An Algebraic Interpretation of the Polynomial Szemerédi Theorem

Finding a Lower Bound in the Polynomial Szemerédi Theorem using Algebraic Number Theory

Bachelor Thesis TWIN
January 16, 2020

Author: Mieke Wessel (6011144)
Supervisor: Damaris Schindler

Universiteit Utrecht

Contents

Conventions and Notation

- We will use the convention that zero is not a natural number.
- We will write $A \subset B$ if A is contained or equal to B. If it needs to be stressed that A is solely contained in B we write $A \subsetneq B$.
- The set of all the natural numbers less or equal to a certain $N \in \mathbb{N}$ is denoted by $[N]$.
- For a susbset A of $\mathbb{N}$, the set $(A-A)$ is the difference set defined as $\{a-a' \mid a, a' \in A\}$. It should be especially noted that $(A-A)$ does not denote the set A without A equal to the empty set. If this concept is needed somewhere, it will be written as $A \backslash A$.
- The symbols $\gg$ and $\ll$ are used if the left side grows or declines faster than the right side respectively. So if $f(x) \gg g(x)$, then there are constants c_1 and c_2 such that for all $x > c_2$ we have $f(x) > c_1 g(x)$. If the choices for c also depend on something else, such as f, we will denote this by $\gg_f$.

Chapter 1

Introduction

In every subset of the natural numbers there can be found certain patterns. For example, if we take the set,

$$A = \{1, 2, 3, 5, 7, 10, 13, 17, 21, 26, 31, 37, 43, 50, 57, 65, 73, \ldots\},$$

you might notice that it contains infinitely many 3-terms $(a, a+b, a+2b)$ where a and b are integers or that it contains no values that are divisible by 8. In mathematics we are always very interested in which patterns we can find and why they arise where they do. One way to discover why patterns arise is to look at the circumstances under which they do not arise. In this thesis we will inspect how big subsets of the natural numbers can get while omitting a certain pattern.

The main idea of inspecting these subsets will be to construct a set A with as many elements as possible, but without a chosen pattern, and estimate its size. A simple example is to try and construct a set without any succesive integers. Thus, we are looking for a set A such that if n is an element of A, then $n+1$ is not an element of A. This makes it clear that at most A can contain one of every two natural numbers n and $n+1$. If we choose A to equal the set of all the odd numbers this is also exactly what happens and A does not contain any succesive integers. Though, one should note here that we might just as well choose all the even numbers, and thus that A does not have to be unique. In both cases we could say that our subset A contains 'half' of the natural numbers, or in mathematical terms, that the density of A is 0.5.

Roughly speaking, the density of a set A is the ratio of elements that A has compared to $\mathbb{N}$. This can be calculated by taking the limit for $N \in \mathbb{N}$ of the number of elements A has less or equal to a certain N divided by N. The density of a set is a good way to express how many elements a set has. However, in many cases our choices of patterns will actually lead to a density of zero. In those cases we will be more interested in how fast the limit of the density goes to zero.

Going back to our first example it would also be interesting to construct a set A without

any 3-terms of the form $(a, a+b, a+2b)$. If we do this naively we get the set,

$$A = \{1, 2, 4, 5, 10, 11, 13, 14, 28, 29, 31, 32, 37, 38, 40, 41, 82, \ldots\}.$$

Noteworthy are the gaps between 5 and 10, 14 and 28 and 41 and 82. Here we skip almost half of the integers we could possibly acquire. Also, because $2 \cdot 10 > 14$ and $2 \cdot 28 > 41$ we see that the number of elements that A has compared with $[N]$ reduces after each gap with more than a factor 2. This gives the idea that the ratio can shrink to $\frac{1}{2^c}$ for any $c \in \mathbb{N}$ if N gets big enough, and thus that the density of A is zero. We will not prove it here, but in general it is true that any set $A \subset \mathbb{N}$ that omits these 3-terms has a density of 0.
Even more general we can also say something about the density of a set A omiting the patern of a k-term $(a, a+b, \ldots, a+(k-1)b)$. For such a subset Gowers [9] proved the following theorem.

Theorem 1.1. *Let k be a natural number and let A be some subset of $[N]$ such that it does not contain a k-term of the form $(a, a+b, \cdots, a+(k-1)b)$ for any $a, b \in \mathbb{Z}$ with $b \neq 0$. Then there exists some constant c_k such that,*

$$|A| \leq \frac{N}{\log\log(N)^{c_k}}.$$

Here, c_k depends on k.

From Theorem 1.1 one can derive that any set without any k-terms for a certain k has to have a density of zero. This fact is known as Szemerédi's Theorem and will be elaborated on in Chapter 2. Furthermore, note that the theorem also gives an upper bound for how fast the limit of the density goes to zero.

Now that we have seen some examples of patterns, we can introduce the pattern that will be central in this thesis. The pattern is based on some integer-valued polynomial f. We will try to construct sets A such that A contains no two elements whose difference equal an outcome of f. Thus if we are given some polynomial $f \in \mathbb{Z}[X]$ then we are searching for some subset $A \subset \mathbb{N}$ such that $(A-A) = \{a - a' \mid a, a' \in A\}$ does not contain any value in $\{f(x) \mid x \in \mathbb{Z}\}$ other than zero. Or even more compact we want that $(A-A) \cap \{f(x) \mid x \in \mathbb{Z}\} \subset \{0\}$. To get a better feel for the condition we will first look at some simple examples. During these examples it is important to keep in mind that often there are multiple sets A that meet the criteria and have the same density and/or decline, so the choice for A is rarely unique.

Examples.

- If our polynomial is $f(X) = 1$ we are actually stating the condition that no succesive integers can be in A. Hence, as before, the density of A is 0.5.
- In general, if $f(X) = c$ for any constant $c \in \mathbb{Z}$ one of the biggest subsets we can make is $A = \{1, 2, \ldots, c, 2c+1, \ldots, 3c, 4c+1, \ldots, \}$ (though, this is not the only biggest A). So here we also find that the density of A is 0.5.

- If $f(X) = X$ it is obvious that A can contain at most one element. If it contains any two different elements their difference must be an integer other than zero and those are all in the image of f. So in this case the density of A has to be zero and it will reach this limit as fast as $\frac{1}{N}$ goes to zero.
- In general, if $f(X) = cX$ with $c \in \mathbb{Z}$ we can at most have c elements in A, one for every residue class. As soon as we have two elements of the same residue class the difference of these elements will be a multiple of c. So this also gives A a density of zero where the limit declines with $\frac{c}{N}$.
- If $f(X) = X^2 + X + 1$ we can note that the image of f contains only odd numbers. Because the differences of $\{1, 3, 5, \ldots\}$ are all even it is easy to see that the density of A in this case is 0.5. Though, here A might just as well have been the set $\{2, 4, 6, \ldots\}$.
- Simillarly if $f(X) = X^2 + 1$ the image of f only contains integers that are equivalent to $1 \mod 3$ or to $2 \mod 3$. The set $\{1, 4, 7, 10, \ldots\}$ only has differences that are divisible by three so the density of A has to be at least $\frac{1}{3}$.
- In general, if there exists some $m \in \mathbb{N}$ such that the image of f does not contain any multiples of m, we can choose the subset $\{1, m + 1, 2m + 1, \ldots\}$. This subset has a density of $\frac{1}{m}$, so A has to have a density of at least $\frac{1}{m}$. The density might even by higher if another choice for A is better.

In the previous examples a few things stand out. First of all most of the sets we considered had a positive density. Secondly, the sets that did not have a positive density, only consisted of finitely many elements. However, the examples we have seen so far are the only examples for which one of these is the case. In all other cases it will be impossible to find a set A with density other than zero, and it will be possible to find an infinte set A. The first half of that statement was proved by Kamae and Mendés France [11]. Their ideas are stated in the following definition and theorem.

Definition 1.1. Let $f(X) \in \mathbb{Z}[X]$. Then $f(X)$ is called *intersective* if for all $m \in \mathbb{Z}$ there is some $x \in \mathbb{Z}$ such that $f(x) \equiv 0 \mod m$.

Theorem 1.2. *For any intersective polynomial $f(X) \in \mathbb{Z}[X]$ and set $A \subset \mathbb{N}$ such that $(A - A) \cap \{f(x) \mid x \in \mathbb{Z}\} \subset \{0\}$, the density of A equals zero.*

Now it will be interesting to look at sets without a pattern obtained form an intersective polynomial. We know that the density of such a set must be zero, but we still want to know how fast it exactly declines. To be able to look at this more thoroughly we first need some notation.

Definition 1.2. Let $f(X)$ be an element of $\mathbb{Z}[X]$. We define the set $A_f[N]$ to be a biggest subset of $[N]$ such that $(A_f[N] - A_f[N]) \cap \{f(x) | x \in \mathbb{Z}\} \subset \{0\}$. Note that $A_f[N]$ is not uniquely defined, but its size is.

Definition 1.3. Let $f(X)$ be an element of $\mathbb{Z}[X]$. We denote the size of $A_f[N]$ by $\alpha(f, N)$,

so $\alpha : \mathbb{Z}[X] \times \mathbb{N} \to \mathbb{N}$ by $(f, N) \mapsto |A_f[N]|$.

The ideas behind these two definitions are that for a given polynomial f the set A we are looking for, equals the limit of $A_f[N]$ for N going to infinity. And consequently the limit of the density of A mimics $\alpha(f, N)/N$. Note, however, that $\alpha(f, N)$ and the number of elements in A up to some N are not exactly the same. It might be possible that $A_f[3] = \{1, 2, 3\}$ but $A \cap [3] = \{1, 2\}$, if for $N > 3$ the 3 becomes disadvantageous. Still, $\alpha(f, N)$ gives us a very good indication of how big A can get because the limits are the same.
With this notation we are ready to look at some examples with intersective polynomials. Before Kamae and Mendés France published their result it was already known that the density of A for $f(X) = X^2$ equals zero. There has also been done quite some research concerning the upperand lower bounds of $\alpha(X^2, N)$. The current upper bound was found by Pintz, Steiger and Szemerédi [14] and the current lower bound comes from Beigel, Gasarch [2] and Lewko [12] using a method from Ruzsa [17].

Theorem 1.3. *For $f(X) = X^2$ and $N \in \mathbb{N}$ there exist positive constants c_0, c_1 and c_2 such that if $N > c_2$,*

$$c_0 N^{\gamma} < \alpha(f, N) \leq \frac{c_1 N}{\log(N)^{\frac{\log\log\log\log(N)}{12}}},$$

where $\gamma = \frac{1}{2}(1 + \log_{205}(12)) = 0.7334\ldots$.

We can see that the upper bound indeed goes to zero if divided by N, and so, that the density is zero. Also, Ruzsa conjectured in [17], that γ cannot exceed $\frac{3}{4}$ by using his method and there are speculations that $c_1 N^{\frac{3}{4}}$ should be the upper bound as well. However, the current upper bound still goes much slower to zero than this speculated one. This shows that there is still a lot of room for improvements.
A logical next step is to look at different powers of X. For $f(X) = X^k$, the lower bound was found by Ruzsa [17] and the upper bound is due to Balog, Pelikán, Pintz and Szemerédi [1].

Theorem 1.4. *For $f(X) = X^k$ and $N \in \mathbb{N}$ there exist positive constants c_0, c_1 and c_2 such that if $N > c_2$,*

$$c_0 N^{\gamma} < \alpha(X^k, N) \leq \frac{c_1 N}{\log(N)^{\frac{\log\log\log\log(N)}{4}}}$$

where $\gamma = \frac{k-1+\log_m(|R|)}{k}$, for m some square-free integer and R a subset of $\{0, 1, \ldots m-1\}$ such that $(R - R)$ does not contain any k-th powers modulo m.

