradicts the maximality of R. We are left with the case where $\phi_2(R) = \mathbb{F}_{p^f}$. The entire pre-image of $\mathbb{F}_{p^f}$ is a subring of A, so that is the only maximal ring we had not accounted for. □

Lemma 7.14. *Let $R \subset R_1 \times R_2$ be a subring of a product of two commutative rings such that the projections $P_1 : R \to R_1$ and $P_2 : R \to R_2$ are surjective. Then there are ideals $I_1 \subset R_1$ and $I_2 \subset R_2$ and a ring isomorphism $\psi : R_1/I_1 \to R_2/I_2$ such that $R = \{(r_1, r_2) \in R_1 \times R_2 : \psi(r_1 + I_1) = r_2 + I_2\}$.*

Proof. This follows from the lemma of Goursat on groups [4, I, §12 exercise 5] by noting that the projections are ring morphisms and hence the normal subgroups are ideals. □

Combining lemmas 7.13 and 7.14 we obtain the following uniform bound for the number of maximal subrings of $\mathcal{O}_E/p\mathcal{O}_E$.

Proposition 7.15. *Let A be a commutative principal ideal ring of characteristic p of finite dimension n as an $\mathbb{F}_p$-module. Then the number of maximal subrings of A is at most $\binom{n}{2}$.*

Proof. Write $A \cong \prod_{i \in I} \mathbb{F}_{p^{f_i}}[X_i]/(X_i^{e_i})$ as in lemma 7.11. We prove the proposition by induction on $\#I$. If $I = \{i\}$, then by lemma 7.13 the number of maximal subrings is at most $f_i - 1$ when $e_i = 1$ and f_i when $e_i \geq 2$. In the first case we have $f_i - 1 \leq \binom{f_i}{2} = \binom{n}{2}$; in the second case $f_i \leq \binom{2f_i}{2} \leq \binom{n}{2}$ holds.

Suppose the claim is true for all rings where $\#I$ is smaller. Write $A = R_1 \times R_2$ as product of rings with $R_2 \cong \mathbb{F}_{p^f}[X]/(X^e)$ local. A maximal subring of A is either the pre-image of maximal subring of R_1, the pre-image of a maximal subring of R_2, or it is a ring as described in lemma 7.14.

If a maximal ring $R \subset R_1 \times R_2$ is of the third kind, let the ideals $I_1 \subset R_1$ and $I_2 \subset R_2$ be as in lemma 7.14. Let $J \subsetneq R_2$ be an ideal strictly containing I_2. The ring $R' = \{(r_1, r_2) \in R_1 \times R_2 : \psi(r_1 + J) = r_2 + \psi(J)\}$ is a subring that strictly

contains R. Since this would contradict the maximality of R, the ideal I_2 is maximal and $R_2/I_2 \cong \mathbb{F}_{p^f} \cong R_1/I_1$. For each choice of I_1 there are f isomorphisms. We see that the number of subrings of the third type equals $f \cdot \#\{i \in I(R_1) : f_i = f\}$.

The total number of maximal subrings of A can therefore be bounded from above by $\binom{n-ef}{2} + \binom{ef}{2} + f \cdot \#\{i \in I(R_1) : f_i = f\}$. The number $\#\{i \in I(R_1) : f_i = f\}$ is bounded from above by $\frac{n-ef}{f}$. So the total number of maximal subrings of A is at most

$$\binom{n-ef}{2} + \binom{ef}{2} + \frac{n-ef}{f} f \leq \binom{n-ef}{2} + \binom{ef}{2} + ef(n-ef) = \binom{n}{2},$$

which proves the proposition. □

Note that the bound from the previous proposition is sharp, since for each $i \in I$ we can take $e_i = 1$ and $f_i = 1$ to obtain $\binom{n}{2}$ maximal subrings.

Using this proposition and lemma 5.2, which was proven in section 5.2, we can prove proposition 7.10 for $d \neq 2$. The result is the following proposition. Note that it also gives a bound for $d = 2$. This bound is however not sharp enough.

Proposition 7.10 for $d \neq 2$. *We can bound*

$$\#W_{1,d}(E) = O_n(p^{d-1)(n-d-1)}),$$

where p ranges over the set of primes, E over the collection of finite étale $\mathbb{Q}_p$-algebras, d over $\{1, \ldots, \deg(E) - 1\}$, and n is the degree of E.

Proof. For a finite étale $\mathbb{Q}_p$-algebra E, the quotient $\mathcal{O}_E/p\mathcal{O}_E$ is an artinian principal ideal ring of characteristic p by lemma 7.11. Its dimension as an $\mathbb{F}_p$-module is equal to the degree of E.

Each maximal subring of $\mathcal{O}_E/p\mathcal{O}_E$ can be viewed as an $\mathbb{F}_p$-linear space of dimension at most $n-1$. For each maximal subring R the map

$$\begin{aligned}&\{R' \subset R : R' \text{ is a subring of } \mathbb{F}_p\text{-dimension } n-d\}\\ &\quad \to \{V \subset R/(1 \cdot \mathbb{F}_p) : V \text{ is an } \mathbb{F}_p\text{-linear subspace of dimension } n-d-1\}\end{aligned}$$

is injective. By lemma 5.2 we obtain the inequality

$$\begin{aligned}&\#\{R' \subset R : R' \text{ is a subring of } \mathbb{F}_p\text{-dimension } n-d\}\\ &\qquad \leq p^{(n-d-1)(\dim_{\mathbb{F}_p}(R/1\cdot\mathbb{F}_p)-(n-d-1))}\\ &\qquad \leq p^{(n-d-1)(n-2-(n-d-1))} = p^{(n-d-1)(d-1)}.\end{aligned}$$

By proposition 7.15, we obtain $\#W_{1,d}(E) \leq \binom{n}{2} p^{(n-d-1)(d-1)} = O_n\left(p^{(d-1)(n-d-1)}\right)$. □

For $d = 2$, we use the theory from chapter 4 to show the required bound.

Proposition 7.10 for $d = 2$. *We can bound*

$$\#\{R \subset A : R \text{ is a subring of index } p^2\} = O_n(p),$$

where p ranges over the set of prime numbers and A over the set of artinian principal ideal rings of characteristic p and n is the dimension of A as an $\mathbb{F}_p$-vector space.

Proof. Let A be an artinian principal ideal rings of characteristic p and dimension n as an $\mathbb{F}_p$-vector space. By proposition 7.15 the number of maximal subrings R of index p^2 is bounded from above $\binom{n}{2}$.

To count the non-maximal R, we let B be a subring of A of index p; there are at most $\binom{n}{2}$ of these subrings. By theorem 4.1, there is a bijection between $\{R \subset B : R \text{ is a subring with } B/R \cong \mathbb{Z}/p\mathbb{Z} \text{ as groups}\}$ and $\{I \subset B : I \text{ is an ideal with } B/I \cong (\mathbb{Z}/p\mathbb{Z})^2 \text{ as groups}\}$.

Let $I \subset B$ be an ideal with $B/I \cong (\mathbb{Z}/p\mathbb{Z})^2$ as groups. If there exist two maximal B-ideals that contain I, then I is the product of these maximal ideals. We can bound the number of such ideals from above by $\binom{\#\mathrm{MaxSpec}(B)}{2} \leq \binom{n}{2}$.

On the other hand, if I is contained in only one maximal B-ideal $\mathfrak{m}$, then we localize B at $\mathfrak{m}$ and take $A_\mathfrak{m}$ to be the corresponding part of A from lemma 6.9. If $B_\mathfrak{m} = A_\mathfrak{m}$ holds, then there is only one possible ideal, namely $I = \mathfrak{m}$ when $\mathfrak{m}$ has index p^2, or $I = \mathfrak{m}^2$ when $\mathfrak{m}$ has index p. Otherwise, $B_\mathfrak{m}$ has index p in $A_\mathfrak{m}$. We look at the ideal $I + \mathfrak{m}^2$. If that ideal is equal to $\mathfrak{m}$, then by Nakayama's lemma, $I = \mathfrak{m}$ and we can bound the number of such I from above by n. If $I + \mathfrak{m}^2$ is not equal to $\mathfrak{m}$, then we have inclusions $I \subset I + \mathfrak{m}^2 \subsetneq \mathfrak{m} \subsetneq B_\mathfrak{m}$; combined with $\#B/I = p^2$ this shows that $I = I + \mathfrak{m}^2$ and $I/\mathfrak{m}^2 \subset \mathfrak{m}/\mathfrak{m}^2$ has index p.

Let $\mathfrak{f} = \mathrm{Ann}_{B_\mathfrak{m}}(A_\mathfrak{m}/B_\mathfrak{m})$ be the conductor of $B_\mathfrak{m}$ in $A_\mathfrak{m}$. From theorem 4.1 it follows that $A_\mathfrak{m}/\mathfrak{f} \cong (A_\mathfrak{m}/B_\mathfrak{m})^2$ has p^2 elements. Since $B_\mathfrak{m}$ is a local ring, $\mathfrak{f}$ equals $\mathfrak{m}$ and therefore $\mathfrak{m}$ is an $A_\mathfrak{m}$-ideal. Since $A_\mathfrak{m}$ is a principal ideal ring, we can bound $\#\mathfrak{m}/\mathfrak{m}^2 \leq \#A/\mathfrak{m} = p^2$. Hence, for each $\mathfrak{m}$, the number of ideals I is bounded from above by the number of subgroups of index p in $\mathfrak{m}/\mathfrak{m}^2$; this number is bounded by $p + 1$.

Combining this, we can bound for each subring $B \subset A$ of index p the number

$$\#\{I \subset B : I \text{ is an ideal with } B/I \cong \mathbb{Z}/p\mathbb{Z} \text{ as groups}\} \leq \binom{n}{2} + n + n(p+1).$$

and hence we can bound

$$\begin{aligned}\#\{R \subset A : R \text{ is a subring of index } p^2\} &\leq \binom{n}{2} + \binom{n}{2}\left(\binom{n}{2} + n + n(p+1)\right) \\ &= O_n(p).\end{aligned}$$

□

It is conceivable that the method used to obtain the bound for $d = 2$ can be used to improve the bounds for larger d. However, the bounds in proposition 7.10 are enough for our purposes.

7.4 Approximate lifts

In this section, E denotes a finite étale $\mathbb{Q}_p$-algebra, n denotes its degree. The integers d and e satisfy $1 \leq d \leq n$ and $e \geq c_{14}(n,p) = 2\left\lfloor \frac{\log n}{\log p} \right\rfloor + 2$.

We will prove theorem 7.3 using the theory from the previous chapter and section 7.2. We start by introducing some notation that will be used throughout this section. Most of the notation is a straightforward transcription of the notation from the previous chapter specified to this case.

Notation 7.16. *Let E be a finite étale $\mathbb{Q}_p$-algebra, and $e > 2$ an integer. Let $\phi : \mathcal{O}_E \to \mathcal{O}_E/p^e\mathcal{O}_E$ be the quotient map. For a ring $R \in W_{e,d}(E)$, we define the $\mathcal{O}_E$-ideals $I_R = \phi^{-1}(I_{R/p^e\mathcal{O}_E})$ and $J_R = \phi^{-1}(J_{R/p^e\mathcal{O}_E})$. The definition of $I_{R/p^e\mathcal{O}_E}$ and $J_{R/p^e\mathcal{O}_E}$ can be found in chapter 6 in the introduction and in section 6.4, respectively. For a $\mathbb{Z}_p$-algebra $T \subset \mathcal{O}_E$, we define $I_T = I_{T+p^e\mathcal{O}_E}$ and $J_T = J_{T+p^e\mathcal{O}_E}$.*

For subrings of a commutative, artinian principal ideal ring A we have defined an equivalence relation $\approx$ in chapter 6, see definition 6.6. For a ring $R \in W_{e,d}(E)$ we call an algebra $T \in V_d(E)$ such that in $\mathcal{O}_E/p^e\mathcal{O}_E$ we have $R/p^e\mathcal{O}_E \approx (T + p^e\mathcal{O}_E)/p^e\mathcal{O}_E$ an *approximate lift of R*. When T is an approximate lift of R, we write $R \approx T$.

Proposition 7.17. *Let e be an integer such that $e \geq c_{14}(n,p) = 2\left\lfloor \frac{\log n}{\log p} \right\rfloor + 2$. Let $R \in W_{e,d}(E)$ be a ring. Then there is a unique approximate lift $T \in V_d(E)$ of R.*

Proof. First we show existence. Assume R is local, let $g \in \mathbb{Z}_p[X]$ be a generalized Eisenstein polynomial and $\beta \in \mathcal{O}_E$ be such that $g(\beta) = 0 \bmod p^e\mathcal{O}_E$ and $R/p^e\mathcal{O}_E = (\mathbb{Z}/p^e\mathbb{Z})[\beta] \cong (\mathbb{Z}/p\mathbb{Z})[X]/(g)$. By the definition of J_R we have $g(\beta) = 0 \bmod g'(\beta)^2 J_R$ and by proposition 6.29 the ring $\mathcal{O}_E$ is complete with respect to J_R. By Hensel's lemma 6.13, there is an element $\alpha \in \mathcal{O}_E$ such that $g(\alpha) = 0$ and $\alpha - \beta \in g'(\beta)J_R = I_R$, where the last equality follows from proposition 6.29. By lemma 6.22 we have $I_R \subset p\mathcal{O}_E$, and therefore the equality $(\mathbb{Z}/p\mathbb{Z})[\alpha] = (\mathbb{Z}/p\mathbb{Z})[\beta]$ as subrings of $\mathcal{O}_E/p\mathcal{O}_E$.

Define the $\mathbb{Z}_p$-algebra $T = \mathbb{Z}_p[\alpha]$. Note that it is generated as a $\mathbb{Z}_p$-module by $\deg(g) = n - d$ elements. The $\mathbb{Z}/p\mathbb{Z}$-module $(T + p\mathcal{O}_E)/\mathcal{O}_E = \mathbb{Z}/p\mathbb{Z}[\alpha] = \mathbb{Z}/p\mathbb{Z}[\beta] = R/p\mathcal{O}_E$ is free of dimension $n-d$. So we can choose a $\mathbb{Z}_p$-module $U \subset \mathcal{O}_E$ such that U is generated by d elements and satisfies $U + T + p\mathcal{O}_E = \mathcal{O}_E$. By Nakayama's lemma we obtain $U + T = \mathcal{O}_E$. The $\mathbb{Z}_p$-module $\mathcal{O}_E$ is in this way generated by $d+(n-d)$ elements. On the other hand, it is free of rank n. So U and T are both free as $\mathbb{Z}_p$-modules of rank d and $n-d$ respectively. Since $\mathcal{O}_E/T = U$ is free of rank d, the $\mathbb{Z}_p$-algebra T is in $V_d(E)$. Since T is free, the $\mathbb{Z}/p^e\mathbb{Z}$-module $(\mathbb{Z}/p^e\mathbb{Z})[\alpha]$ is free, and satisfies $R/p^e\mathcal{O}_E \approx (\mathbb{Z}/p^e\mathbb{Z})[\alpha]$. Hence T is an approximate lift of R.

For general R, let $x \in R/p^e\mathcal{O}_E$ be an idempotent. For x we have $x^2 - x \equiv 0 \bmod p^e$. Since $((x^2-x)')^2 = 4x^2 - 4x + 1 \equiv 1 \bmod x^2 - x$ holds, we obtain $x^2 - x \equiv 0 \bmod (2x-1)^2 p^e$. Since R is complete with respect to p^e, we can use Hensel to lift the idempotents of $R/p^e\mathcal{O}_E$ to R.

So we can write $R = \prod_i R_i$ as product of local rings R_i. Let $\mathcal{O}_E = \prod_i \mathcal{O}_{E_i}$ be the corresponding product from lemma 6.9 and let $T_i \subset \mathcal{O}_{E_i}$ be the approximate lift of R_i. Then $T = \prod_i T_i$ is an approximate lift of R.

Next, we show uniqueness. Let $T_1, T_2 \in V_d(E)$ be such that $(T_1 + p^e\mathcal{O}_E)/p^e\mathcal{O}_E \approx (T_2 + p^e\mathcal{O}_E)/p^e\mathcal{O}_E$.

First we assume that T_1 is local. Let $\alpha_1 \in T_1$ be such that $T_1 = \mathbb{Z}_p[\alpha_1]$ and let $g \in \mathbb{Z}_p[X]$ be the minimal polynomial of α_1. By proposition 6.32, there exists an element $\alpha_2 \in T_2$ such that $\alpha_1 - \alpha_2 \in I_{T_1}$ and $g(\alpha_2) = 0 \bmod p^e\mathcal{O}_E$.

The ring T_2 is complete with respect to $T_2 \cap J_{T_2}$. We apply Hensel's lemma to obtain that there is a unique $\alpha_3 \in T_2$ such that $g(\alpha_3) = 0$ and $\alpha_2 - \alpha_3 \in I_{T_2} = I_{T_1}$. Both α_1 and α_3 are the unique element $\alpha \in \mathcal{O}_E$ such that $g(\alpha) = 0$ and $\alpha - \alpha_2 \in I_{T_1}$, so they are equal and $T_1 \subset T_2$. From lemma 6.31 it follows that $(T_2 + p^e\mathcal{O}_E)/p^e\mathcal{O}_E$ is local, and hence that T_2 is local. By symmetry, we also have $T_2 \subset T_1$.

The general case follows from the local one by applying lemma 6.31 to the $\mathbb{Z}/p^e\mathbb{Z}$-algebras $(T_1 + p^e\mathcal{O}_E)/p^e\mathcal{O}_E$ and $(T_2 + p^e\mathcal{O}_E)/p^e\mathcal{O}_E$. □

For a $\mathbb{Z}_p$-algebra $T \in V_d(E)$, write $T = \prod_{\mathfrak{m} \in \mathrm{MaxSpec}(T)} T_\mathfrak{m}$ as product of local $\mathbb{Z}_p$-algebras and let $\mathcal{O}_E = \prod_{\mathfrak{m} \in \mathrm{MaxSpec}T} (\mathcal{O}_E)_\mathfrak{m}$ be the corresponding product from lemma 6.9. Denote the rank $[(\mathcal{O}_E)_\mathfrak{m} : T_\mathfrak{m}]$ by $r_\mathfrak{m}$, the inertia degree of $T_\mathfrak{m}/\mathbb{Z}_p$ by $f_\mathfrak{m}$ and the ramification index of $T_\mathfrak{m}/\mathbb{Z}_p$ by $e_\mathfrak{m}$.

Proposition 7.18. *Let E be a finite étale $\mathbb{Q}_p$-algebra, d a positive integer smaller than the degree of E and $T \in V_d(E)$ a $\mathbb{Z}_p$-algebra; let $e \geq c_{14}(n,p) = 2\left\lfloor \frac{\log n}{\log p} \right\rfloor + 2$ be an integer.*

1. *If p is greater than n, then we have*

$$\#\{R \in W_{e,d}(E) : R \approx T\} = p^{\sum_\mathfrak{m} f_\mathfrak{m}(e_\mathfrak{m}-1)(r_\mathfrak{m}-1)}.$$

2. *For $p \leq n$, we can bound*

$$\#\{R \in W_{e,d}(E) : R \approx T\} = O_n(1),$$

where p ranges over the set of primes less than n, the T ranges over $V_d(E)$ for a finite étale $\mathbb{Q}_p$-algebra E of degree n, and $1 \leq d \leq n-1$ and $e \geq c_{14}(n,p)$ are integers.

Proof. By theorem 6.5 we can write the ring T as product $T = \prod_{\mathfrak{m} \in \mathrm{MaxSpec}(T)} T_\mathfrak{m} = \prod_\mathfrak{m} \mathbb{Z}_p[\alpha_\mathfrak{m}] \cong \prod_\mathfrak{m} \mathbb{Z}_p[X]/(g_\mathfrak{m})$ where each $g_\mathfrak{m}$ is the minimal polynomial of $\alpha_\mathfrak{m}$ and

is generalized Eisenstein. Let Z be the ring $\mathbb{Z}/p^e\mathbb{Z}$. Theorem 6.8 tells us that

$$\#\{R \in W_{e,d}(E) : R \approx T\} = \prod_{\mathfrak{m}} \Delta^{r_{\mathfrak{m}}-1}_{((T_{\mathfrak{m}}+p^e\mathcal{O}_E)/p^e\mathcal{O}_E)/Z} = \prod_{\mathfrak{m}} \left(\#(T_{\mathfrak{m}}/g'_{\mathfrak{m}}(\alpha_{\mathfrak{m}}))\right)^{r_{\mathfrak{m}}-1}.$$

If $p > n$, then $e_{\mathfrak{m}}$ is invertible in Z, so by proposition 6.27, we have $\#T_{\mathfrak{m}}/g'(\alpha_{\mathfrak{m}}) = p^{f_{\mathfrak{m}}(e_{\mathfrak{m}}-1)}$. Hence in the first case, the number $\#\{R \in W_{e,d}(E) : R \approx T\}$ is equal to $\prod_{\mathfrak{m}} \left(p^{f_{\mathfrak{m}}(e_{\mathfrak{m}}-1)}\right)^{r_{\mathfrak{m}}-1} = p^{\sum_{\mathfrak{m}} f_{\mathfrak{m}}(e_{\mathfrak{m}}-1)(r_{\mathfrak{m}}-1)}$.