In the case that $k = 3$ the best quantative lower bound is from Lewko [12] who found the value $\gamma = 0.8616$. Here we can again note that the gap between the lower and upper bound is still really big.
In the general case where f is any intersective polynomial Rice [15] proved a very similar upper bound.

Theorem 1.5. *For $f(X)$ an intersective polynomial of degree d and $N \in \mathbb{N}$ there exist*

positive constants c_1 and c_2 such that if $N > c_2$,

$$\alpha(f,N) \leq \frac{c_1 N}{\log(N)^{\frac{\log\log\log\log(N)}{c}}}$$

For any $c > \log(\frac{d^2+d}{2})$.

Unfortunately such a lower bound has not yet been discovered. The most general lower bound was recently found by Younis [23].

Theorem 3.1. *Let $m \geq 2$ be square-free, $d \geq k \geq 2, a_d \neq 0$ and $\gcd(a_k, m) = 1$. Suppose that $f(X) = \sum_{i=k}^{d} a_i X^i \in \mathbb{Z}[X]$ has zero as its only root modulo m. Then for all positive integers N we have $\alpha(f,N) \gg_{m,f} N^{\gamma}$, where*

$$\gamma = \frac{d - 1 + \log_m |R|}{d}.$$

With R is a subset of $\{0, 1, \ldots m-1\}$ such that $(R - R)$ does not contain any k-th powers modulo m.

Most of the previous upper bounds were proved using techniques of Fourier-analysis. The lower bounds used techniques from both combinatorics and number theory. Our main concern in this thesis will be to improve the lower bound from Younis by making it more explicit. In the statement of Theorem 3.1 there is no clarity about whether there exist m and R such that the theorem can be used. In Chapter 5 it will be proved that for a certain set of polynomials such m do always exist and that in some cases we can even certainly find a set R with $|R| \geq 2$. The main result will be the following.

Theorem 5.14. *Let $f(X) = \sum_{i=k}^{d} a_i X^i \in \mathbb{Z}[X]$ such that $k \geq 2$, $a_d \neq 0$ and $f = X^k g(X)$ where $g(X)$ is the minimal polynomial for some $\alpha \in \overline{\mathbb{Q}}$. Furthermore let E be the Galois extension of $\mathbb{Q}[X]/g(X)$ and assume that $\mathbb{Q}(\zeta_k) \cap E = \mathbb{Q}$ where ζ_k is a kth root of unity if k is odd and $\zeta_k = i$ if k is even. Then there exists a prime p such that for all $N \in \mathbb{N}$ the number $\alpha(f,N) \gg_{p,f} N^{\gamma}$ with:*

$$\gamma = \frac{d - 1 + \log_p |R|}{d}$$

such that $|R| \geq 2$.

To prove Theorem 5.14 we will use Theorem 3.1 and some concepts from algebraic number theory.

Before this, in Chapter 2, we will give a more general approach to the polynomial Szemerédi Theoerem. We will see that our problem is just one of the cases generated by this theorem, and that the normal Szemerédi Theorem, concering k-terms, is another.
Then, in the first section of Chapter 3, the ideas and techniques for the proofs of the lower bounds by Ruzsa and Younis will be explained. In the second section follow some of my own results concerning the function $\alpha(f,N)$ if the coefficients of$f$ have a common divisor. This

will also lead to a theorem that reformulates Theorem 3.1 for polynomials with a domain in $n\mathbb{Z}$ instead of $\mathbb{Z}$.
Chapter 4 provides the background information on algebraic number theory needed to understand and proof Dedekind's criterion in Chapter 5. It starts with the definitions around algebraic integers and ideals and ends with showing that inside a ring of integers there always is unique factorisation of ideals into prime ideals. The approach of the chapter is that anyone with a basic knowledge of abstract algebra should be able to understand it.
My own main results can be found in Chapter 5. The first section contains a proof of Dedekind's criterion. The criterion will be used in the second section to give an algebraic condition for square-free m to check if m meets the requirements as in Theorem 3.1 if f is monic. With the help of Chebotarev's density Theorem we will then see that for one class of polynomials we can be certain that there exists such an m. More fore we will be able to prove Theorem 5.14 which, as stated above, gives a more explicit form of Younis lower bound for certain polynomials.
Finally the thesis will end with an outreach in Chapter 6 about possible further research that can be done. One of main conern is certainly to look for an even more explicit lower bound by estimating p in Theorem 5.14 and by finding sets R containing more than 2 elements.

Chapter 2

Szemerédi's Theorem

In this chapter we will work towards understanding what Szemerédi's Theorem states and why this is such a strong result. We will not prove the Theorem. Afterwards we will discuss the polynomial Szemerédi Theorem.
We start with formalising some concepts.

Definition 2.1. Let A be a subset of $\mathbb{N}$, then the *density* of A is:

$$\lim_{N\to\infty} \frac{|A \cap [N]|}{N}.$$

With $N \in \mathbb{N}$. Notation: $d(A)$.

Remarks. Regarding this definition, we can make the following remarks:

- For some choices of A the limit may not exist. In these cases we say that $d(A)$ does not have a well-defined value.
- Because $|A \cap [N]|$ is bigger or equal to 0 and smaller or equal to N we know that $d(A)$ is between 0 and 1 for all $A \subset \mathbb{N}$.
- If we let $B \subset A$ then we also know that $B \cap [N]$ is a subset of $A \cap [N]$ for all $N \in \mathbb{N}$. Hence, the value $|B \cap [N]|$ is smaller or equal to $|A \cap [N]|$. Taking a limit does not change that, and we find $d(B) \leq d(A)$.

Density gives us a way to compare two sets that are both countably infinite. It coincides with the intuitive idea that a set that only contains half of the elements of $\mathbb{N}$ has a different extent than $\mathbb{N}$ itself, even if it does have the same size.

Examples.

- Let $A = \mathbb{N}$, then $|A \cap [N]| = N$ and thus $d(\mathbb{N}) = 1$.
- Let $A = 2\mathbb{N}$, then for all odd N we have that $|A \cap [N]| = \frac{1}{2}N - \frac{1}{2}$ and for all even N that $|A \cap [N]| = \frac{1}{2}N$. However for $N \to \infty$ these both go to $\frac{1}{2}N$ and thus $d(2\mathbb{N}) = \frac{1}{2}$.

In general, it is easy to show that for $n \in \mathbb{N}$ we have $d(n\mathbb{N}) = \frac{1}{n}$.

- Let $A = \{1, 2, 3, 4, 6, 10\}$, then for all $N \geq 10$ we have that $|A \cap [N]| = 6$. If we now look at $\frac{6}{N}$ and let N go to infinity it is obvious that $d(A) = 0$. In general we know for any finite set A that $d(A) = 0$.
- Let $A = \mathbb{N}/\{1, 2, 3, 4, 6, 10\}$, then for all $N \geq 10$ we have that $|A \cap [N]| = N - 6$. If we now look at $\frac{N-6}{N}$ and let N go to infinity we see that $d(A)$ becomes 1. In general it is true that $d(A) + d(A^c) = 1$. (For a proof see Lemma 2.1)
- Let $A = \{n^2 \mid n \in \mathbb{N}\}$, then $A \cap [N]$ consits of $\lfloor \sqrt{N} \rfloor$ elements. Indeed, for all integers less than $\lfloor \sqrt{N} \rfloor$ we know their square to be less than N, and for all integers bigger than $\lfloor \sqrt{N} \rfloor$ we know their square to be bigger than N. Hence,:

$$d(A) = \lim_{N \to \infty} \frac{\lfloor \sqrt{N} \rfloor}{N} \leq \frac{1}{\sqrt{N}} \to 0$$

  and $d(A) = 0$.
- As noted before, if we let A be some set such that $(A - A) \cap \{x^2 \mid x \in \mathbb{Z}\} = \{0\}$, then $d(A) = 0$.
- Let A be the union of $[2^n + 1, 2^{n+1}]$ for all even n. Then if we take N to be an even power of two we find $|A \cap [N]| = 1 + 2^2 + 2^4 + \ldots + \frac{N}{4} = \frac{N-1}{3}$. But if instead we let N be an odd power of two, we find $|A \cap [N]| = 1 + 2^2 + 2^4 + \ldots + \frac{N}{2} = \frac{2N-1}{3}$. We see that $d(A)$ is not a well-defined limit and thus does not have a value.

In the last example we found that not all sets have a well-defined density. However, it is obvious that in this example A should have some kind of positive density, because it always has between the $\frac{N}{3}$ and $\frac{2N}{3}$ elements. To account for this we also introduce the concepts of upper and lower density. Roughly these are the highest and lowest values that $|A \cap [N]|$ takes for N goes to infinity.

Definition 2.2. Let A be a subset of $\mathbb{N}$, then the *upper-* and *lower density* of A are respectively:

$$\limsup_{N \to \infty} \frac{|A \cap [N]|}{N}$$

$$\liminf_{N \to \infty} \frac{|A \cap [N]|}{N}$$

for $N \in \mathbb{N}$. Notation $\overline{d}(A)$ and $\underline{d}(A)$.

Using this definition and looking at our last example we can see that $\overline{d}(A) = \frac{2}{3}$ and $\underline{d}(A) = \frac{1}{3}$. For all cases were $d(A)$ was already well defined we should note that $d(A) = \overline{d}(A) = \underline{d}(A)$. Furthermore, both remarks about the general density also hold for the upper and lower density. Thus, $0 \leq \overline{d}(A), \underline{d}(A) \leq 1$ and if $B \subset A$ then $\overline{d}(B) \leq \overline{d}(A)$ and $\underline{d}(B) \leq \underline{d}(A)$.

To understand how important the notion of density can be, we will compare some sets with and without a density of zero. To do this we first prove the following Lemma:

Lemma 2.1. *Let $A, B \subset \mathbb{N}$ such that $A \cap B = \emptyset$, then $d(A \cup B) = d(A) + d(B)$.*

Proof. Because A and B are disjoint we know that $A \cap [N]$ and $B \cap [N]$ must also be disjoint for any $N \in \mathbb{N}$. Now, the elements in $(A \cup B) \cap [N]$ are exactly the elements in $A \cap [N]$ with the elements of $B \cap [N]$. Thus, the amount of elements in $(A \cup B) \cap [N]$ also equals the sum of the amount of elements in these two sets. We see that $|(A \cup B) \cap [N]| = |A \cap [N]| + |B \cap [N]|$. Now if we divide both sides by N and take the limit we indeed get $d(A \cup B) = d(A) + d(B)$. $\square$

Remarks.

- The previous lemma also holds for the upper and the lower density. The proof goes exactly the same.
- In particular the previous lemma tells us that $d(A) + d(A^c) = 1$.

Now, let us consider some set A with density zero and some set B with density greater than zero. In this case we claim that the set B must contain infinitely many elements of A^c. To check this we suppose the contrary. Then there must be some $N \in \mathbb{N}$ such that for all $n > N$ with $n \in A^c$ we know that $n \notin B$. Thus $B \subset ([N] \cap A^c) \cup A$. Now using Lemma 2.1 we see that this means $d(B) \leq d([N] \cap A^c) + d(A) \leq d([N]) + d(A) = 0$. However we assumed that $d(B) > 0$, so this leads to a contradiction.
If we look back at our examples, this means for instance that for any n the set $n\mathbb{N}$ contains infinitely many pairs a, b such that $|a-b|$ is a square. So to say that a set has a density unequal to zero also means it cannot meet any of the conditions that sets with a density of zero do meet. Szemerédi's Theorem concerns itself with the condition that a set cannot contain a sequence with a constant difference. Such sequences are called arithmetic progressions.