In the case where $p \leq n$, we let $\phi_{\mathfrak{m}}$ be the valuation on the local principal ideal Z-algebra $(T_{\mathfrak{m}} + p^e\mathcal{O}_E)/p^e\mathcal{O}_E$. Since $\deg(g_{\mathfrak{m}}) \leq n$, we know that $\phi_{\mathfrak{m}}(\deg(g_{\mathfrak{m}})) \leq \max_{j \leq n} \phi_{\mathfrak{m}}(j) = e_{\mathfrak{m}} \left\lfloor \frac{\log n}{\log p} \right\rfloor < e_{\mathfrak{m}} e$. Hence $\phi_{\mathfrak{m}}(\deg(g_{\mathfrak{m}})) \in H_{l_{\mathfrak{m}}}$ is represented in $H_{l_{\mathfrak{m}}} = \mathbb{Z}/\sim$ by a unique integer, which we will also denote by $\phi_{\mathfrak{m}}(\deg(g_{\mathfrak{m}}))$. We now use proposition 6.27 to bound $\#T_{\mathfrak{m}}/g'(\alpha_{\mathfrak{m}}) \leq p^{f_{\mathfrak{m}}(\phi_{\mathfrak{m}}(\deg(g_{\mathfrak{m}}))+e_{\mathfrak{m}}-1)}$

From the inequality

$$p^{f_{\mathfrak{m}}(\phi_{\mathfrak{m}}(\deg(g_{\mathfrak{m}}))+e_{\mathfrak{m}}-1)} \leq p^{e_{\mathfrak{m}} f_{\mathfrak{m}}\left(\frac{\log n}{\log p}+e_{\mathfrak{m}}-1\right)} = n^{e_{\mathfrak{m}} f_{\mathfrak{m}}} p^{f_{\mathfrak{m}}(e_{\mathfrak{m}}-1)}$$

we can now bound, using $n = [\mathcal{O}_E : \mathbb{Z}_p] = \sum_{\mathfrak{m}} [(\mathcal{O}_E)_{\mathfrak{m}} : T_{\mathfrak{m}}][T_{\mathfrak{m}} : \mathbb{Z}_p] = \sum_{\mathfrak{m}} r_{\mathfrak{m}} f_{\mathfrak{m}} e_{\mathfrak{m}}$,

$$\#\{R \in W_{e,d}(E) : R \approx T\} \leq \prod_{\mathfrak{m}} (n^{e_{\mathfrak{m}} f_{\mathfrak{m}}} p^{f_{\mathfrak{m}}(e_{\mathfrak{m}}-1)})^{r_{\mathfrak{m}}-1} \leq n^n p^n \leq n^{2n}.$$

Hence, $\#\{R \in W_{e,d}(E) : R \approx T\} = O_n(1)$ is as required. □

Recall the definition of $c_{15}(n,d)$ from the introduction to the present chapter. We will prove theorem 7.3, restated below.

Theorem 7.3. *We can bound*

$$\#W_{e,d}(E) = O_n\left(p^{c_{15}(n,d)}\right),$$

where p ranges over the set of primes, E over the collection of finite étale $\mathbb{Q}_p$-algebras, e over the set of integers with $e \geq c_{14}(\deg(E), p)$, the number d ranges over $\{1, \ldots, \deg(E) - 1\}$, and n is the degree of E.

Moreover, for every quadruple of integers n, d, p, e with $n \geq 2$, $1 \leq d \leq n-1$, $p > n$ with p prime and $e \geq c_{14}(n,p)$, there exists a finite étale $\mathbb{Q}_p$-algebra E of degree n such that

$$\#W_{e,d}(E) \geq p^{c_{15}(n,d)}.$$

Proof. We first look at the case where $p > n$. Let $T \in V_d(E)$ be a $\mathbb{Z}_p$-algebra. From [6, I §4, proposition 10] we have $n - d = [T : \mathbb{Z}_p] = \sum_{\mathfrak{m}} [T_{\mathfrak{m}} : \mathbb{Z}_p] = \sum_{\mathfrak{m}} e_{\mathfrak{m}} f_{\mathfrak{m}}$ and $n = [\mathcal{O}_E : \mathbb{Z}_p] = \sum_{\mathfrak{m}} [(\mathcal{O}_E)_{\mathfrak{m}} : T_{\mathfrak{m}}][T_{\mathfrak{m}} : \mathbb{Z}_p] = \sum_{\mathfrak{m}} r_{\mathfrak{m}} e_{\mathfrak{m}} f_{\mathfrak{m}}$.

Proposition 7.18 tells us that a uniform upper bound for $\#\{R \in W_{e,d}(E) : R \approx T\}$ over all $T \in V_d(E)$ can be found by maximizing the quantity $\sum_{\mathfrak{m}} f_{\mathfrak{m}}(e_{\mathfrak{m}}-1)(r_{\mathfrak{m}}-1) =$

$d - \sum_{\mathfrak{m}} f_{\mathfrak{m}}(r_{\mathfrak{m}} - 1)$ under the constraints that $d = \sum_{\mathfrak{m}}(r_{\mathfrak{m}} - 1)e_{\mathfrak{m}}f_{\mathfrak{m}}$ and $n = \sum_{\mathfrak{m}} r_{\mathfrak{m}}e_{\mathfrak{m}}f_{\mathfrak{m}}$; if the maximum is M, then p^M is a uniform upper bound. Now, if the system of integers $(e_{\mathfrak{m}}, f_{\mathfrak{m}}, r_{\mathfrak{m}})_{\mathfrak{m}}$ satisfies the constraints and at least one $f_{\mathfrak{m}}$ is greater than 1, then the solution $(e'_{\mathfrak{m}}, f'_{\mathfrak{m}}, r'_{\mathfrak{m}})_{\mathfrak{m}} = (e_{\mathfrak{m}}f_{\mathfrak{m}}, 1, r_{\mathfrak{m}})_{\mathfrak{m}}$ has a higher value for $d - \sum_{\mathfrak{m}} f_{\mathfrak{m}}(r_{\mathfrak{m}} - 1)$, so the maximum is attained when all $f_{\mathfrak{m}}$ equal 1. Hence for $p > n$ and $e \geq c_{14}(n, p)$ we obtain the uniform bound $\#\{R \in W_{e,d}(E) : R \approx T\} \leq p^{c_{15}(n,d)}$ for all $T \in V_d(E)$.

From proposition 7.8 we know that $\#V_d(E) = O_n(1)$. Hence, if $p > n$ and $e \geq c_{14}(n, p)$, then we have

$$\#W_{e,d}(E) \leq O_n\big(p^{c_{15}(n,d)}\big).$$

By combining proposition 7.8 and the second part of proposition 7.18 we obtain for $p \leq n$ the bound $\#W_{e,d}(E) = O_n(1)$.

For the final statement of the theorem, we let $(e_j, r_j)_j$ be the integers that maximize $c_{15}(n, d)$. The finite étale $\mathbb{Q}_p$-algebra $E = \prod_j \left(\mathbb{Q}_p[X]/(X^{e_j} - p)\right)^{r_j}$ has degree $\sum_j e_j r_j = n$ and integral closure $\mathcal{O}_E = \prod_j \left(\mathcal{O}_{\mathbb{Q}_p[X]/(X^{e_j}-p)}\right)^{r_j}$. Define the $\mathbb{Z}_p$-algebra $T = \prod_j T_j \subset \mathcal{O}_E$ by letting each $T_j = \mathcal{O}_{\mathbb{Q}_p[X]/(X^{e_j}-p)}$ be the diagonal in $\left(\mathcal{O}_{\mathbb{Q}_p[X]/(X^{e_j}-p)}\right)^{r_j}$. As a $\mathbb{Z}_p$-module $\mathcal{O}_E/T$ is free of dimension $\sum_j e_j(r_j - 1) = d$, so T is in $V_d(E)$. Since we have $p > n$, we can use proposition 7.18 to conclude

$$\#W_{e,d}(E) \geq \#\{R \in W_{e,d}(E) : R \approx T\} = p^{\sum_j (e_j-1)(r_j-1)} = p^{d - \sum_j (r_j - 1)} = p^{c_{15}(n,d)}.$$

□

7.5 Bound on round rings

We will now prove theorem 7.1, the bound on the number of round rings. We start by comparing the exponents of the bounds in proposition 7.10 and theorem 7.3.

Lemma 7.19. *For all integers n and d with $1 \leq d \leq n-1$ the inequality $c_{15}(n, d) \leq c_{10}(n, d)$ holds.*

Proof. We will first show the inequality for $d \neq 2$. It that case, we need to prove that $c_{15}(n, d) \leq (d-1)(n-d-1)$. Since the r_j in definition 7.2 are positive integers and $d = \sum_j (r_j - 1)e_j$ is positive as well, there exists j such that $r_j - 1$ is positive. So we have $c_{15}(n, d) = d - \sum_j (r_j - 1) \leq d - 1$. Therefore the inequality holds if $n - d - 1 \geq 1$.

The only remaining case is $n - d - 1 = 0$. Since we have $n - d = \sum_j e_j$, there is only one possible solution, namely $\#J = 1$ and $e_j = 1$, which implies $r_j = n$. In this case we have $c_{15}(n, d) = d - (n - 1) = 0 = (d - 1)(n - d - 1)$ so the inequality holds.

It remains to show that $c_{15}(n, 2) \leq 1$. Suppose $c_{15}(n, 2) > 1$. Then every r_j is 1 and we obtain $n = \sum_j r_j e_j = \sum_j e_j = d$, which is a contradiction with the requirement $d \leq n - 1$. □

Theorem 7.1. *Define for integers n the constants $c_{10}(n,1) = 0$ and $c_{10}(n,2) = 1$. Furthermore, define for integers n and d with $3 \leq d \leq n-1$ the constant $c_{10}(n,d) = (d-1)(n-d-1)$. Then we can bound*

$$\#W_{e,d}(E) = O_n\left(p^{c_{10}(n,d)}\right),$$

where p ranges over the set of primes, E over the collection of finite étale $\mathbb{Q}_p$-algebras, e over the set of positive integers, d over $\{1, \ldots, \deg(E) - 1\}$, and n is the degree of E.

Proof of theorem 7.1. Proposition 7.10 tells us that $\#W_{1,d}(E) = O_n\left(p^{(d-1)(n-d-1)}\right)$ and combining theorem 7.3 and lemma 7.19 gives $\#W_{e,d}(E) = O_n\left(p^{(d-1)(n-d-1)}\right)$ for $e \geq c_{14}(n,p)$. When we have $p > n$, then $c_{14}(n,p) = 2$ shows we have dealt with all possible values of e. For the remaining cases, $p \leq n$ and $e < 2\left\lfloor \frac{\log n}{\log 2} \right\rfloor + 2$ are both bounded in n. Hence, by proposition 5.7, we can bound $\#W_{e,d}(E) = O_n(1)$, where e is in $\{2, \ldots, c_{14}(n,p) - 1\}$. Combining these three bounds gives $\#W_{e,d}(E) = O_n\left(p^{(d-1)(n-d-1)}\right)$ where e ranges over all positive integers. □

Bibliography

[1] N. Bourbaki, *Algebra II, chapters 4–7*, Springer-Verlag, New York, 1990.