Definition 2.3. Let d be some element of $\mathbb{Z}$. An *arithmetic progression of length k* is a sequence $(a_i)_{1 \leq i \leq k}$ in $\mathbb{Z}$ such that for all $1 \leq i \leq k-1$ we have that $a_{i+1} - a_i = d$. We call d the *distance* and a_1 the *starting point* of the arithmetic progression.

Remarks.

- Given a length in $\mathbb{N}$ and a distance and starting point in $\mathbb{Z}$, there is exactly one arithmetic progression. For example, the arithmetic progression of length 3 with starting point 5 and distance 2 is $(5, 7, 9)$.
- Any integer $n \in \mathbb{N}$ is an arithmetic progression of length 1 with starting point n and whatever distance.
- Any pair of integers n, m with $n < m$ is an arithmetic progression of length 2 with starting point n and distance $m - n$. Thus we see that any set $A \subset \mathbb{N}$ with $|A| \geq 2$ has an arithmetic progression of length 2.

- If $(a_i)_{1\leq i\leq k}$ is some arithmetic progression of length k, then $(a_i)_{1\leq i\leq k-1}$ is an arithmetic progression of length $k-1$. So if a set contains an arithmetic progression of length k, it also contains an arithmetic progression of length k' for all $k' \leq k$.

Previous remarks already show that we can draw some conclusion about whether or not a set $A \subset \mathbb{N}$ contains certain arithmetic progressions. Szemerédi's Theorem is also about this idea, however, being much stronger.

Theorem 2.2 (Szemerédi's Theorem)**.** *Let $A \subset \mathbb{N}$ have positive upper density. Then for all $k \in \mathbb{N}$ there exists an arithmetic progression in A of length k.*

To illustrate just how strong this result is, consider the following challenge. Try to make a set $A \subset \mathbb{N}$ without any arithmetic progressions of length 7. Then according to Szemerédi's theorem this set must have an upper density of 0. Hence, for all $\varepsilon > 0$ there must be some N such that for all $n \geq N$ we can at most have εn elements in our set A. And this is not only true for 7 but for any length $k \in \mathbb{N}$.
Unfortunately for us the proof of Szemerédi's Theorem is quite involved, it being one of the most important combinatorial theorems around. So we will not be able to prove the Theorem here. It is nice to note that there do exist multiple completely different proofs of the Theorem. Two well-known ones being the purely combinatorial one from Szemerédi [19] himself and a proof from Furstenberg [8] using ergodic theory.
" To understand the resembelance of Szemerédi's Theorem with our own problem we will first state its negotiate.

Theorem 2.3. *Let $A \subset \mathbb{N}$. Assume there exists some $k \in \mathbb{N}$ such that A does not contain any arithmetic progressions of length k. Then $d(A) = 0$.*

Going back to the examples from before, we can easily check Szemerédi's Theorem and its negotiate for some of them.

Examples.

- If $A = n\mathbb{Z}$, let the starting point be 0 and the distance n, then all the elements $0, n, 2n, \ldots (k-1)n$ are in A and this is an arithmetic progression of length k.
- If A is finite then it cannot contain an arithmetic progression for any length $k > |A|$.
- If A^c is finite then A^c must contain some maximal integer a. The sequence $a+1, a+2, \ldots a+k$ is then an arithmetic progression of length k in A for all $k \in \mathbb{N}$.
- If A is the union of $[2^n+1, 2^{n+1}]$ for all even n, there must exist for all $k \in \mathbb{N}$ some even n such that $k < 2^n$. Then $2^n+1, \ldots 2^n+k$ is an arithmetic progression of length k contained in A.

Much like in the previous chapter the question that now comes to mind is 'how fast does a subset without an arithmetic progression of length k go to zero?'. We already stated a general upper bound by Gowers in Theorem 1.1. Gowers [9] also gave an expression for c_k for all k. Furthermore, O'Bryant [13] found a general lower bound. This leads to the following

theorem:

Theorem 2.4. *Let $A \subset [N]$ be a biggest set such that A does not contain any arithmetic progressions of length k. There exists real numbers $c_0, c = \lceil \log k \rceil$ and $c_k = 2^{-2^{k+9}}$ such that:*

$$\frac{c_0 N}{2^{c2^{(c-1)/2}\sqrt[c]{\log(N)} - \frac{\log\log(N)}{2c}}} \leq |A| \leq \frac{N}{\log\log(N)^{c_k}}.$$

For some specific k the bound has been improved further.
For $k = 1$ and $k = 2$ we already stated that A has to be finite. For $k = 3$ Roth [16] found the first upper bound, before Szemerédi's Theorem was even proved, to be $\frac{N}{\log\log(N)}$. This bound has been improved by many with the current best upper bound being from Bloom [6]. It is stated in the next theorem together with the best lower bound from O'Bryant [13].

Theorem 2.5. *Let $A \subset [N]$ be a biggest set such that A does not contain any arithmetic progressions of length 3. There exist a real number c such that:*

$$\frac{N}{2^{\sqrt{8\log(N)}}} \leq |A| \leq c_2 \frac{N(\log\log(N))^4}{\log(N)}.$$

For $k = 4$ Green and Tao [10] discovered an upper bound.

Theorem 2.6. *Let $A \subset [N]$ be a biggest set such that A does not contain any arithmetic progressions of length 4. There exist real numbers c_1 and c_2 such that:*

$$|A| \leq \frac{c_1 N}{\log(N)^{c_2}}$$

Finally there is also a better lower bound for k that are primes. This one is from Taranchuck [21].

Theorem 2.7. *Let $A \subset [N]$ be a biggest set such that A does not contain any arithmetic progressions of length k with k prime. There exist a real numbers c_k such that:*

$$N^{1-\frac{c_k}{k\log(k)}} < |A|,$$

where $c_k \to 1$ for $k \to \infty$.

Szemerédi's theorem has been adapted in many directions. For instance there is a Szemerédi's theorem for finite fields and one for vector spaces. Tao and Ziegler [20] even proved that the set of prime numbers contains arithmetic progressions of arbitrary length. The extension that is relevant for our problem is the polynomial Szemerédi Theorem. It was proved by Bergelson and Leibman [3].

Theorem 2.8 (Polynomial Szemerédi's Theorem)**.** *Let $f_1, f_2, \ldots, f_k$ be integer polynomials such that $f_i(0) = 0$ for all $i \in \mathbb{N}$. If A is a set with positive upper density it contains the elements $a + f_1(x), a + f_2(x), \ldots, a + f_k(x)$ for infinitely many $a \in \mathbb{Z}$ and $x \in \mathbb{N}$.*

This is indeed a direct extension from the original Szemerédi's Theorem. If we take $f_i(X) = iX$ for all $1 \leq i \leq k$ we find that any set A with positive upper density has an arithmetic progression of length k with starting point a and distance x. It also has a great overlap with the problem of finding $\alpha(f, N)$. Taking $f_1(X) = 0$ and $f_2(X) = f(X)$ there are infinitely many pairs $a, a + f(x)$ in A. Obviously their difference is $f(x)$ and this lies in the image of f. Hence, the Polynomial Szemerédi Theorem tells us that A cannot have a positive upper density if $(A - A)$ contains no elements of the image of some $f(X)$ with $f(0) = 0$. As mentioned in the introduction Bergelson and Leibman extended this Theorem such that it is true for all intersective polynomials $f(X)$. It becomes clear now that our problem is really about finding arithmetic progressions of length 2 with a certain distance.

Chapter 3

On 'Lower Bounds in the Polynomial Szemerédi Theorem'

In this chapter we will discuss the article Lower Bounds in the Polynomial Szemerédi Theorem written by Khalid Younis [23]. We will state the three main theorems, give an idea of the proofs and show where certain conditions come into play. The chapter will end with some new results which demonstrate that an adaption of Theorem 3.1 can also be used to calculate a lower bound N^γ for other kind of polynomials.

3.1 Results

Before we can state the three main theorems we need the definitions of some sets R, $(R_i)_{i\geq 0}$ and R' respectively. These sets are all quite alike and play a similar role in their respective theorems.

Definition 3.1. Let m and k be integers. We define R to be some subset of $\{0, 1, \ldots, m-1\}$ such that $(R - R) \cap \{x^k \mod m \mid x \in [m]\} = \{0\}$.

Definition 3.2. Let m and k be integers. We define $(R_i)_{i\geq 0}$ to be some sequence of subsets of $\{0, 1, \ldots, m-1\}$ such that $(R_n - R_n) \cap \{x^k \mod m \mid x \in (R_{n-1} - R_{n-1})\} = \{0\}$.

Definition 3.3. Let m and k be integers and $F(\mathbf{x})$ a homogeneous polynomial from $\mathbb{Z}^n$ to $\mathbb{Z}$. We define R' to be some subset of $\{0, 1, \ldots, m^k - 1\}$ such that $(R' - R') \cap \{F(\mathbf{x}) \mod m^k \mid \mathbf{x} \in \mathbb{Z}^n\} = \{0\}$.

Note that R, $(R_i)_{i\geq 0}$ and R' are all not uniquely determined by these definitions. In the theorems we will want them to be as big as possible and will only be concerned with the sizes of the sets.
Now we have all the information we need to be able to understand the main theorems of the article.

Theorem 3.1 (Inhomogeneous polynomials)**.** *Let $m \geq 2$ be square-free, $d \geq k \geq 2, a_d \neq 0$ and $\gcd(a_k, m) = 1$. Suppose that $f(X) = \sum_{i=k}^{d} a_i X^i \in \mathbb{Z}[X]$ has zero as its only root modulo m. Then for all positive integers N we have $\alpha(f, N) \gg_{m,f} N^{\gamma}$, where*

$$\gamma = \frac{d - 1 + \log_m |R|}{d}.$$

Theorem 3.2 (Non-linear progressions)**.** *Let m be square-free and $k \geq 2$. For all $\varepsilon > 0$ and all positive integers N, there exists a set $A \subset [N]$ with no non-trivial configuration of the form $\{x, x + y, x + y^k\}$ and $|A| \gg_{m,\varepsilon} N^{\gamma - \varepsilon}$, where*

$$\gamma = (k-1)\left(\frac{\log_m |R_0|}{k} + \frac{\log_m |R_1|}{k^2} + \ldots + \frac{\log_m |R_n|}{k^{n+1}} + \ldots\right)$$

Theorem 3.3 (Homogeneous multivariate polynomials)**.** *Let $m \geq 2$ be a positive integer. Let $F(\mathbf{X}) \in \mathbb{Z}[X_1, \ldots, X_n]$ be a homogeneous polynomial of degree $k \geq 2$. Suppose that the only roots of F modulo m^k are congruent to $\mathbf{0}$ modulo m. Then for all integers N, there exists a set $A \subset [N]$ with $(A - A) \cap F(\mathbb{Z}^n) = \{0\}$ and $|A| \gg_{m,k} N^{\gamma}$, where*

$$\gamma = \frac{\log_m |R'|}{k}.$$

In this thesis, the main focus will lay on Theorem 3.1, as mentioned before. However, it is nice to note the similarities between these three theorems and their proofs. First of all, all three of the theorems give lower bounds for a specific case of the polynomial Szemerédi Theorem. In Theorems 3.1 and 3.3 the set A cannot contain an arithmetic progressions of length 2 with a distance in $f(\mathbb{Z})$ or $F(\mathbb{Z}^n)$ respectively. For Theorem 3.2 we could choose $f_1(X) = 0, f_2(X) = X$ and $f_3(X) = X^k$ to get the same problem as formulated in the polynomial Szemerédi Theorem. Secondly, all three proofs use the same techniques that were originally developed by Ruzsa to find a lower bound for $\alpha(X^k, N)$ [17]. Ruzsa's result was stated in Theorem 1.4 and also has the same form as the three theorems from Younis. To understand the techniques of these proofs a little better we will look closely at the proof of Theorem 3.1 and afterwards discuss what the proofs of the other two theorems have in common with this proof and what not.

The goal to be had in mind is that one wants to construct a subset A of $[N]$ as big as possible that meets a certain condition. In the case of Theorem 3.1 this condition is that $(A - A)$ cannot contain elements of the image of f. The main idea behind the proof is then to construct a subset that meets the condition and calculate its size. Our biggest subset must be at least as big as our constructed subset, thus giving a lower bound for the biggest subset.
In the proof A will represent the constructed subset. To construct A we make use of the set R and and of the m-ary expansion of an integer. The m-ary expansion of an integer is a way to write down an integer as a sum of powers of m.

Definition 3.4. The *m-ary expansion* of an integer $n \in \mathbb{N}$ is the unique way to write n in the form

$$\sum_{0 \leq i} u_i m^i,$$

where u_i equals $\frac{n-(u_0+u_1 m+\ldots+u_{i-1}m^{i-1})}{m^i} \mod m$.

Note that u_i is a residue class of m and thus always takes a value in $\{0, 1, \ldots, m-1\}$. More specifically u_i represents how many times m^i fits in n without it becoming m^{i+1}.
Before we can really start with the proof we need one more lemma.

Lemma 3.4. *For m and f as in Theorem 3.1, if $f(x) \equiv 0 \mod m^j$ then $x \equiv 0 \mod m^{\lceil j/k \rceil}$.*

Proof. The proof will be by induction on $\lceil j/k \rceil$.
First assume that $j \leq k$ such that $\lceil j/k \rceil = 1$. Then the conditions on f and m by Theorem 3.1 give us that $f(x) \equiv 0 \mod m$ if and only if $x \equiv 0 \mod m$. Hence, the statement of the lemma is true for $j \leq k$.
Now assume that $j > k$ and that we know the statement to be true for $j' = j - k$ and all f. Note that $\lceil j/k \rceil = \lceil j'/k \rceil + 1$. Because $f(x) \equiv 0 \mod m^j$ we also know that $f(x) \equiv 0 \mod m$ and thus that $x \equiv 0 \mod m$. We can rewrite x as ym for some $y \in \mathbb{Z}$. If we put this expression into $f(x)$ we get, $f(x) = \sum_{i=k}^{d} a_i y^i m^i \equiv 0 \mod m^j$. Now define $g(y) := \sum_{i=k}^{d} a_i m^{i-k} y^i$. Because $\gcd(a_k, m) = 1$ and m is square-free we see that g also meets the conditions of f in Theorem 3.1. Furthermore $g(y) \equiv 0 \mod m^{j-k}$. From our hypothesis we get that y must be equivalent to 0 modulo $m^{\lceil j'/k \rceil}$. Thus $x = my$ has to be divisible by $m^{\lceil j'/k \rceil + 1} = m^{\lceil j/k \rceil}$ as wished.
By the principle of induction it follows that for all $j \in \mathbb{N}$ the statement of the lemma must hold. □

The proof we will now give of Theorem 3.1 is a reformulation of the proof Younis gave in his paper.

Proof. (Of Theorem 3.1.)
Define the numbers $Y = \log_m(N)$ and $Z = k(Y+1)/d$ and assume that N is sufficiently large such that if $|x| \geq m^{Z/k}$ we have that $|f(x)| \geq \frac{|a_d|}{2}|x|^d$. Such an N always exists because eventually every polynomial gets dominated by it's leading term $a_d x^d$.
Now let A be the subset of $[N]$ containing all $u = \sum_{0 \leq i < Y} u_i m^i$ satisfying:

$$u_i \in \begin{cases} a_k R \mod m & \text{if } k \mid i \text{ and } 0 \leq i < Z \\ u_i \in \{0, 1, \ldots, m-1\} & \text{otherwise.} \end{cases}$$

The claim is that for all distinct $u, v \in A$ and $x \in \mathbb{Z}$ we have that $u - v \neq f(x)$. To prove this we assume the opposite. Thus, suppose there are some $u = \sum u_i m^i$, $v = \sum v_i m^i$ and $x \in \mathbb{Z}$ such that $u - v = f(x)$. Because u and v are distinct we know that there must be a

smallest index j such that $u_j \neq v_j$. We can now rewrite $u - v$ as:

$$m^j(u_j - v_j) + zm^{j+1} = u - v = f(x)$$

with $z \in \mathbb{Z}$. Inspecting the left side we see that it is divisible by m^j. Also, because u_j and v_j are distinct and both smaller than m, we see that $u_j - v_j \not\equiv 0 \mod m$. So $m^j(u_j - v_j)$ is not divisible by m^{j+1} and thus neither is the left side. This means that $u - v = f(x)$ has exactly j factors of m. Lemma 3.4 now says that $x \equiv 0 \mod m^{\lceil j/k \rceil}$. We rewrite x as $ym^{\lceil j/k \rceil}$ for some $y \in \mathbb{Z}$. Because $f(0) = 0$ we know that $y \neq 0$. Putting this exprssion for x into $f(x)$ we get:

$$m^j(u_j - v_j) + zm^{j+1} = \sum_{i=k}^{d} a_i(ym^{\lceil j/k \rceil})^i. \tag{3.1}$$

The right side of this equation contains at least $k \cdot \lceil j/k \rceil$ factors m. However, $k \cdot \lceil j/k \rceil$ is greater or equal to j with equality if and only if k divides j. Because the left and right side must be equal they must also be divisible by the same amount of factors m. We derive that $k \mid j$. Firstly, this gives us that we can divide both sides by m^j. Secondly, we find that either u_j and v_j are both elements of a_kR or $j \geq Z$. We will consider these two cases separately.

Case 1. Suppose that $j \geq Z$. It is always true that,

$$|f(x)| = |u - v| \leq \max(u, v) < m^Y = N. \tag{3.2}$$

But now because $j \geq Z$ we also know that $x = ym^{j/k} \geq m^{Z/k}$ and from our definition of Z it then follows that,

$$|f(x)| \geq \frac{|a_d|}{2}|x|^d = \frac{|a_d|}{2}|y|^d m^{jd/k} \geq \frac{|a_d|}{2}m^{Zd/k} = \frac{|a_d|}{2}m^{Y+1} = \frac{|a_d|}{2}mN. \tag{3.3}$$

Combining Equations 3.2 and 3.3 we find that $N > \frac{|a_d|}{2}mN$, and thus $2 > |a_d|m \geq m$. But we assumed that $m \geq 2$ so this cannot be true.

Case 2. Suppose that $j < Z$ and thus $u_j, v_j \in a_kR \mod m$. We may consider the equation (3.1) divided by m^j modulo m and find:

$$u_j - v_j \equiv a_k y^k \mod m. \tag{3.4}$$

Furthermore, we can write $u_j \equiv a_k u'_j \mod m$ and $v_j \equiv a_k v'_j \mod m$ with $u'_j, v'_j \in R$. Recall that this means that $u'_j - v'_j$ cannot equal a k-th power modulo m. But because $\gcd(a_k, m) = 1$ we can divide both sides of equation (3.4) by a_k and we get,

$$u'_j - v'_j \equiv y^k \mod m,$$

which contradicts the previous statement.

We conclude that in all cases there can't exist u, v and x such that $u - v = f(x)$. And thus $|A|$ gives a lower bound for $\alpha(f, N)$.

The next step is to estimate the size of A. If we want to take an arbitrary element out of A we have to make $\lceil Y \rceil$ choices. One for every value of u_i for $0 \leq i < Y$. Note that $a_k R \mod m$ has the same size as R because $\gcd(a_k, m) = 1$. So for $i < Z$ such that $k \mid i$ we have $|R|$ possibilities and for all other i we have m possibilities. There are exactly $\lceil Z/k \rceil$ that fit into the first category. So this gives us a total of $|R|^{\lceil Z/k \rceil} m^{\lceil Y \rceil - \lceil Z/k \rceil}$ possibilities for elements in A. We find that,

$$|A| = |R|^{\lceil Z/k \rceil} m^{\lceil Y \rceil - \lceil Z/k \rceil} \geq m^{-2} |R|^{Y/d} m^{Y - Y/d} = c m^{Y/d(\log_m |R| + d - 1)} = c N^{\gamma}.$$

Where c is some constant and $\gamma = \frac{d - 1 + \log_m |R|}{d}$.
Hence we have that $\alpha(f, N) \geq |A| \gg_{m,f} N^{\gamma}$, as wished. □

The most important part of this proof is that we limit the values that u_i can take for some i but not for all i such that it is enough to get a contradiction from how we defined the set R. This is also what is done in the proofs of the other two theorems. The biggest difference is that we do not use R but $(R_i)_{i \geq 0}$ and R' and define the u_i in another way.
In Theorem 3.2 we let $u_i \in R_n$ if i has exactly n factors of k. You can see this in the Theorem by the fact that $\log_m(R_n)$ gets divided by k^{n+1}, because there are $\lceil \log_m(N)/k^n \rceil$ integers between 0 and $\log_m(N)$ with n or more factors k. Then we assume that there exist $(u, v, w) = (x, x + y, x + y^k)$ in A and compare $(w - u)$ with $(v - u)^k$. By taking again the smallest indices such that $u_j \neq w_j$ and $u_l \neq v_l$ we can count factors of m. This will show that j must equal kl which will give a contradiction with the definition of $(R_i)_{i \geq 0}$. So this all goes very similar to the second case in the proof of Theorem 3.1. The first case is not relevant for Theorem 3.2. Afterwards $|A|$ is calculated by counting the possible values u can take based on the u_i and finally there has to be a correction with ε because $(R_i)_{i \geq 0}$ is an infinite sequence which are not all used if N is finite.
In Theorem 3.3 the similarities with the proof of Theorem 3.1 are even bigger. The only real differences are that we do not look at m, but at $M := m^k$, and that we take $u_i \in R'$ for all i. We still compare $F(x)$ with $u - v$, take the smallest index j such that $u_j \neq v_j$ and come across a contradiction based on the definition of R' when counting the factors M. In the end we calculate $|A|$ by counting the possible values $u \in A$ can take given the possible values of each u_i. γ has only $\log_m |R'|$ in the numerator because all u_i were in $|R'|$ and none could take a value outside of $|R'|$.

3.2 Further results

Here we will look at some simple results concerning the calculation of $\alpha(f, N)$ and how Theorem 3.1 can be adapted for polynomials from $l\mathbb{Z}$ to $\mathbb{Z}$.
We start with a theorem that shows how the growth of $\alpha(f, N)$ is linearly dependent on

divisors of f. Note that this theorem holds for all $f \in \mathbb{Z}[X]$ and not only for polynomials that meet the conditions of Theorem 3.1 or are intersective.