[2] J. A. Buchmann, H. W. Lenstra, Jr., *Approximating rings of integers in number fields*, J. Théor. Nombres Bordeaux **6** (1994), 221–260.

[3] R. Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977.

[4] S. Lang, *Algebra, third edition*, Addison-Wesley, Reading, 1993.

[5] J. S. Milne, *Étale cohomology*, Princeton University Press, Princeton, 1980.

[6] J.-P. Serre, *Local fields*, Springer-Verlag, New York, 1979.

Chapter 8

Quintic rings

In [1] Manjul Bhargava counts the number of number fields of degree 5. One of the results he uses is the following.

Theorem 8.1. *Define for a number field K and integer m the number*

$$f_K(m) = \#\{R \subset \mathcal{O}_K : R \text{ is a subring of index } (\mathcal{O}_K : R) = m\}.$$

Then we can bound

$$\sum_{k=1}^{\infty} f_K(p^k)/p^{2k} = O(1/p^2),$$

where K ranges over all number fields of degree 5 and p over all primes.

The theory from the previous chapters was started to prove this bound. As it is now, it is almost enough to do this. There is one cotype, $(3,1,0,0)$, that requires a little more work. The theory at the end of section 5.5 suffices to prove the required bound on this last cotype. Define for a finite étale $\mathbb{Q}_p$-algebra E of degree n and partition λ of length at most $n-1$ the number

$$f_E(\lambda) = \#\{R \subset \mathcal{O}_E : R \text{ is a subring of cotype } \lambda\}.$$

Proposition 8.2. *Let λ be the partition $(3,1,0,0)$. We can bound*

$$f_E(\lambda) = O(p^6),$$

where p ranges over the set of prime numbers and E over the collection of finite étale $\mathbb{Q}_p$-algebras of degree 5.

Proof. We apply the map $\rho_{1,2}$ from proposition 5.32 to the $\mathbb{Z}_p$-module $\mathcal{O}_E/1 \cdot \mathbb{Z}_p$. This rounding chain map is the product of two rounding maps, so every subring of cotype λ maps to a pair of subrings (R_1, R_2) where R_1 is a subring of $\mathcal{O}_E$ of cotype $(1,0,0,0)$ and R_2 of cotype $(1,1,0,0)$. By proposition 7.10, the number of such pairs is bounded by $\#W_{1,1}(E) \cdot \#W_{1,2}(E) = O(1) \cdot O(p) = O(p)$.

Combining this bound with the bound on the size of the fibres of $\rho_{1,2}$ from proposition 5.32 gives

$$\begin{aligned} f_E(\lambda) &= O(p)O\left(p^{-d_2(r-d_2)(\lambda_{d_2}-2\lambda_{d_2+1})-d_1(d_2-d_1)(\lambda_{d_1}-2\lambda_{d_1+1})+\sum_{i=1}^{r}((r+1-2i)\lambda_i)}\right) \\ &= O(p)O(p^{-2\cdot 2\cdot 1-1\cdot 1\cdot 1+3\cdot 3+1\cdot 1}) = O(p^6). \end{aligned}$$

□

This bound and the bounds from chapter 5 give us enough ingredients to prove theorem 8.1.

Proof of theorem 8.1. Recall the definition of $c_{12}(n,d,\lambda)$ from chapter 5 and define for each partition λ of length at most 4 the constant $c_{16}(\lambda) = \min_{0\le d\le 3} c_{12}(5,d,\lambda)$. The fourth row of table 5a shows that for all these partitions λ we can bound $c_{16}(\lambda) \le \frac{20}{11}k$, where $k = \sum_i \lambda_i$ is the size of the partition. From lemma 5.13 it follows that we can bound $f_E(\lambda) = O(p^{\frac{20}{11}k})$, where λ ranges over the set of partitions of length at most 4.

We will also use the bound $f_E(\lambda) = O(p^{2k-2})$. This bound is worse than the bound above for $k > 11$. There are only a limited number of partitions of size $k \le 11$. A computer search shows that lemma 5.13 suffices to prove the bound $f_E(\lambda) = O(p^{2k-2})$ for all but one partition, namely $(3,1,0,0)$. Proposition 8.2 provides the required bound for this last cotype.

Furthermore, we denote the set of partitions λ of size k and length at most 4 by $\Lambda(k)$ and note that we can bound $\Lambda(k) \le k^4$.

Now we can bound

$$\begin{aligned} \sum_{k=1}^{\infty} f_K(p^k)/p^{2k} &= \sum_{k=1}^{11} f_K(p^k)/p^{2k} + \sum_{k=12}^{\infty} f_K(p^k)/p^{2k} \\ &= \sum_{k=1}^{11} \sum_{\lambda\in\Lambda(k)} O(p^{2k-2}/p^{2k}) + \sum_{k=12}^{\infty} \sum_{\lambda\in\Lambda(k)} O\left(p^{\frac{20}{11}k}\right)/p^{2k} \\ &= O(p^{-2}) + \sum_{k=12}^{\infty} k^4 O\left(p^{\frac{-2}{11}k}\right) \\ &= O(p^{-2}) + O\left(\sum_{k=12}^{\infty} p^{\frac{-2}{12}k}\right) \\ &= O(p^{-2}) + O\left(\frac{p^{-2}}{1-p^{-2/12}}\right) \\ &= O(p^{-2}) \end{aligned}$$

as required. □

Bibliography

[1] M. Bhargava, *The density of discriminants of quintic rings and fields*, Ann. of Math., Princeton, to appear.

Chapter 9

Class numbers for general orders

Let K be a number field of degree n and $\mathcal{O}_K$ its ring of integers. Denote by $\Delta(\mathcal{O}_K)$ the absolute value of the discriminant of $\mathcal{O}_K$ over $\mathbb{Z}$. The *class group* or *Picard group* of $\mathcal{O}_K$ is the group

$$\mathrm{Cl}(\mathcal{O}_K) = \mathrm{Frac}(\mathcal{O}_K)/\mathrm{PFrac}(\mathcal{O}_K).$$

A priori this is the semigroup $\mathrm{Frac}(\mathcal{O}_K)$ divided by the action of $\mathrm{PFrac}(\mathcal{O}_K)$. However, since every fractional $\mathcal{O}_K$-ideal is invertible, the semigroup $\mathrm{Frac}(\mathcal{O}_K)$ is in fact the group $\mathrm{Inv}(\mathcal{O}_K)$, and the quotient becomes a quotient of groups.

From the Minkowski bound [5, chapter V, §4, theorem 4] it follows that the class number $\#\mathrm{Cl}(\mathcal{O}_K)$ satisfies

$$\#\mathrm{Cl}(\mathcal{O}_K) \leq \Delta(\mathcal{O}_K)^{1/2+o_n(1)},$$

where K ranges over the collection of number fields and n is the degree of K, see [6, theorem 6.5] for a proof of this bound.

We will generalize the notion of class group to orders $A \subset \mathcal{O}_K$ of finite index, that is, subrings of $\mathcal{O}_K$ of finite index. Denote this index $(\mathcal{O}_K : A)$ by m and the absolute value of the discriminant of A by $\Delta(A)$. The discriminant of A is related to the discriminant of $\mathcal{O}_K$; we have $\Delta(A) = m^2\Delta(\mathcal{O}_K)$.

There are two ways to generalize the notion of the class group. We define the *Picard group* of A to be

$$\mathrm{Pic}(A) = \mathrm{Inv}(A)/\mathrm{PFrac}(A)$$

and the *class semigroup* of A is

$$\mathrm{Cl}(A) = \mathrm{Frac}(A)/\mathrm{PFrac}(A).$$

For the Picard group, the quotient is a quotient of groups, but for the class semigroup, the quotient is the semigroup $\mathrm{Frac}(A)$ divided out by the action of the group $\mathrm{PFrac}(A)$. Note that $\mathrm{Pic}(A)$ consists of the invertible elements of $\mathrm{Cl}(A)$.

We would like to bound $\#\mathrm{Pic}(A)$ and $\#\mathrm{Cl}(A)$ in terms of the degree n of K and the discriminant $\Delta(A)$ of A. For the Picard group the bound resembles the bound on $\#\mathrm{Cl}(\mathcal{O}_K)$ given above, and for the class semigroup the bound we give has an extra factor depending on the index m and the degree n. The bounds are given in the following two theorems.

Theorem 9.1. *We can bound*

$$\#\mathrm{Pic}(A) \leq \Delta(A)^{1/2+o_n(1)},$$

where K ranges over the collection of number fields, A over the set of suborders of $\mathcal{O}_K$ of finite index and n is the degree of K.

Theorem 9.2. *We can bound*

$$\#\mathrm{Cl}(A) \leq \Delta(\mathcal{O}_K)^{1/2+o_n(1)} m^{2n},$$

where K ranges over the collection of number fields, A over the set of suborders of $\mathcal{O}_K$ of finite index, m is the index of A in $\mathcal{O}_K$ and n is the degree of K.

There are no good lower bounds known for $\mathrm{Cl}(\mathcal{O}_K)$ in terms of $\Delta(\mathcal{O}_K)$. We can give lower bounds when we put the regulator into play.

To define the regulator, we write $\mathcal{O}_K^* \cong T \times \mathbb{Z}^r$ as $\mathbb{Z}$-modules. Here T is a finite torsion group consisting of the roots of unity of $\mathcal{O}_K$; we denote by $w(\mathcal{O}_K)$ the order of this group. The integer $r+1$ is equal to the number of infinite places of K. Define the map

$$\begin{aligned} \mathcal{O}_K^*/T &\to \mathbb{R}^{r+1} \\ x &\mapsto (N_v \log |x|_v)_v, \end{aligned}$$

where v runs over the infinite places of K; if v is real, then we set $N_v = 1$, and if v is complex, we set $N_v = 2$. The image of this map is an r-dimensional lattice. The *regulator* $R(\mathcal{O}_K)$ of $\mathcal{O}_K$ is the co-volume of the projection of this lattice on the first r coordinates. In other words, it is the absolute value of the determinant of the matrix $(N_v \log |x_i|_v)_{i,v=1,\ldots r}$, where $x_1, \ldots, x_r$ is a basis of $\mathcal{O}_K^*/T$. The absolute value of this determinant is independent of the ordering of the places.

The Brauer-Siegel theorem [2] states upper and lower bounds on the product of the class number and the regulator.

Lemma 9.3 (Brauer-Siegel theorem)**.** *We can bound*

$$\frac{\#\mathrm{Cl}(\mathcal{O}_K) \cdot R(\mathcal{O}_K)}{w(\mathcal{O}_K)} = \Delta(\mathcal{O}_K)^{1/2+o_n(1)},$$

where K ranges over the collection of number fields and n is the degree of K.