Theorem 3.5. *Let $f, g \in \mathbb{Z}[X]$ such that $f(X) = mg(X)$ for some $m \in \mathbb{Z}$. Then $\alpha(f, mN) = m\alpha(g, N)$ for all $N \in \mathbb{N}$.*

Proof. First we will construct a set $B \subset [mN]$ which is m times as big as $\alpha(g, N)$ such that $(B - B) \cap \{f(x) \mid x \in \mathbb{Z}\} \subset \{0\}$. We will use an arbitrary set $A_g[N]$ for this.
Let $B = \{mx - a \in \mathbb{N} \mid x \in A_g[N] \text{ and } 0 \leq a \leq m - 1\}$. It is clear that $|B| = m|A_g[N]|$ because a can take m values. Furthermore because $x \leq N$ we see that $mx - a \leq mN$ as wished. Now assume there are $y, z \in B$ such that $|y - z| = f(x)$ for some $x \in \mathbb{Z}$. We write $y = mx_y - a_y$ and $z = mx_z - a_z$, with $x_y, x_z \in A_g[N]$ and $a_y, a_z \leq m - 1$. So $|y - z| = |m(x_y - x_z) + a_z - a_y| \equiv |a_y - a_z| \mod m$. Note that m divides $f(x)$ for all x so $|y - z| = f(x) \equiv 0 \mod m$ and thus $a_y = a_z$. This gives that $m(x_y - x_z) = f(x) = mg(x)$ and $|x_y - x_z| = g(x)$. But we assumed x_y and x_z to be in $A_g[N]$ so their difference can't equal $g(x)$ for any x. We have arived at a contradiction and see that such y and z cannot exist in B. We conclude that $(B-B)\cap\{f(x) \mid x \in \mathbb{Z}\} \subset \{0\}$. We also know that B can have at most as many elements as a set $A_f[mN]$ has and we can see that $\alpha(f, mN) \geq |B| \geq m\alpha(g, N)$.
For the second part of the proof we assume that $\alpha(f, mN)$ is bigger than $m\alpha(g, N)$. Assuming this, we will be able to find a set $C \subset [N]$ which is bigger than $\alpha(g, N)$ such that also $(C - C) \cap \{g(x) \mid x \in \mathbb{Z}\} \subset \{0\}$. This is obviously in disagreement with the definition of α.
Let $A_f[mN]$ be a set as defined before. We can divide $A_f[mN]$ into m disjoint sets by their congruence classes modulo m. Because of the pigeon hole principle there must be at least one set that is bigger than $\alpha(g, N)$. Assume this set to be the one with elements congruent to a modulo m and call it C_a. Now we construct a set $C := \{\frac{x+m-a}{m} \mid x \in C_a\}$. Then $|C| = |C_a| > \alpha(g, N)$ and all $y \in C$ are smaller or equal to N. By definition of $\alpha(g, N)$, there must be two elements y and z in C such that $|y - z| = g(x)$ for some $x \in \mathbb{Z}$. Write $y = \frac{x_y+m-a}{m}$ and $z = \frac{x_z+m-a}{m}$ with $x_y, x_z \in C_a \subset A_f[mN]$. Then $g(x) = |\frac{x_y-x_z}{m}|$. Now multiplying both sides with m we see that $f(x) = mg(x) = |(x_y - x_z)|$. But x_y and x_z are elements of $A_f[mN]$ and thus they can't have a difference that equals a value of f. We have shown that it is impossible that $\alpha(f, mN) > m\alpha(g, N)$ and thus know that $\alpha(f, mN) \leq m\alpha(g, N)$.
Using both inequalities we see that $\alpha(f, mN) = m\alpha(g, N)$. □

Now, considering the fact that all f are divisible by the greatest common divisor of their coefficients we also find the following corollary.

Corollary 3.5.1. *For $f(X) = \sum_{i=0}^{d} a_i X^i \in \mathbb{Z}(X)$ define $a := \gcd(a_d, \ldots a_0)$. Then $f(X) = ag(X)$ with $g(X) \in \mathbb{Z}[X]$ and $\alpha(f, aN) = a\alpha(g, N)$.*

When finding $\alpha(f, N)$ we are mostly interested in the limit if N goes to infinity. For this we do not need to know the value of $\alpha(f, N)$ for all $N \in \mathbb{N}$ but only what happens when N gets large. This limit will thus be the same for $\alpha(f, N)$ and $\alpha(f, mN)$. Together with Corollary 3.5.1 this gives a good motivation to assume from now on that $\gcd(a_d, \ldots, a_0) = 1$.

Another interesting problem in polynomial Szemerédi Theorem is what happens when f has a different domain than $\mathbb{Z}$. (The image of f has to be in $\mathbb{Z}$, otherwise we cannot speak of progressions.) If we let the domain be $l\mathbb{Z}$ for some $l \in \mathbb{N}$ we can nicely use Theorem 3.5 to calculate $\alpha(f, N)$. Here we define $\alpha(f, N)$ for $f : l\mathbb{Z} \to \mathbb{Z}$ in the same manner as when f has a domain in $\mathbb{Z}$. The only distinction is that the differences set of $A_f[N]$ should now not contain any values $f(x)$ where x takes values in $l\mathbb{Z}$ instead of values in $\mathbb{Z}$.

Theorem 3.6. *Let $f(X) = \sum_{i=k}^{d} a_i X^i \in \mathbb{Z}[X]$ with X only taking values in $l\mathbb{Z}$ for some $l \in \mathbb{N}$. Then $\alpha(f, l^k N) = l^k \alpha(g, N)$ where $g(Y) = \sum_{i=k}^{d} l^{i-k} a_i Y^i$ for $Y \in \mathbb{Z}$.*

Proof. It is easy to see that for all $y \in \mathbb{Z}$ and $x = ly \in l\mathbb{Z}$ we have $l^k g(y) = f(ly) = f(x)$. This also means that $\{l^k g(y) \mid y \in \mathbb{Z}\} = \{f(x) \mid x \in l\mathbb{Z}\}$. Thus $(A - A) \cap \{l^k g(y) \mid y \in \mathbb{Z}\} = \{0\}$ exactly when $(A - A) \cap \{f(x) \mid x \in l\mathbb{Z}\} = \{0\}$. So $\alpha(l^k g, N)$ must equal $\alpha(f, N)$. Now using Theorem 3.5, we see that $\alpha(f, l^k N) = \alpha(l^k g, l^k N) = l^k \alpha(g, N)$, as wished. □

One nice aspect of Theorem 3.6 is that if we have a polynomial from $n\mathbb{Z}$ to $\mathbb{Z}$ which meets the requirements of Theorem 3.1. we can always find a lower bound for α using Theorem 3.1. To see this one should note that $g(Y)$ (as defined in Theorem 3.6) meets the requirements of Theorem 3.1 precisely when $f(X)$ does.
To illustrate this we will give a lower bound for $\alpha(f, 25N)$ with $f(Y) = Y^2 + Y^3$ and $Y \in 5\mathbb{Z}$. Theorem 3.6 tells us that this lower bound corresponds with a lower bound for $\alpha(X^2 + 5X^3, N)$ with $X \in \mathbb{Z}$. Younis already calculated a lower bound for this polynomial.

Theorem 3.7. *For all positive integers N, there exists a set $A \subset [N]$ with all non-zero differences avoiding the set $\{x^2 + 5x^3 \mid x \in \mathbb{Z}\}$ and $|A| \gg N^\gamma$, where*

$$\gamma = \frac{2 + \log_5(2)}{3} = 0.8102\ldots.$$

Thus using Theorems 3.6 and 3.7 we have the following corollary.

Corollary 3.7.1. *For all positive integers N, there exists a set $A \subset [25N]$ with all non-zero differences avoiding the set $\{y^2 + y^3 \mid y \in 5\mathbb{Z}\}$ and $|A| \gg 25N^\gamma$, where*

$$\gamma = \frac{2 + 2\log_5 2}{3} = 0.8102\ldots$$

As a final remark about Theorem 3.6 one should note that $g(Y)$ has a very specific form where all terms except $a_k y^k$ are divisible by l. Because of this we can nicely estimate $\alpha(\frac{g}{\gcd(l,a_k)}, N)$ with Theorem 3.1 by choosing m to be some square-free divisor of $\frac{l}{\gcd(l,a_k)}$. It is then easy to verify that the greatest common divisor of m and $\frac{a_k}{\gcd(l,a_k)}$ is 1, and that $\frac{g}{\gcd(l,a_k)}(y) \equiv 0 \mod m$ if and only if $y \equiv 0 \mod m$. Using Theorems 3.5 and 3.6 this also gives a good estimate for $\alpha(g, N)$ and thus for $\alpha(f, N)$. The only thing left to check would be that the R that belongs with this m has a size of at least 2, otherwise the result is not very interesting. In Chapter 5 we will see for which m and k we know R to contain 2 or more elements.

Chapter 4

Algebraic number theory

This chapter will be devoted to explaining some algebraic number theory. The goal will be to understand all notions to be able to prove Dedekind's Criterion in chapter 5. However, some other important ideas will also be discussed.
The structure and definitions of the first four sections are loosely based on [5], [4] and [18]. The proof of the last section is based on [7].

4.1 Algebra recap

Before we start with the actual algebraic number theory we will refresh some definitions from basic algebra.

Definition 4.1. A *ring* $(R, +, 0, \cdot, 1)$ (or *commutative ring*) is a set R together with two operations $+$ (addition) and $\cdot$ (multiplication) and two distinct elements $0, 1 \in R$ such that:

- $(R, +, 0)$ is an abelian group.
- $1 \cdot a = a$ for all $a \in R$.
- $a \cdot b = b \cdot a$ for all $a, b \in R$. (Multiplication is commutative.)
- $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in R$. (Multiplication is associative.)
- $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in R$. (Addition and multiplication are distributive.)

Usually we write $a \cdot b$ as ab.
Some basic examples of rings are $(\mathbb{Q}, +, 0, \cdot, 1)$, $(\mathbb{Z}, +, 0, \cdot, 1)$ and $(\mathbb{Z}_n, +, 0, \cdot, 1)$ where $+$, $\cdot$, 1 and 0 are all defined as usual and $\mathbb{Z}_n$ equals the residue classes modulo n in $\mathbb{Z}$.

Definition 4.2. An element a of a ring R is called a *unit* if there exists some $b \in R$ such that $ab = 1$. The set of all units from R form a *unit group* denoted by $(R^*, \cdot, 1)$.

In $\mathbb{Q}$ all non-zero elements are units and in $\mathbb{Z}$ the only units are 1 and -1. An element $m \in \mathbb{Z}_n$ is a unit if and only if $\gcd(n, m) = 1$. Also note that $(R^*, \cdot, 1)$ is an abelian group for all rings R.

Definition 4.3. A ring R is called a *field* if all its non-zero elements are units.

From the examples above we can conclude that $\mathbb{Q}$ is a field, $\mathbb{Z}$ is not and $\mathbb{Z}_n$ is a field if and only if n is prime.

Definition 4.4. A non-zero element a of a ring R is called a *zero-divisor* if there exists some $b \in R$ with $b \neq 0$ such that $ab = 0$.

Both $\mathbb{Q}$ and $\mathbb{Z}$ do not have any zero-divisors. Any $m \in \mathbb{Z}_n$ is a zero-divisor if $\gcd(m, n) \neq 1$. In that case $\frac{n}{\gcd(n,m)} \in \mathbb{Z}_n$ and $m \cdot \frac{n}{\gcd(n,m)} \equiv 0 \mod n$. Also every m with $\gcd(n, m) = 1$ is not a zero-divisor. In general it is true that a unit can never be a zero-divisor.