We can extend the definition of regulator to suborders A of $\mathcal{O}_K$ of finite index. If $(\mathcal{O}_K : A)$ is finite, then $(\mathcal{O}_K^* : A^*)$ is also finite [7, lemma 2.5]. This implies we can write $A^* \cong T_A \times \mathbb{Z}^r$ as $\mathbb{Z}$-modules, where again T_A is a finite torsion group. The definition of $R(A)$, the regulator of A, and $w(A)$ are analogous to the definition for $\mathcal{O}_K$.

The upper bound for the Brauer-Siegel theorem has been generalized for the Picard group of a general order in [7]. We will generalize this even further; we will give a lower bound on $\frac{\#\mathrm{Pic}(A)\cdot R(A)}{w(A)}$ and we will give upper and lower bounds for an analogous quantity related to $\mathrm{Cl}(A)$ instead of $\mathrm{Pic}(A)$.

Theorem 9.4. *We can bound*

$$\frac{\#\mathrm{Pic}(A)\cdot R(A)}{w(A)} = \Delta(A)^{1/2+o_n(1)},$$

where K ranges over the collection of number fields, A over the suborders of $\mathcal{O}_K$ of finite index and n is the degree of K.

For an ideal $I \in \mathrm{Frac}(A)$, we denote the ring $\{x \in K : xI \subset I\}$ by $\mathrm{End}(I)$, called the endomorphism ring. This notation is justified by the fact that there is an isomorphism between $\mathrm{End}(I)$ and the ring $\mathrm{End}_A(I)$ consisting of the A-module endomorphisms of I. We have inclusions $A \subset \mathrm{End}(I) \subset \mathcal{O}_K$. If $I, J \in \mathrm{Frac}(A)$ are such that $[I] = [J]$ in $\mathrm{Cl}(A)$, then their endomorphism rings are equal. We can therefore talk about the endomorphism ring $\mathrm{End}[I]$ for a class $[I]$ in $\mathrm{Cl}(A)$.

Theorem 9.5. *We can bound*

$$\sum_{[I]\in\mathrm{Cl}(A)} \frac{R(\mathrm{End}[I])}{w(\mathrm{End}[I])} \leq \Delta(\mathcal{O}_K)^{1/2+o_n(1)} m^{2n}$$

and

$$\sum_{[I]\in\mathrm{Cl}(A)} \frac{R(\mathrm{End}[I])}{w(\mathrm{End}[I])} \geq \Delta(\mathcal{O}_K)^{1/2+o_n(1)} m^{1+o_n(1)},$$

where K ranges over the collection of number fields, A over the set of suborders of $\mathcal{O}_K$ of finite index, m is the index of A in $\mathcal{O}_K$ and n is the degree of K.

For an ideal class $[I] \in \mathrm{Cl}(\mathcal{O}_K)$, the ring $\mathrm{End}[I]$ is equal to $\mathcal{O}_K$, so the sum

$$\sum_{[I]\in\mathrm{Cl}(\mathcal{O}_K)} \frac{R(\mathrm{End}[I])}{w(\mathrm{End}[I])} = \#\mathrm{Cl}(\mathcal{O}_K)\frac{R(\mathcal{O}_K)}{w(\mathcal{O}_K)}$$

is the same as the quantity studied in the Brauer-Siegel theorem.

The upper and lower bounds in theorem 9.5 are not equal. In fact, these bounds cannot be equal. This follows from the following two theorems. The second of these theorems also shows that the lower bound in theorem 9.5 is sharp.

Theorem 9.6. *For every real $\epsilon > 0$ and integer $n > 1$, there exists $D > 0$ such that for all number fields K of degree n with $\Delta(\mathcal{O}_K) > D$ and all integers M there is a subring $A \subset \mathcal{O}_K$ of index $m > M$ such that*

$$\sum_{[I]\in \mathrm{Cl}(A)} \frac{R(\mathrm{End}[I])}{w(\mathrm{End}[I])} \geq \Delta(\mathcal{O}_K)^{1/2-\epsilon} m^{(n-2)/4}.$$

Theorem 9.7. *For every real $\epsilon > 0$ and integer $n > 1$, there exists $D > 0$ such that for all number fields K of degree n with $\Delta(\mathcal{O}_K) > D$ and all integers M there is a subring $A \subset \mathcal{O}_K$ of index $m > M$ such that*

$$\sum_{[I]\in \mathrm{Cl}(A)} \frac{R(\mathrm{End}[I])}{w(\mathrm{End}[I])} \leq \Delta(\mathcal{O}_K)^{1/2+\epsilon} m.$$

The proofs of theorems 9.1, 9.2, 9.4 and 9.5 have similar structure. We relate the general Picard group or class semigroup to the class group of $\mathcal{O}_K$. The difference can be related to the finite subsemigroup S_A of $\mathrm{Frac}(A)$ consisting of the ideals I that satisfy $I\mathcal{O}_K = \mathcal{O}_K$; we call this semigroup the *normalization kernel*. This semigroup was studied by Dade, Taussky and Zassenhaus in [3]. In that article, they showed some basic properties of this object. Amongst others, they showed that it is indeed a semigroup.

In the next section, the articulation, we will state the relations between $\mathrm{Pic}(A)$, $\mathrm{Cl}(A)$ and $\mathrm{Cl}(\mathcal{O}_K)$ as well as the bounds on S_A. Using these relations and bounds, we prove theorems 9.1, 9.2, 9.4 and 9.5. In sections 9.2–9.4 we prove the relations used in the articulation and in section 9.5 we will prove the various bounds on S_A.

In section 9.6 we prove theorems 9.6 and 9.7.

9.1 Articulation of the proofs

In this section we prove the theorems from the introduction. In those proofs we will use results proved in later sections. We start by stating those results.

Conductors

Let K be a number field. For an order $A \subset \mathcal{O}_K$ of finite index the $\mathcal{O}_K$-ideal $\mathfrak{f}_A = \{x \in \mathcal{O}_K : x\mathcal{O}_K \subset A\}$ is called the *conductor* of A in $\mathcal{O}_K$. If the index $(\mathcal{O}_K : A)$ is m, then we have the inclusion $m\mathcal{O}_K \subset \mathfrak{f}_A$. This shows that $\mathcal{O}_K/\mathfrak{f}_A$ is finite.

Note that the conductor is the largest $\mathcal{O}_K$-ideal contained in A. For fractional A-ideals I that satisfy $I\mathcal{O}_K = \mathcal{O}_K$, we get the inclusion

$$\mathfrak{f}_A = \mathfrak{f}_A\mathcal{O}_K = \mathfrak{f}_A\mathcal{O}_K I \subset AI = I.$$

The normalization kernel

For a number field K and an order $A \subset \mathcal{O}_K$ of finite index, we define the semigroup S_A to be the kernel of the map

$$\begin{aligned} \mathrm{Frac}(A) &\to \mathrm{Frac}(\mathcal{O}_K) \\ I &\mapsto I\mathcal{O}_K. \end{aligned}$$

It consists of all fractional A-ideals I that satisfy $I\mathcal{O}_K = \mathcal{O}_K$. We call this semigroup the *normalization kernel of* A. We know that for every ideal $I \in S_A$ we have the inclusions $\mathfrak{f}_A \subset I \subset \mathcal{O}_K$. Since $\mathcal{O}_K/\mathfrak{f}_A$ is finite, this shows that S_A is finite.

A fractional $\mathcal{O}_K$-ideal does not change if we multiply it by an element of $\mathcal{O}_K^*$. The action of $\mathcal{O}_K^*$ on $\mathrm{Frac}(A)$ therefore stabilizes S_A. This gives us an action of the group $\mathcal{O}_K^*$ on the set S_A. We denote the semigroup of orbits of S_A under this action by $S_A/\mathcal{O}_K^*$. Since S_A^* is stable under this action, we can also define the group $S_A^*/\mathcal{O}_K^*$.

The normalization kernel is used to relate the Picard group and class semigroup of A to those of $\mathcal{O}_K$. To prove bounds on the class numbers of A, we will require some bounds on the size of S_A. The used bounds are given in the following proposition. It is proven in section 9.5.

Proposition 9.8. *The normalization kernel S_A is bounded by*

1. $\#S_A \leq m^{2n}$ *and*
2. $\#S_A^* = m^{1+o_n(1)}$,

where K ranges over the collection of number fields, A over the set of suborders of $\mathcal{O}_K$ of finite index, m is the index of A in $\mathcal{O}_K$ and n is the degree of K.

Relations between class semigroups

The normalization kernel S_A provides a link between the Picard group and class semigroup of A on the one hand and the class group of $\mathcal{O}_K$ on the other hand. For the Picard group the result we use is the following proposition. It is proven in section 9.2.

Proposition 9.9. *For every maximal order $\mathcal{O}_K$ and suborder A there is an exact sequence of groups*

$$1 \to A^* \to \mathcal{O}_K^* \to S_A^* \to \mathrm{Pic}(A) \to \mathrm{Pic}(\mathcal{O}_K) \to 1.$$

For class semigroups, we have a similar result. This is phrased a little differently, since the notion of exact sequence for semigroups cannot be used to bound the relative size of the objects in the sequence. This proposition is proven in section 9.3.

Proposition 9.10. *Each fibre of the map*

$$\begin{aligned} \psi : \mathrm{Cl}(A) &\to \mathrm{Cl}(\mathcal{O}_K) \\ [I] &\mapsto [I\mathcal{O}_K] \end{aligned}$$

has $\#(S_A/\mathcal{O}_K^*)$ elements.

To relate the regulators of A and $\mathcal{O}_K$, we use the following lemma, which is proven in section 9.4.

Lemma 9.11. *For a maximal order $\mathcal{O}_K$ and a suborder A, the equation*

$$(\mathcal{O}_K^* : A^*) = \frac{R(A)w(\mathcal{O}_K)}{w(A)R(\mathcal{O}_K)}$$

holds.

Bounds on class numbers

We now have all the ingredients we use to prove theorems 9.1, 9.2 and 9.4 from the introduction.