Definition 4.5. A ring R is called a *domain* if it does not contain any zero-divisors.

We see now that $\mathbb{Q}, \mathbb{Z}$ and $\mathbb{Z}_n$ if n is prime, are all domains. If n is not prime then $\mathbb{Z}_n$ is not a domain. Because a unit is never a zero-divisor it also follows that every field is a domain.

Definition 4.6. An element $a \notin R^*$ and $a \neq 0$ of a domain R is called *irreducible* if $a = bc$ implies that b or c is a unit.

Because all non-zero elements in a field are units, fields do not have any irreducible elements. So, $\mathbb{Q}$ does not have any irreducible elements. In $\mathbb{Z}$ an element is irreducible if and only if it is prime or -1 times a prime. $\mathbb{Z}_n$ is either a field or not a domain, so it does not have any irreducible elements.

Definition 4.7. Let R be a domain, then its *quotient field* is the smallest field which contains R. Notation: $Q(R)$.

The main idea behind making a quotient field is adding an inverse with respect to multiplication for every element in R. Then, because $Q(R)$ has to be closed under addition as well as multiplication, some other elements may follow. The quotient field of $\mathbb{Z}$ is $Q(\mathbb{Z}) = \mathbb{Q}$. Obviously the quotient field of a field is itself.

Definition 4.8. Let R be a ring, then its polynomial ring is defined by $\{\sum_{i=0}^{n} a_i X^i \mid a_i \in R\}$. Notation: $R[X]$.

In general we use the notation $R[\alpha]$ for the smallest ring containing both R and α.
Remark that a polynomial ring is indeed a ring with $0, 1$ and the operators of R. It is also true that the polynomial ring of a domain is again a domain. However, $R[X]$ can never be a field because X does not have an inverse.
Irreducible elements of $R[X]$ are sometimes also called irreducible polynomials in R. Some examples of irreducible polynomials in $\mathbb{Q}$ are $X + 1$, $X^2 - 5$ and $\frac{1}{5}X^4 + 2$. But $X^2 - 1$, for instance, is reducible, because it can be written as $(X + 1)(X - 1)$.
In $Z_{11}[X]$ we have that $X^2 - 5 \equiv X^2 - 16 = (X + 4)(X - 4)$, thus then $X^2 - 5$ is reducible.
In the following section polynomial rings and irreducible polynomials will play a central role.

4.2 Algebraic numbers

The first step behind algebraic number theory is to expand the definition of rational numbers and integers. These will be called algebraic numbers and algebraic integers respectively. We know that $\mathbb{Q}$ and $\mathbb{Z}$ have many nice properties, such as prime factorisation and closure under multiplication and addition. We will see that algebraic numbers share some of these properties.

Definition 4.9. An *algebraic number* α *from* $\mathbb{Q}$ is an element in $\mathbb{C}$ such that there exists some non-zero $p(X) \in \mathbb{Q}[X]$ with $p(\alpha) = 0$. The set of all algebraic numbers is called the *algebraic closure of* $\mathbb{Q}$ and is denoted by $\overline{\mathbb{Q}}$.

Note that if α is an algebraic number by $a_n\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0$ and $a_i \in \mathbb{Q}$, then also $a_n + a_{n-1}\frac{1}{\alpha} + \ldots + a_1(\frac{1}{\alpha})^{n-1} + a_0(\frac{1}{\alpha})^n = 0$. So if α is an algebraic number, then $\frac{1}{\alpha}$ is as well.

Definition 4.10. The *degree* of $\alpha \in \overline{\mathbb{Q}}$ is the minimal positive degree of $p(X) \in \mathbb{Q}[X]$ such that α is a root of p.

It is important to understand that the notion of a degree is well-defined. Assume that α is an algebraic number. We can then find a $p(X) \in \mathbb{Q}[X]$ such that $p(\alpha) = 0$. $p(X)$ will have some finite degree n and thus we only have to check whether there also exists a polynomial with root α that has a lower degree.

Definition 4.11. The *minimal polynomial of* $\alpha \in \overline{\mathbb{Q}}$ is some $p(X) \in \mathbb{Q}[X]$ with leading coefficient 1 and the degree of α, such that $p(\alpha) = 0$.

For any algebraic number α we know that there exists some $p(X) \in \mathbb{Q}[X]$ with $p(\alpha) = 0$. Now assume the leading coefficient of p to be a_n. Then $\frac{1}{a_n}p(X)$ also has root α, is still in $\mathbb{Q}[X]$ and has leading coefficient 1. Thus, every $\alpha \in \overline{\mathbb{Q}}$ has a minimal polynomial.

Examples.

- Every element q of $\mathbb{Q}$ is an algebraic number and has minimal polynomial $p(X) = X - q$.
- Let d be some rational number such that $\sqrt{d}$ is irrational. Then $\sqrt{d}$ is an algebraic number with $p(X) = X^2 - d$. If $\sqrt{d}$ is rational, the minimal polynomial is $p(X) = X - \sqrt{d}$.
- Let $\zeta_n = e^{2i\pi/n}$, then it is an n-th root of unity, which is algebraic. If n is odd this has minimal polynomial $p(X) = X^n - 1$. If n is even we get minimal polynomial $X^{n/2} - 1$. Taking $n = 4$ we see that $i \in \mathbb{C}$ is algebraic with minimal polynomial $X^2 - 1$.

Note that the minimal polynomial of α is unique. If this would not be the case we can find two minimal polynomials $p(X)$ and $q(X)$ of α with the same degree. But then $p(X) - q(X)$ also has α as a root, and because p and q both have the same leading coefficient, $(p - q)(X)$ would be a polynomial of lower degree. This is in contradiction with the fact that $p(X)$ and $q(X)$ are minimal. The only possibility is that $p(X) = q(X)$.

Definition 4.12. An *algebraic extension of a field F by $\alpha \in \overline{\mathbb{Q}}$* is the minimal field containing both F and α. It is denoted by $F(\alpha)$.

Pay attention to the difference in notation between the minimal field containing F and α (i.e. $F(\alpha)$), and the minimal ring containing F and α (i.e. $F[\alpha]$).

Examples.

- If we extend $\mathbb{Q}$ with any element q of $\mathbb{Q}$ itself it becomes $\mathbb{Q}$ again. Thus: $\mathbb{Q}(q) = \mathbb{Q}$.
- The most well-known (non-trivial) extension of $\mathbb{Q}$ is $\mathbb{Q}(i)$ consisting of all the complex numbers with rational coefficients. Thus, $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\} \subset \mathbb{C}$.
- $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$ where d is in $\mathbb{Q}$ such that $\sqrt{d}$ is not.
- $\mathbb{Q}(\zeta_n) = \{a_1 + a_2\zeta_n + a_3\zeta_n^2 + \ldots + a_n\zeta_n^{n-1} \mid a_i \in \mathbb{Q}\}$ if $\zeta_n = e^{2i\pi/n}$ and n is odd.
  If n is even $\mathbb{Q}(\zeta_n) = \{a_1 + a_2\zeta_n + a_3\zeta_n^2 + \ldots + a_{n/2}\zeta_n^{n/2-1} \mid a_i \in \mathbb{Q}\}$.

As you may note from previous examples, we needed multiple elements in $\mathbb{Q}$ to describe an element in $\mathbb{Q}(\alpha)$. In this sense we can see algebraic extensions of $\mathbb{Q}$ as $\mathbb{Q}$-vector spaces. Here the dimension of the vector space corresponds to the amount of elements in $\mathbb{Q}$ needed to describe an element of the extension. You may also have noted that we needed exactly $\deg(\alpha)$ elements in $\mathbb{Q}$ to generate $\mathbb{Q}(\alpha)$. This is understandable by looking at powers of α. Every power of α must be in $\mathbb{Q}(\alpha)$ to make it a field. Now if $n < \deg(\alpha)$ we can show that α^n has to be independent from all the smaller powers of α. If they would not be independent, we could write $a_n\alpha^n + \ldots a_1\alpha + a_0 = 0$ with $a_i \in \mathbb{Q}$. But then, $a_nX^n + \ldots a_1X + a_0$ would have α as a root which would give the contradiction that $\deg(\alpha) \leq n$. Furthermore the extensions can also not have a higher dimension than $\deg \alpha$ because $\alpha^{\deg \alpha}$ is not independent with the lower powers of α. We can conclude that the dimension of $\mathbb{Q}(\alpha)$ is $\deg(\alpha)$.
Now, because $\mathbb{Q}(\alpha)$ is again a field we may also extend this field by some $\beta \in \overline{\mathbb{Q}}$. We write this as $\mathbb{Q}(\alpha, \beta)$. We cannot be sure what the dimension of our new field is because β does not have to be independent of α. However, we can say that the dimension stays less than $\deg(\alpha) + \deg(\beta)$, and thus finite.
This motivates the following definition:

Definition 4.13. A *number field* K is a finite field extension of $\mathbb{Q}$. Thus K is a $\mathbb{Q}$-vector space with finite dimension. The dimension of K is called the *degree* of K.

Examples. From our previous analysis of the algebraic extension of our examples we easily find,

- $\mathbb{Q}(q)$ with $q \in \mathbb{Q}$ is a number field of degree 1.
- $\mathbb{Q}(i)$ is a number field of degree 2.
- $\mathbb{Q}(\sqrt{d})$ is a number field of degree 2 if and only if $\sqrt{d} \notin \mathbb{Q}$.
- $\mathbb{Q}(\zeta_n)$ is a number field of degree n if n is odd, and a number field of degree $\frac{n}{2}$ if n is even.

Now we know enough about algebraic numbers to be able to define what an algebraic integer is.

Definition 4.14. An element α of $\overline{\mathbb{Q}}$ is called an *algebraic integer* if its minimal polynomial has only integer coefficients, and thus is in $\mathbb{Z}[X]$.

Examples. Looking back at our examples of minimal polynomials we find,

- $q \in \mathbb{Q}$ is an algebraic integer precisely if $q \in \mathbb{Z}$.
- The same holds for $\sqrt{d}$, it is an algebraic if and only if $d \in \mathbb{Z}$.
- ζ_n (and thus i) is always an algebraic integer.
- However, $q\zeta_n$ with $q \in \mathbb{Q}\backslash\mathbb{Z}$ is not an algebraic integer because it has minimal polynomial $X^n - q$ or $X^{n/2} - q$.

In a similar way can find some $k \in \mathbb{Q}$ such that $k\sqrt{d}$ and kq are algebraic integers, even if $\sqrt{d}$ and q are not. We prove this with the following more general theorem.