Proof of theorem 9.1. The exact sequence from proposition 9.9 gives the equality $\#\mathrm{Pic}(A) = \#(S_A^*/\mathcal{O}_K^*) \cdot \#\mathrm{Pic}(\mathcal{O}_K)$. Using the upper bound on S_A^* from proposition 9.8 and the known bound on $\#\mathrm{Pic}(\mathcal{O}_K)$ we obtain

$$\begin{aligned}\#\mathrm{Pic}(A) &= \#(S_A^*/\mathcal{O}_K^*) \cdot \#\mathrm{Pic}(\mathcal{O}_K) \\ &\leq \#S_A^* \cdot \#\mathrm{Pic}(\mathcal{O}_K) \\ &\leq m^{1+o_n(1)}\Delta(\mathcal{O}_K)^{1/2+o_n(1)} \\ &= \Delta(A)^{1/2+o_n(1)},\end{aligned}$$

the claimed result. □

Proof of theorem 9.2. Proposition 9.10 gives the equality $\#\mathrm{Cl}(A) = \#(S_A/\mathcal{O}_K^*) \cdot \#\mathrm{Cl}(\mathcal{O}_K)$. We bound $\#(S_A/\mathcal{O}_K^*) \leq \#S_A \leq m^{2n}$ using proposition 9.8 and see that

$$\#\mathrm{Cl}(A) = \#(S_A/\mathcal{O}_K^*) \cdot \#\mathrm{Cl}(\mathcal{O}_K) \leq m^{2n}\Delta(\mathcal{O}_K)^{1/2+o_n(1)},$$

as desired. □

Proof of theorem 9.4. The exact sequence from proposition 9.9 gives the equality $\#\mathrm{Pic}(A) \cdot (\mathcal{O}_K^* : A^*) = \#S_A^* \cdot \#\mathrm{Pic}(\mathcal{O}_K)$. Combining this with the equality in lemma 9.11 yields

$$\begin{aligned}\#\mathrm{Pic}(A)\frac{R(A)}{w(A)} &= \#\mathrm{Pic}(A) \cdot (\mathcal{O}_K^* : A^*)\frac{R(\mathcal{O}_K)}{w(\mathcal{O}_K)} \\ &= \#S_A^* \cdot \#\mathrm{Pic}(\mathcal{O}_K)\frac{R(\mathcal{O}_K)}{w(\mathcal{O}_K)} \\ &= m^{1+o_n(1)}\Delta(\mathcal{O}_K)^{1/2+o_n(1)},\end{aligned}$$

where the last step follows from the bound in proposition 9.8 and the Brauer-Siegel theorem. □

The relation $\#\mathrm{Pic}(A)\frac{R(A)}{w(A)} = \#S_A^* \cdot \#\mathrm{Pic}(\mathcal{O}_K)\frac{R(\mathcal{O}_K)}{w(\mathcal{O}_K)}$, which was shown in the previous proof, can be generalized to the class semigroup. The result is the following proposition, which will be proved in section 9.4.

Proposition 9.12. *For a maximal order $\mathcal{O}_K$ and a suborder A, we have*

$$\sum_{[I]\in\mathrm{Cl}(A)} \frac{R(\mathrm{End}[I])}{w(\mathrm{End}[I])} = \#S_A \cdot \#\mathrm{Cl}(\mathcal{O}_K)\frac{R(\mathcal{O}_K)}{w(\mathcal{O}_K)}.$$

This proposition, combined with proposition 9.8 and the Brauer-Siegel theorem allows us to prove theorem 9.5.

Proof of theorem 9.5. Proposition 9.8 gives for $\#S_A$ the upper bound $\#S_A \leq m^{2n}$ and lower bound $\#S_A \geq \#S_A^* = m^{1+o_n(1)}$, so we obtain

$$\sum_{[I]\in\mathrm{Cl}(A)} \frac{R(\mathrm{End}[I])}{w(\mathrm{End}[I])} = \#S_A \cdot \#\mathrm{Cl}(\mathcal{O}_K)\frac{R(\mathcal{O}_K)}{w(\mathcal{O}_K)} \leq m^{2n}\Delta(\mathcal{O}_K)^{1/2+o_n(1)}$$

and

$$\sum_{[I]\in\mathrm{Cl}(A)} \frac{R(\mathrm{End}[I])}{w(\mathrm{End}[I])} = \#S_A \cdot \#\mathrm{Cl}(\mathcal{O}_K)\frac{R(\mathcal{O}_K)}{w(\mathcal{O}_K)} \geq m^{1+o_n(1)}\Delta(\mathcal{O}_K)^{1/2+o_n(1)}.$$

□

Note that we can also obtain the lower bound of this theorem by restricting the sum to the classes $[I] \in \mathrm{Pic}(A)$ and applying theorem 9.4.

9.2 Picard groups

In this section the ring A is an order of finite index in a maximal order $\mathcal{O}_K$. We relate the Picard group of A to that of $\mathcal{O}_K$ and prove proposition 9.9.

Lemma 9.13. *The morphism*

$$\begin{aligned} \mathrm{Inv}(A) &\to \mathrm{Inv}(\mathcal{O}_K) \\ I &\mapsto I\mathcal{O}_K \end{aligned}$$

is surjective.

Proof. [3, corollary 2.1.11]. □

We now prove proposition 9.9, restated below for convenience.

Proposition 9.9. *For every maximal order $\mathcal{O}_K$ and suborder A there is an exact sequence of groups*

$$1 \to A^* \to \mathcal{O}_K^* \to S_A^* \to \mathrm{Pic}(A) \to \mathrm{Pic}(\mathcal{O}_K) \to 1.$$

Proof. Consider the following diagram.

$$\begin{array}{ccccc} 1 & \longrightarrow & K^* & \xrightarrow{\sim} & K^* \\ \downarrow & & \downarrow & & \downarrow \\ S_A^* & \rightarrowtail & \mathrm{Inv}(A) & \twoheadrightarrow & \mathrm{Inv}(\mathcal{O}_K) \end{array}$$

Lemma 9.13 shows the surjectivity of the last arrow in the second row, the rest of the maps are the obvious ones. It is a commutative diagram with exact rows.

Applying the snake lemma [1, proposition 2.10] to this diagram gives the following commutative diagram with exact rows and columns.

$$\begin{array}{ccccc} 1 & \longrightarrow & A^* & \longrightarrow & \mathcal{O}_K^* \\ \downarrow & & \downarrow & & \downarrow \\ 1 & \longrightarrow & K^* & \xrightarrow{\sim} & K^* \\ \downarrow & & \downarrow & & \downarrow \\ S_A^* & \rightarrowtail & \mathrm{Inv}(A) & \twoheadrightarrow & \mathrm{Inv}(\mathcal{O}_K) \\ \downarrow & & \downarrow & & \downarrow \\ S_A^* & \longrightarrow & \mathrm{Pic}(A) & \twoheadrightarrow & \mathrm{Pic}(\mathcal{O}_K) \end{array}$$

The snake is the required exact sequence. □

9.3 Class semigroups

In this section the ring A is an order of finite index in a maximal order $\mathcal{O}_K$. We relate the class group of A to that of $\mathcal{O}_K$ and prove proposition 9.10, restated below for convenience.

Proposition 9.10. *Each fibre of the map*

$$\begin{aligned} \psi : \mathrm{Cl}(A) &\to \mathrm{Cl}(\mathcal{O}_K) \\ [I] &\mapsto [I\mathcal{O}_K] \end{aligned}$$

has $\#(S_A/\mathcal{O}_K^*)$ elements.

Proof. The group $\mathrm{Inv}(A)$ acts on both $\mathrm{Cl}(A)$ and $\mathrm{Cl}(\mathcal{O}_K)$ and ψ respects these actions. By lemma 9.13 the action on $\mathrm{Cl}(\mathcal{O}_K)$ is transitive. Hence each fibre of ψ has the same number of elements.

It suffices to determine $\#\psi^{-1}([\mathcal{O}_K])$. We have

$$\begin{aligned}\psi^{-1}([\mathcal{O}_K]) &= \{[I] \in \mathrm{Cl}(A) : \exists \alpha \in K^* : \alpha I \mathcal{O}_K = \mathcal{O}_K\} \\ &= \{[I] \in \mathrm{Cl}(A) : I \in \mathrm{Frac}(A), I\mathcal{O}_K = \mathcal{O}_K\}.\end{aligned}$$

Note that in the last description of $\psi^{-1}([\mathcal{O}_K])$ not every $I' \in [I]$ needs to satisfy the condition, only one suffices.

If $I_1, I_2 \in \mathrm{Frac}(A)$ are two ideals such that $I_1\mathcal{O}_K = \mathcal{O}_K = I_2\mathcal{O}_K$ and $[I_1] = [I_2]$ in $\psi^{-1}([\mathcal{O}_K])$, then there exists $\alpha \in K^*$ such that $\alpha I_1 = I_2$. Since we have $\alpha\mathcal{O}_K = \alpha I_1\mathcal{O}_K = I_2\mathcal{O}_K = \mathcal{O}_K$, the element α is in $\mathcal{O}_K^*$. Conversely, if $I_1 = \alpha I_2$ holds for some $\alpha \in \mathcal{O}_K^*$, then clearly $[I_1] = [I_2]$ holds. We obtain the semigroup isomorphism

$$\psi^{-1}([\mathcal{O}_K]) \cong \{I \in \mathrm{Frac}(A) : I\mathcal{O}_K = \mathcal{O}_K\}/\mathcal{O}_K^* = S_A/\mathcal{O}_K^*.$$

□

9.4 Regulators

In this section we prove lemma 9.11 and proposition 9.12. Recall the definition of the regulator $R(A)$ from the introduction and of the torsion group T_A consisting of the roots of unity of the order A. Lemma 9.11 is restated below.

Lemma 9.11. *For a maximal order $\mathcal{O}_K$ and a suborder A, the equation*

$$(\mathcal{O}_K^* : A^*) = \frac{R(A)w(\mathcal{O}_K)}{w(A)R(\mathcal{O}_K)}$$

holds.

Proof. We write the index $(\mathcal{O}_K^* : A^*)$ as product of $(T_{\mathcal{O}_K} : T_A)$ and the index of the lattice A^*/T_A in the lattice $\mathcal{O}_K^*/T_{\mathcal{O}_K}$. By definition, the first factor is $w(\mathcal{O}_K)/w(A)$ and by linear algebra, the lattice index is $R(A)/R(\mathcal{O}_K)$. □

Proposition 9.12. *For a maximal order $\mathcal{O}_K$ and a suborder A, we have*

$$\sum_{[I]\in\mathrm{Cl}(A)} \frac{R(\mathrm{End}[I])}{w(\mathrm{End}[I])} = \#S_A \cdot \#\mathrm{Cl}(\mathcal{O}_K)\frac{R(\mathcal{O}_K)}{w(\mathcal{O}_K)}.$$

Proof. From lemma 9.11 we have

$$\sum_{[I]\in\mathrm{Cl}(A)} \frac{R(\mathrm{End}[I])}{w(\mathrm{End}[I])} = \sum_{[I]\in\mathrm{Cl}(A)} (\mathcal{O}_K^* : \mathrm{End}[I]^*)\frac{R(\mathcal{O}_K)}{w(\mathcal{O}_K)}.$$

The map ψ from proposition 9.10 shows that this is equal to

$$\frac{R(\mathcal{O}_K)}{w(\mathcal{O}_K)} \sum_{[J]\in \mathrm{Cl}(\mathcal{O}_K)} \sum_{[I]\in\psi^{-1}([J])} (\mathcal{O}_K^* : \mathrm{End}[I]^*).$$