Theorem 4.1. *For every number field $\mathbb{Q}(\alpha)$ we can find some $d \in \mathbb{Z}$ such that $d\alpha$ is an algebraic integer and $\mathbb{Q}(\alpha) = \mathbb{Q}(d\alpha)$.*

Proof. Because we know that $\alpha \in \mathbb{Q}(d\alpha)$ and $d\alpha \in \mathbb{Q}(\alpha)$ and that they are both the smallest field containing respectively $d\alpha$ and α, they must be the same number field. Thus what is left to prove is that for each $\alpha \in \overline{\mathbb{Q}}$ there exists some $d \in \mathbb{Z}$ such that $d\alpha$ is an algebraic integer.
It is obvious that for all polynomials $p(X)$ in $\mathbb{Q}[X]$ we can find an integer d such that $dp(X) \in \mathbb{Z}$. Now let $\alpha \in \overline{\mathbb{Q}}$ with minimal polynomial $p(X)$ such that $dp(X)$ has integer coefficients. We will prove that $d\alpha$ is an algebraic integer. First we write $p(X) = \sum_{i=0}^{n} a_i x^i$. Now define $q(x) = \sum_{i=0}^{n} d^{n-i} x^i$, then $q(x) \in \mathbb{Z}$ because all except the leading coefficient are multiplied by at least one factor d, and we already know that the leading coefficient of p is 1. Furthermore $q(d\alpha) = d^n p(\alpha) = 0$, so $d\alpha$ is a root of $q(x)$. Note that $q(X)$ is even the minimal polynomial of $d\alpha$. Because if there would exist a polynomial with lower degree and root $d\alpha$, then there would also be a polynomial with root α of lower degree. To see this you can use the same idea as how we constructed q from p, but replacing d by $\frac{1}{d}$. Thus, every $\alpha \in \overline{\mathbb{Q}}$ can be 'made algebraic' by multiplying it by some factor in $\mathbb{Q}$. □

Definition 4.15. The set of all algebraic integers in a field K is denoted by $\mathcal{O}_K$. We call $\mathcal{O}_K$ the *ring of integers of K*.

In Section 4.4 we will prove that $\mathcal{O}_K$ is indeed a ring for every field $\mathbb{Q}(\alpha)$. For now we will simply assume it.

Examples.

- We can easily see that $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.

- If $K = \mathbb{Q}(i)$ we have that $\mathcal{O}_K = \{a + bi \mid a, b \in \mathbb{Z}\}$. To see this, we note that the minimal polynomial of $a+bi$, for $b \neq 0$, is $X^2 - 2aX + a^2 + b^2$. So $a+bi$ is an algebraic integer if and only if $2a \in \mathbb{Z}$ and $a^2 + b^2 \in \mathbb{Z}$. Because we already know that $a, b \in \mathbb{Q}$ this means that $a, b \in \mathbb{Z}$ or $a - \frac{1}{2} \in \mathbb{Z}$ and $b^2 - \frac{3}{4} \in \mathbb{Z}$. However, the second case is impossible if $b \in \mathbb{Q}$, thus we see that $a, b \in \mathbb{Z}$.

- Let $K = \mathbb{Q}(\sqrt{d})$ with d a square-free integer. Then we claim that,
  $\mathcal{O}_K = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$ if $d \not\equiv 1 \mod 4$ and $\mathcal{O}_K = \{a + b\frac{1+\sqrt{d}}{2} \mid a, b \in \mathbb{Z}\}$ if $d \equiv 1 \mod 4$.
  If we look at $a + b\sqrt{d} \in K$ then we know that it has some minimal polynomial of maximal degree 2. Now $(a + b\sqrt{d})^2 = a^2 + 2ab\sqrt{d} + b^2 d$. Thus $X^2 - 2aX + a^2 - b^2 d$ is its minimal polynomial. Hence, $a + b\sqrt{d}$ is an algebraic integer if $2a$ and $a^2 - b^2 d$ are both integers. This implies that either a is an integer or $a + \frac{1}{2}$ is.
  If a is an integer, then $b^2 d$ has to be an integer as well. We stated that d is square-free, thus it follows that b has to be an integer.
  If $a + \frac{1}{2}$ is an integer we find that $(a + \frac{1}{2})(a - \frac{1}{2}) = a^2 - \frac{1}{4}$ is an integer. Hence, $\frac{1}{4} - b^2 d$ has to be an integer. Write $b = \frac{p}{q}$ with $p, q \in \mathbb{Z}$. Then we want that $\frac{p^2 d}{q^2} = n + \frac{1}{4}$ with $n \in \mathbb{Z}$. Thus $\frac{p^2 d}{q^2} = \frac{4n+1}{4}$ and because 4 is a square this means that $q = 2$ and $p^2 d = 4n + 1$. Now p^2 is either 1 or 0 modulo 4, so the equation only has solutions if d is congruent to 1 modulo 4. If this is the case, p can be any odd integer, meaning that $b + \frac{1}{2}$ is an integer. So for $d \equiv 1 \mod 4$ we have seen that $a + b\sqrt{d}$ is an algebraic integer if $a, b \in \mathbb{Z}$ or $a + \frac{1}{2}, b + \frac{1}{2} \in \mathbb{Z}$. If $d \not\equiv 1 \mod 4$ we are only left with the case that $a, b \in \mathbb{Z}$.

In general it is true that if K has degree n, then $\mathcal{O}_K$ is a $\mathbb{Z}$-vector field of dimension n. Thus we can write $\mathcal{O}_K = \{m_1\omega_1 + m_2\omega_2 + \ldots + m_n\omega_n \mid m_1, \ldots m_n \in \mathbb{Z}\}$. We will not prove this here.

Definition 4.16. Let $\mathcal{O}_K$ equal $\{m_1\omega_1 + m_2\omega_2 + \ldots + m_n\omega_n \mid m_1, \ldots m_n \in \mathbb{Z}\}$, we call the set $\{\omega_1, \ldots, \omega_n\}$ a *basis of integers* in K.

Examples.

- The basis of integers in $\mathbb{Q}$ is $\{1\}$.
- The basis of integers in $\mathbb{Q}(i)$ equals $\{1, i\}$.
- In $\mathbb{Q}(\sqrt{d})$ with $d \not\equiv 1 \mod 4$ the basis of integers is $\{1, \sqrt{d}\}$.
- If $d \equiv 1 \mod 4$ the basis of integers in $\mathbb{Q}(\sqrt{d})$ is $\{1, \frac{1+\sqrt{d}}{2}\}$.

If α is an algebraic integer and $K = \mathbb{Q}(\alpha)$ then obviously $\alpha \in \mathcal{O}_K$. More fore, because $\mathcal{O}_K$ is a ring, we also know that $\alpha^i \in \mathcal{O}_K$ for all $i \in \mathbb{Z}$. This means that $\{m_1 + m_2\alpha + \ldots m_n\alpha^{n-1} \mid m_1, \ldots, m_n \in \mathbb{Z}\} \subset \mathcal{O}_K$. This subset is known as $\mathbb{Z}[\alpha]$, the minimal ring containing both $\mathbb{Z}$ and α. However, it is not always true that $\mathbb{Z}[\alpha] = \mathcal{O}_K$. A counterexample is $\alpha = \sqrt{5}$, then $\frac{1+\sqrt{5}}{2}$ is in the ring of integers but not in $\mathbb{Z}[\sqrt{5}]$.

The index of α is a way to quantify the difference between $\mathcal{O}_K$ and $\mathbb{Z}[\alpha]$. The index is a natural number that tells us how close the basis generated by α comes to generating the ring of integers.

Definition 4.17. Let α be an algebraic integer and $\{\omega_i \mid 0 \leq i \leq n\}$ some basis of integers in $K = \mathbb{Q}(\alpha)$. Assume d_i to be the minimal element of $\mathbb{Z}$ such that $d_i\omega \in \mathbb{Z}[\alpha]$. Then we define the *index of* α as,

$$\text{ind}(\alpha) := \prod_{i=1}^{n} d_i.$$

To show that the index of α is always well-defined we prove the following small lemma.

Lemma 4.2. *Let α be an algebraic integer and $\{\omega_i \mid 0 \leq i \leq n\}$ some basis of integers in $K = \mathbb{Q}(\alpha)$. Then every $\omega_i = a/d_i$ with $a \in \mathbb{Z}[\alpha]$ and $d_i \in \mathbb{Z}$.*

Proof. We know that $\mathbb{Z}[\alpha] \subset \mathcal{O}_K \subset \mathbb{Q}(\alpha) = Q(\mathbb{Z}[\alpha])$. Where the last step follows from the fact that both $\mathbb{Q}$ and α must be in the quotient field of $\mathbb{Z}[\alpha]$. Now because $\omega_i \in \mathbb{Q}(\alpha)$ for all $0 \leq i \leq n$ we have that $\omega_i = \frac{p}{q}a'$ with $p, q \in \mathbb{Z}$ and $a' \in \mathbb{Z}[\alpha]$. Obviously, $pa' \in \mathbb{Z}[\alpha]$ and we can choose $a = pa'$ and $d_i = q$. □

Examples.

- If $\mathcal{O}_K = \mathbb{Z}[\alpha]$ then $\text{ind}(\alpha) = 1$. This is the case for α in $\mathbb{Q}$, i, and $\sqrt{d}$ with $d \not\equiv 1 \mod 4$.
- If $d \equiv 1 \mod 4$, we have that $1 \cdot 1 \in \mathbb{Z}[\sqrt{d}]$ and $2 \cdot \frac{1+\sqrt{d}}{2} \in \mathbb{Z}[\sqrt{d}]$. Hence the index of $\sqrt{d}$ equals 2.

Another way to figure out the index of α is by calculating discriminants. The advantage of this second method is that one does not need to know the basis of integers beforehand. Combining these two equivalent definitions can even be used as a method to calculate the ring of integers of K. We will, however, not need these notions to reach our goal. Hence, we will not discuss them here.

4.3 Ideals

Now that we know what algebraic numbers and integers are we want to study further properties of these rings and fields. Of especial interest to us is the way the integers can be factored. In $\mathbb{Z}$ we know that every integer can be written as a unique product of prime numbers. But if we look at $\mathbb{Q}(\sqrt{7})$ we see that $-6 = (1 + \sqrt{7})(1 - \sqrt{7}) = -2 \cdot 3$. Thus -6 cannot be uniquely factored. However, for every ring of integers $\mathcal{O}_K$ we do have unique factorisation of ideals. We will prove this in Section 4.5, after we have introduced some concepts about ideals and Dedekind domains.

Definition 4.18. Let $(R, +, 0, \cdot, 1)$ be a commutative ring, we say that $I \subset R$ is an *ideal of* R if for all $a, b \in I$ and $r \in R$:

- $ra \in I$,
- $a - b \in I$, so I is an additive subgroup.

Examples.

- For every ring R we have the two trivial ideals R and $\{0\}$.
- If an ideal I contains some unit, I equals the entire ring R. Hence, in a field (such as $\mathbb{Q}$,) the only ideals are the trivial ones.
- For $R = \mathbb{Z}$, we have the ideals $n\mathbb{Z}$ for all $n \in \mathbb{N}$. This is exactly the set containing all elements of the form mn with $m \in \mathbb{Z}$.
- In general, for any commutative ring R, we have that the set consisting of ar for all $a \in R$ and some $r \in R$ is an ideal. We say that this ideal is generated by r and write (r) or rR.
- Let $K = \mathbb{Q}(\sqrt{6})$. In $\mathcal{O}_K$ we then have the ideal $\{m_1 2 + m_2\sqrt{6} \mid m_1, m_2 \in \mathcal{O}_K\}$. We say that this ideal is generated by 2 and $\sqrt{6}$ and write $(2, \sqrt{6})$.

Definition 4.19. An ideal I of R is said to be *generated by* a set of elements $J \subset R$ if $I = \{\sum_{j \in J} m_j j \mid m_j \in R\}$. If I is generated by a single element $r \in R$ we call it a *principal ideal*. Notation: (r).

For every element a of an ideal I of R we can easily see that $(a) \subset I$. Thus I is always generated by a subset of its own elements. (Though, this subset need not be finite.) Besides, every generated set is always an ideal.
In $\mathbb{Z}$ all ideals are principal. Because of this we call $\mathbb{Z}$ a principal ideal domain or PID. We will see that this is also the reason that $\mathbb{Z}$ has both unique factorisation in ideals as in elements (up to units).
Before we can understand factorisation of ideals we need to define the building blocks of these factorisation, prime ideals.