Let $\mathfrak{a} \in \mathrm{Inv}(A)$ be a fractional ideal. Then for every fractional ideal $I \in \mathrm{Frac}(A)$ the set $\{x \in K : x\mathfrak{a}I \subset \mathfrak{a}I\}$ is equal to $\{x \in K : xI \subset I\}$. So the action of $\mathrm{Inv}(A)$ on $\mathrm{Frac}(A)$ leaves $\mathrm{End}(I)$ invariant. Since the action of $\mathrm{Inv}(A)$ on $\mathrm{Cl}(\mathcal{O}_K)$ is transitive, the number $\sum_{[I]\in\psi^{-1}([J])}(\mathcal{O}_K^* : \mathrm{End}[I]^*)$ is the same for every $[J] \in \mathrm{Cl}(\mathcal{O}_K)$. Hence we have the equality

$$\sum_{[J]\in \mathrm{Cl}(\mathcal{O}_K)} \sum_{[I]\in\psi^{-1}([J])} (\mathcal{O}_K^* : \mathrm{End}[I]^*) = \#\mathrm{Cl}(\mathcal{O}_K) \sum_{[I]\in\psi^{-1}([\mathcal{O}_K])} (\mathcal{O}_K^* : \mathrm{End}[I]^*).$$

We saw in the proof of proposition 9.10 that the fibre $\psi^{-1}([\mathcal{O}_K])$ is equal to the set $\{[I] \in \mathrm{Cl}(A) : I \in S_A\}/\mathcal{O}_K^*$. Take $I \in S_A$. Then the stabilizer of I under the action of $\mathcal{O}_K^*$ is $\{x \in \mathcal{O}_K^* : xI = I\} = \mathrm{End}(I)^*$. Hence the orbit of I has length $(\mathcal{O}_K^* : \mathrm{End}(I)^*)$. We obtain

$$\#S_A = \sum_{I\in S_A/\mathcal{O}_K*} (\mathcal{O}_K^* : \mathrm{End}(I)^*) = \sum_{[I]\in\psi^{-1}([\mathcal{O}_K])} (\mathcal{O}_K^* : \mathrm{End}[I]^*).$$

□

9.5 The size of the normalization kernel

In this section, we will provide the bounds on the size of the normalization kernel S_A and on the subgroup S_A^* from proposition 9.8.

For the bounds on $\#S_A^*$, we rely heavily on the work of Sands [7].

Proposition 9.14. *For every number field K and order $A \subset \mathcal{O}_K$ there is a group isomorphism*

$$S_A^* \to (\mathcal{O}_K/\mathfrak{f}_A)^*/(A/\mathfrak{f}_A)^*.$$

Proof. This follows from the exact sequence

$$1 \to (A/\mathfrak{f}_A)^* \to (\mathcal{O}_K/\mathfrak{f}_A)^* \to S_A^* \to 1,$$

which is in the proof of [7, theorem 3.7]. □

Proposition 9.15. *Let R be a finite commutative ring such that the additive group is generated n elements and $T \subset R$ a subring of index $m > 1$, then we can bound*

$$(R^* : T^*) > m \left(\frac{3}{\pi^2 \log\log(3m^2)}\right)^{n-1}.$$

Proof. For a prime $\mathfrak{p} \in \mathrm{Spec}(T)$, we define the norm $N\mathfrak{p} = \#T/\mathfrak{p}$. Since T is finite, it can be written as product of local rings $T = \prod_{\mathfrak{p}\in\mathrm{Spec}(T)} T_\mathfrak{p}$. For each local factor $T_\mathfrak{p}$, we have $\#T_\mathfrak{p}^* = \#T_\mathfrak{p}(1 - \frac{1}{N\mathfrak{p}})$. By taking the product, we see

$$\#T^* = \#T \prod_{\mathfrak{p}\in\mathrm{Spec}(T)} \left(1 - \frac{1}{N\mathfrak{p}}\right).$$

Combining this with a similar result for R gives

$$(R^* : T^*) = (R : T)\frac{\prod_{\mathfrak{q}\in\mathrm{Spec}(R)} (1 - 1/N\mathfrak{q})}{\prod_{\mathfrak{p}\in\mathrm{Spec}(T)} (1 - 1/N\mathfrak{p})}.$$

For every prime $\mathfrak{p} \in \mathrm{Spec}(T)$, we choose a prime $\mathfrak{q} \in \mathrm{Spec}(R)$ such that $\mathfrak{q} \cap T = \mathfrak{p}$. For that prime we have $N\mathfrak{q} \geq N\mathfrak{p}$ and hence $1 - 1/N\mathfrak{q} \geq 1 - 1/N\mathfrak{p}$. Let P be the set of all chosen $\mathfrak{q}$. Then we can bound

$$(R^* : T^*) \geq (R : T) \prod_{\mathfrak{q}\in\mathrm{Spec}(R)\setminus P} (1 - 1/N\mathfrak{q}).$$

For each prime number $p \mid m$ there are at most n primes $\mathfrak{q} \in \mathrm{Spec}(R)$ that lie above p, that is, they have a norm that is a power of p. At least one of those is in P, so we can bound the above by

$$(R^* : T^*) \geq m \prod_{p|m} (1 - 1/p)^{n-1}.$$

Define on the set of positive integers the functions $a(m) = \prod_{p|m}(1 - 1/p)$ and $b(m) = \prod_{p|m}(1 + 1/p)$. From [7, proposition 5.2], we have for $m > 1$ the bound $b(m) < 2\log\log(3m^2)$. Combining this with the inequality

$$a(m)b(m) = \prod_{p|m}(1 - 1/p^2) > \prod_{p}(1 - 1/p^2) = \frac{6}{\pi^2}$$

gives the required result. □

Lemma 9.16. *For every number field K and order $A \subset \mathcal{O}_K$ we can bound*

$$\#(\mathcal{O}_K/\mathfrak{f}_A) \leq \#(\mathcal{O}_K/A)^2.$$

Proof. For the orders we are looking at, corollary 2 of [4] amounts to

$$\#(\mathcal{O}_K/\mathfrak{f}_A)\Delta(\mathcal{O}_K) \mid \Delta(A).$$

Combining this with the fact that $\Delta(A) = (\mathcal{O}_K : A)^2\Delta(\mathcal{O}_K)$ gives the result. □

We now prove proposition 9.8, which is restated below.

Proposition 9.8. *The semigroup S_A is bounded by*

1. $\#S_A \leq m^{2n}$ *and*
2. $\#S_A^* = m^{1+o_n(1)}$,

where K ranges over the collection of number fields, A over the set of suborders of $\mathcal{O}_K$ of finite index, m is the index of A in $\mathcal{O}_K$ and n is the degree of K.

Proof. To prove the bound on $\#S_A$, we first note that there is a canonical injection $S_A \to \{G \subset \mathcal{O}_K/\mathfrak{f}_A : G \text{ is a subgroup}\}$. Since $\mathcal{O}_K$ is as group isomorphic to $\mathbb{Z}^n$, we can bound the number of subgroups of $\mathcal{O}_K/\mathfrak{f}_A$ from above by $(\#\mathcal{O}_K/\mathfrak{f}_A)^n$. Combining this with the bound from lemma 9.16 gives the desired result.

To prove the lower bound on $\#S_A^*$, we obtain from proposition 9.14 the equality $\#S_A^* = ((\mathcal{O}_K/\mathfrak{f}_A)^* : (A/\mathfrak{f}_A)^*)$. Applying proposition 9.15 to $\mathcal{O}_K/\mathfrak{f}_A$ and $A/\mathfrak{f}_A$ gives the result

$$\#S_A^* = ((\mathcal{O}_K/\mathfrak{f}_A)^* : (A/\mathfrak{f}_A)^*) \geq m \left(\frac{3}{\pi^2 \log\log(3m^2)} \right)^{n-1} \geq m^{1+o_n(1)}.$$

The upper bound on $\#S_A^*$ follows directly from propositions 5.1 and 5.2 in [7]. Define on the set of positive integers the function $b(m) = \prod_{p|m}(1 + 1/p)$. Then we can bound

$$\#S_A^* \leq m\, b(m)^{n/2} \leq m(2\log\log(3m^2))^{n/2}.$$

□

9.6 Examples

In this section we will construct orders A such that the normalization kernel S_A is large and orders such that this semigroup is small. This will allow us to prove theorems 9.6 and 9.7.

Theorem 9.6. *For every real $\epsilon > 0$ and integer $n > 1$, there exists $D > 0$ such that for all number fields K of degree n with $\Delta(\mathcal{O}_K) > D$ and all integers M there is a subring $A \subset \mathcal{O}_K$ of index $m > M$ such that*

$$\sum_{[I] \in \mathrm{Cl}(A)} \frac{R(\mathrm{End}[I])}{w(\mathrm{End}[I])} \geq \Delta(\mathcal{O}_K)^{1/2-\epsilon} m^{(n-2)/4}.$$

Proof. By the Brauer-Siegel theorem, there exists $D = D(\epsilon)$ such that for all number fields of degree n and discriminant $\Delta(\mathcal{O}_K) > D$ we have

$$\frac{\#\mathrm{Cl}(\mathcal{O}_K)R(\mathcal{O}_K)}{w(\mathcal{O}_K)} \geq \Delta(\mathcal{O}_K)^{1/2-\epsilon}.$$

Take K a number field of degree n and discriminant $\Delta(\mathcal{O}_K) > D$. Let $p > M$ be a prime. Define the subring $A = p\mathcal{O}_K + \mathbb{Z} \subset \mathcal{O}_K$ and the quotient rings $\bar{A} = A/p\mathcal{O}_K$ and $\bar{\mathcal{O}}_K = \mathcal{O}_K/p\mathcal{O}_K$. The index of A in $\mathcal{O}_K$ is $p^{n-1} > M$. Since $\bar{A}$ has conductor 0 in $\bar{\mathcal{O}}_K$, the ring A has conductor $p\mathcal{O}_K$.

For every subgroup $N \subset \mathcal{O}_K$ with $A \subset N$, we define $\bar{N} = N/p\mathcal{O}_K$ and see that N satisfies

$$AN = (p\mathcal{O}_K + \mathbb{Z})N = p\mathcal{O}_K N + N = N$$

and is a fractional A-ideal. Furthermore, N also satisfies $N\mathcal{O}_K \supset A\mathcal{O}_K = \mathcal{O}_K$. So S_A contains the set of subgroups N with $A \subset N \subset \mathcal{O}_K$. The number of these subgroups is at least $p^{(n-1)^2/4}$ when n is odd (take $d = (n-1)/2$ in lemma 5.2) and $p^{n(n-2)/4}$ when n is even (take $d = n/2$).

From proposition 9.12 it now follows that for this particular K and A, we can bound

$$\begin{aligned}\sum_{[I]\in\mathrm{Cl}(A)} \frac{R(\mathrm{End}[I])}{w(\mathrm{End}[I])} &= \#S_A \cdot \#\mathrm{Cl}(\mathcal{O}_K)\frac{R(\mathcal{O}_K)}{w(\mathcal{O}_K)} \\ &\geq p^{n(n-2)/4}\Delta(\mathcal{O}_K)^{1/2-\epsilon} \\ &\geq \Delta(\mathcal{O}_K)^{1/2-\epsilon}m^{(n-2)/4}.\end{aligned}$$

□

The proof of theorem 9.7 goes similarly.

Theorem 9.7. *For every real $\epsilon > 0$ and integer $n > 1$, there exists $D > 0$ such that for all number fields K of degree n with $\Delta(\mathcal{O}_K) > D$ and all integers M there is a subring $A \subset \mathcal{O}_K$ of index $m > M$ such that*

$$\sum_{[I]\in\mathrm{Cl}(A)} \frac{R(\mathrm{End}[I])}{w(\mathrm{End}[I])} \leq \Delta(\mathcal{O}_K)^{1/2+\epsilon}m.$$

Proof. By the Brauer-Siegel theorem, there exists $D = D(\epsilon)$ such that for all number fields K of degree n and discriminant $\Delta(\mathcal{O}_K) > D$ we have

$$\frac{\#\mathrm{Cl}(\mathcal{O}_K)R(\mathcal{O}_K)}{w(\mathcal{O}_K)} \leq \Delta(\mathcal{O}_K)^{1/2+\epsilon}.$$

Take K a number field of degree n and discriminant $\Delta(\mathcal{O}_K) > D$. Let $p > M$ be a prime that splits completely in K and let $\phi : \mathcal{O}_K \to \mathbb{F}_p \times \mathbb{F}_p$ be a surjective

ring morphism. Define the subring $A = \phi^{-1}(\mathbb{F}_p \cdot (1,1)) \subset \mathcal{O}_K$ and the quotient rings $\bar{A} = A/\ker(\phi)$ and $\bar{\mathcal{O}}_K = \mathcal{O}_K/\ker(\phi)$. The ring A has index $p > M$ in $\mathcal{O}_K$ and conductor $\ker(\phi)$.

For every subgroup $N \subset \mathcal{O}_K$ with $\ker(\phi) \subsetneq N$, we define $\bar{N} = N/\ker(\phi)$. Such a subgroup N is an A-ideal if and only if $\bar{N}$ is an $\bar{A}$-module. Such an A-module N satisfies $N\mathcal{O}_K = \mathcal{O}_K$ if and only if it satisfies $\bar{N}\bar{\mathcal{O}}_K = \bar{\mathcal{O}}_K$. Since $\bar{\mathcal{O}}_K$ is isomorphic to $\mathbb{F}_p \times \mathbb{F}_p$, we obtain

$$\#S_A = \#\{I \subset \mathbb{F}_p \times \mathbb{F}_p : I \text{ is an } \mathbb{F}_p\text{-module such that } I(\mathbb{F}_p \times \mathbb{F}_p) = \mathbb{F}_p \times \mathbb{F}_p\} = p,$$

From proposition 9.12 it now follows that for this particular K and A, we can bound

$$\begin{aligned}\sum_{[I] \in \mathrm{Cl}(A)} \frac{R(\mathrm{End}[I])}{w(\mathrm{End}[I])} &= \#S_A \cdot \#\mathrm{Cl}(\mathcal{O}_K) \frac{R(\mathcal{O}_K)}{w(\mathcal{O}_K)} \\ &\leq p\Delta(\mathcal{O}_K)^{1/2+\epsilon} \\ &= \Delta(\mathcal{O}_K)^{1/2+\epsilon} m.\end{aligned}$$

□

Bibliography

[1] M. F. Atiyah, I. G. Macdonald, *Introduction to commutative algebra*, Westview Press, Oxford, 1969.

[2] R. Brauer, *On the zeta-function of algebraic number fields*, Amer. J. Math. **69** (1947), 243–250.

[3] E. C. Dade, O. Taussky, H. Zassenhaus, *On the theory of orders, in particular on the semi-group of ideal classes and genera of an order in an algebraic number field*, Math. Ann. **148** (1962), 31–64.

[4] I. Del Corso, R. Dvornicich, *Relations among discriminant, different, and conductor of an order*, J. of Alg. **224** (2000), 77–90.

[5] S. Lang, *Algebraic number theory, second edition*, Springer-Verlag, New York, 1994.

[6] H. W. Lenstra, Jr., *Algorithms in algebraic number theory*, Bull. Amer. Math. Soc. (N.S.) **26** (1992), 211–244.

[7] J. W. Sands, *Generalization of a theorem of Siegel*, Acta Arith. **58** (1991), 47–57.

Samenvatting

Telproblemen voor getallenringen

Een *getallenlichaam* is een lichaam dat eindig is als vectorruimte over $\mathbb{Q}$, het lichaam van rationale getallen. De dimensie van de vectorruimte heet de *graad* van het getallenlichaam. Een *getallenring* is een domein waarvan het breukenlichaam een getallenlichaam is. Meestal zullen we enkel de getallenringen bekijken die eindig voortgebracht zijn als groep. Een andere naam voor een eindig voortgebrachte getallenring is *orde*.

Aan een orde kennen we twee gehele getallen toe die de grootte van de orde meten. De eerste is de *rang*, die gelijk is aan de graad van het breukenlichaam van de orde. De tweede is de *discriminant*, die de dichtheid van de elementen meet. Een grotere discriminant duidt erop dat de elementen verder van elkaar liggen. Dit is het eenvoudigst te zien voor imaginair kwadratische ordes; voor een positief geheel getal d heeft de orde $\mathbb{Z}[\sqrt{-d}]$ discriminant $4d$, en als we $\mathbb{Z}[\sqrt{-d}]$ in $\mathbb{C}$ inbedden, dan is de oppervlakte van het parallellogram $(0, \sqrt{-d}, 1 + \sqrt{-d}, 1)$ gelijk aan $\sqrt{d}$. Dit parallellogram noemen we een *fundamentaalgebied* van de orde. De discriminant van de orde R duiden we aan met $\Delta(R)$. Merk op dat wat we hier aanduiden met de discriminant de absolute waarde is van de gebruikelijke discriminant.

Wanneer we van een orde de rang en de discriminant weten, dan ligt de orde bijna vast; voor elke rang en discriminant zijn er namelijk maar eindig veel ordes met die rang en discriminant. Dit is een essentieel feit wanneer we ordes willen tellen, maar het helpt niet bij het maken van ordes.

Een manier om een orde te construeren is om een monisch irreducibel polynoom $f \in \mathbb{Z}[X]$ te nemen en uit te delen naar het ideaal dat het voortbrengt. Het resultaat is de ring $\mathbb{Z}[X]/(f)$. Deze ring heeft breukenlichaam $\mathbb{Q}[X]/(f)$ en is daarom een getallenring. Het kan worden ingebed in $\mathbb{C}$ door een nulpunt α van f te kiezen in $\mathbb{C}$ en de afbeelding

$$\begin{aligned} \mathbb{Z}[X]/(f) &\to \mathbb{Z}[\alpha] \\ X &\mapsto \alpha \end{aligned}$$

te nemen. Ordes van dit type heten *monogeen*; we kunnen ze voortbrengen als $\mathbb{Z}$-algebra door één element. De rang van een monogene orde $\mathbb{Z}[\alpha] \cong \mathbb{Z}[X]/(f)$ is gelijk aan de graad van f en de discriminant van deze orde is gelijk aan de absolute waarde van de discriminant van f.

In elk getallenlichaam kunnen we de deelordes van dat getallenlichaam ordenen met inclusie. Er is dan een unieke grootste orde, die alle andere ordes bevat. Deze grootste orde heet de *maximale orde* van dat getallenlichaam. Elke orde heeft eindige index in de maximale orde van zijn breukenlichaam.

Als een orde R bevat is in een grotere orde R' van dezelfde rang, dan is zijn discriminant $\Delta(R)$ deelbaar door de discriminant $\Delta(R')$ van de grotere orde. Het quotiënt is het kwadraat van de index van R in R'.

De ideaalstructuur van een maximale orde $\mathcal{O}$ kunnen we beschrijven met de *klassengroep*, die we aanduiden met $\mathrm{Cl}(\mathcal{O})$. Het is een eindige abelse groep die het verschil meet tussen de groep van gebroken $\mathcal{O}$-idealen en de ondergroep van gebroken hoofdidealen. Als de orde een hoofdideaaldomein is, zoals bijvoorbeeld $\mathbb{Z}[i]$, dan is zijn klassengroep de triviale groep. De grootte van de klassengroep noemen we het *klassengetal* en duiden we aan met $h(\mathcal{O})$.

In dit proefschrift beschouwen we drie telproblemen die te maken hebben met ordes. Het eerste probleem legt een verband tussen de beschrijving van ordes in termen van polynomen en maximale ordes. Het gaat over de vraag wat de kans is dat voor een willekeurig polynoom $f \in \mathbb{Z}[X]$ de orde $\mathbb{Z}[X]/(f)$ de maximale orde van $\mathbb{Q}[X]/(f)$ is.

Het tweede probleem gaat over het tellen van deelordes binnen maximale ordes. We weten dat het aantal deelringen van gegeven index eindig is. We bepalen grenzen voor het aantal deelordes in termen van de rang van de maximale orde en de index van de deelorde.

Het laatste probleem heeft te maken met klassengroepen. Er zijn grenzen bekend voor het klassengetal van maximale ordes, en we gebruiken deze grenzen om grenzen voor het klassengetal van algemene ordes af te leiden.

Curriculum vitae

Jos Brakenhoff werd geboren op 14 november 1980 te Heemskerk. In 1999 behaalde hij het vwo-diploma aan het Jac. P. Thijsse College te Castricum. Daarna begon hij aan de studie wiskunde en statistiek aan de Universiteit Leiden. Hij schreef zijn afstudeerscriptie getiteld *The representation ring and the center of the group ring* onder begeleiding van dr. B. de Smit. Daarmee studeerde hij in februari 2005 cum laude af in de wiskunde.

In mei 2005 begon hij als promovendus bij het Mathematisch Instituut in Leiden. Het promotieonderzoek werd begeleid door prof. dr. H. W. Lenstra en leidde tot dit proefschrift. Hij gaf voordrachten over zijn afstudeer- en promotieonderzoek in Eindhoven, Nijmegen, Heeze, Oberwolfach (Duitsland) en Cetraro (Italië).

Tijdens zijn studie was hij onder andere betrokken bij de training van het Nederlandse team voor de Internationale Wiskunde Olympiade (2001–2002) en de organisatie van de Wetenschapsdag (2001–2002), waarvoor hij van 2001 tot en met 2006 elk jaar een logisch labyrint heeft ontworpen. Verder was hij tijdens zijn studie werkzaam als bureauredacteur van het Nieuw Archief voor Wiskunde (2002–2005). Sinds 2003 helpt hij bij de voorbereiding en begeleiding van de zomerkampen van Vierkant voor Wiskunde.

Buiten de wiskunde is hij actief in het theater. Hij heeft opgetreden met een theatersportgroep, drie musicalgroepen, een toneelvereniging en een minderbroederkoor. Daarnaast heeft hij geacteerd in een aantal kleine projecten.