Definition 4.20. Let I be some non-trivial ideal of R, then I is a *prime ideal* if for all $ab \in I$ we have $a \in I$ or $b \in I$.

Note that this definition is consistent with how primes are defined in the natural numbers. If $p \in \mathbb{N}$ is some prime that divides ab with $a, b \in \mathbb{Z}$, then we know that p either divides a or b.

Examples.

- In $\mathbb{Z}$ we have that (n) is a prime ideal exactly when n is prime. If n is not prime we know that n can be written as ab with $a, b \in \mathbb{Z}$ but $a, b \notin (n)$.
- In a field there are no prime ideals.

- In $\mathbb{Z}_n$ all the prime ideals are the ideals (m) such that $\gcd(n, m)$ is prime.
- In $\mathcal{O}_K$ with $K = \mathbb{Q}(i)$ the ideal (2) is not prime. To see this observe that $2 = (1+i)(1-i)$ but neither is in (2).
- If $K = \mathbb{Q}(\sqrt{5})$ the ideal (2) is prime in $\mathcal{O}_K$. This might be surprising because 2 can be written as the product of $-(1+\sqrt{5})$ and $\frac{1+\sqrt{5}}{2}$. However, we proved before that $\frac{1+\sqrt{5}}{2} \in \mathcal{O}_K$ so $(1+\sqrt{5})$ is in (2). In $\mathbb{Z}[\sqrt{5}]$ this argument does not hold and (2) is not prime.

Much like we can add, subtract and multiply integers to get new integers, we can also construct ideals from ideals. This leads to the following lemma.

Lemma 4.3. *Let I and J be two ideals of R, then $I + J = \{i + j \mod i \in I, j \in J\}$, $I \cap J$ and $IJ = \{\sum_{i=1}^{n} x_i y_i \mid x_i \in I, y_i \in J, n \in \mathbb{N}\}$ are again ideals of R. More fore $I + J$ is the smallest ideal that contains both I and J.*

Proof. We will prove these statement by checking the conditions for ideals for each construction separately.
Let $a, b \in I + J$ and $r \in R$ then $a = i_a + j_a$ and $b = i_b + j_b$ with $i_a, i_b \in I$ and $j_a, j_b \in J$. Then $ra \in I + J$, because $ra = ri_a + rj_a$ and we know $ri_a \in I$ and $rj_a \in J$. Also $a - b \in I + J$, because we have that it equals $i_a - i_b + j_a - j_b$ and we know that $i_a - i_b$ and $j_a - j_b$ are in I and J respectively.
Taking $i_a = 0$ we see that $I + J$ contains J, and with $j_a = 0$ we can also make all the elements of I. Furthermore if we are searching an ideal that contains both I and J we need that it contains $I + J$ because otherwise the elements $a - b$ would not be in the ideal. We conclude that $I + J$ is the smallest ideal containing both I and J.
Let $a, b \in I \cap J$ and $r \in R$, then $a, b \in I$ and $a, b \in J$. Now ra also has to be in I and J so $ra \in I \cap J$. Also $a - b$ has to be in both I and J so it has to be in $I \cap J$. Thus we easily see that $I \cap J$ is an ideal.
Let $a, b \in IJ$ and $r \in R$, then $a = \sum_{i=1}^{n} x_{i,a} y_{i,a}$ and $b = \sum_{i=1}^{m} x_{i,b} y_{i,b}$ for some $x_{i,a}, x_{i,b} \in I$ and $y_{i,a}, y_{i,b} \in J$. Thus, $ra = \sum_{i=1}^{n} r x_{i,a} y_{i,a}$ and because $r x_{i,a} \in I$ for all i we see that $ra \in IJ$. This also shows that $-b \in IJ$, so $a - b$ is just the sum of two sums. This is a sum of length $n + m$ where each term is still the product of an element from I with an element from J. So $a - b \in IJ$. This proves that IJ is also an ideal. □

If we look at $\mathbb{Z}$ again we see that $(m)(n)$ is exactly the ideal consisting of integers that are divisible by mn, thus (mn). Also $(m) + (n)$ are the integers that can be written as $am + bn$, using the Euclidian algorithm we know this to be all multiples of $\gcd(m, n)$, so $(m) + (n) = (\gcd(m, n))$. Lastly the ideal $(m) \cap (n)$ consists of the integers that are divisible by both m and n and these are exactly the multiples of $\operatorname{lcm}(m, n)$, and so $(m) \cap (n) = (\operatorname{lcm}(m, n))$.
Before we go further we will look at an equivalent definition of prime ideals that is very useful.

Definition 4.21. Let I be an ideal of R, then I is a *prime ideal* if for all ideals J and H of R such that $JH \subset I$ we have $J \subset I$ or $H \subset I$. In general, if I and J are two ideals of R, we say that I *divides* J if $J \subset I$.

Lemma 4.4. *The two Definitions 4.20 and 4.21 of a prime ideal are equivalent.*

Proof. First we assume that for all $ab \in I$ we know that either $a \in I$ or $b \in I$. Now let J and H be some ideals such that $JH \subset I$ and suppose that H is not contained in I. Then there is some $h \in H$ such that $h \notin I$. However, $jh \in JH$ for all $j \in J$ so jh is in I for all $j \in J$. Because I is a prime ideal this means that either $j \in I$ or $h \in I$. But we assumed that h was not in I, so for any $j \in J$ we find $j \in I$. Thus we have $J \subset I$.
Next we assume that for all $JH \subset I$ we have either $J \subset I$ or $H \subset I$. Suppose some $ab \in I$, then $(a)(b) = (ab) \subset I$. So either $(a) \subset I$ and $a \in I$ or $(b) \subset I$ and $b \in I$. Which is exactly what we wanted to prove. □

This equivalent definition also makes the idea of ideal-division more intuitive. If I is an ideal, $IJ \subset I$ for all ideals J, so I always divides IJ. Furthermore R divides all its own ideals, and can thus be associated with the integer 1. The other trivial ideal $\{0\}$ can be compared to 0. In a similar fashion we can see the $+$ and $\cap$ operations on ideals as searching the gcd or lcm respectively. This is even more motivated by the definition of coprime ideals.

Definition 4.22. We say that two ideals I and J of R are *coprime* if $I + J = R$.

We already proved that $I + J$ is the smallest ideal that divides both I and J. If R is this ideal, that means that there does not exist any other ideal than R that divides both I and J. We can also prove that $IJ = I \cap J$ if the two ideals are indeed coprime. This is again consistent with the idea that $\cap$ is the lcm.
It is also noteworthy that R contains 1, so if I and J are coprime we know that there exist $i \in I$ and $j \in J$ such that $i + j = 1$. This is much like the algorithm of Euclides for coprime integers. If two integers m and n are coprime, there exist $a, b \in \mathbb{Z}$ such that $an + bm = 1$.
Unfortunately it is not true that any prime ideal is only divisible by R or itself. For example the ideal $(1 + \sqrt{5})$ is prime in $\mathbb{Z}[\sqrt{5}]$ but still divides $(1 + \sqrt{5}, 2)$. In this case we say that $(1+\sqrt{5})$ is not maximal. Later on we will see that in number rings we do have that all prime ideals are maximal.

Definition 4.23. A *maximal ideal* I of R is an ideal such that $I \subset J \subset R$ implies $J = I$ or $J = R$. In other words, I is only divisible by R and itself.

Theorem 4.5. *Every maximal ideal is a prime ideal.*

Proof. We will prove this by using Definition 4.20.
Let I be some maximal ideal in R such that $ab \in I$ for some $a, b \in R$. If both $a, b \in I$ then also either a or b is in I and we are done. If one of a and b is not in I we may without loss of generality assume that this is a. Because a is not in I and I is maximal we know that $I + (a) = R$. So we can find some element $i \in I$ and $r \in R$, such that $i + ra = 1$. Multiplying

both sides by b we see that $bi + rab = b$. We assumed $ab \in I$, so both terms on the left side are in I and we may conclude that $b \in I$. Hence, for every $ab \in I$ we have either a or b in I, which exactly means that I is a prime ideal. □

Besides being able to multiply ideals with each other, there is also a way to take their inverses. To do this we need the definition of a fractional ideal.

Definition 4.24. We call J a *fractional ideal of* R if $J \subset Q(R)$ and there is some $r \in R$ such that rJ is an ideal of R.

Examples.

- For every ring R and ideal I of R it is easily seen that I is a fractional ideal by taking $r = 1$.
- In a field the only fractional ideals are the trivial ideals.
- In $\mathbb{Z}$ all fractional ideals are of the form (q) with $q \in \mathbb{Q}$.

We can define multiplication and addition with respect to fractional ideals in a similar was as for normal ideals in Lemma 4.3. Using multiplication we can also define what it means for a fractional ideal to be invertible.

Definition 4.25. A fractional ideal J of R is *invertible* if there exists some other fractional ideal J^{-1} of R such that $JJ^{-1} = R$.

Lemma 4.6. *If a fractional ideal J of R is invertible its inverse J^{-1} has the form $\{x \in Q(R) \mid xJ \subset R\}$.*

Proof. We know that J is invertible so we may assume that there exists some fractional ideal I such that $JI = R$. First we show that J^{-1} is a fractional ideal and then we will prove that J^{-1} has to be a subset of I and I has to be a subset of J^{-1}.
We know that there must exist some element r of R such that rJ is an ideal of R. This implies that for a certain $j \in J$ we have that rj is an element of both J and R. Now let x be some element of J^{-1}. Then $xJ \subset R$ and thus xrj must be in R as well. This shows that rjJ^{-1} is a subset of R. It is easily checked that this subset meets the conditions of an ideal and thus we may conclude that J^{-1} is a fractional ideal.
From how J^{-1} is defined it is immediately clear that $JJ^{-1} \subset R$. This can be rewritten as $JJ^{-1} \subset JI$. Multiplying both sides with I again gives us that indeed $J^{-1} \subset I$.
Let $i \in I$ be arbitrary then from the fact that $JI = R$ it follows that iJ is a subset of R and thus I is also contained in J^{-1}. □

The previous lemma gives us a nice way to check if a fractional ideal is invertible. We only have to check if $JJ^{-1} = R$ with J^{-1} defined as in the lemma.

Examples.

- In $\mathbb{Z}$ all fractional ideals are invertible. If (q) with $q \in \mathbb{Q}$ is some fractional ideal then the inverse equals $(\frac{1}{q})$.
- In $\mathbb{Z}[\sqrt{5}]$ the ideal $(2, 1+\sqrt{5})$ does not have an inverse. We can prove this by showing, if $x \in \mathbb{Q}(\sqrt{5})$ such that $x(2, 1+\sqrt{5})$ contains a unit, then $x(2, 1+\sqrt{5})$ must contain some element that is not in $\mathbb{Z}[\sqrt{5}]$.

In $\mathcal{O}_K$ all ideals have an inverse and the fractional ideals even form a group under multiplication. However, we will not prove this here.
Now, before we move on the next section we need one more key concept of ideals.

Definition 4.26. Let I be some ideal of R, we can then define the *factor ring* R/I by the following equivalence relation:

$$a \equiv b \mod I \text{ if and only if } a - b \in I.$$

Thus $R/I = \{[a] \mid a \in R\}$, where $[a] = \{b \in R \mid a \equiv b \mod I\}$.

We can easily check that every factor ring R/I is again a ring. Take the same operations, zero-element $[0] = I$ and one-element $[1]$.

Examples.

- From the trivial ideals we get the factor rings $R/R = \{0\}$ and $R/\{0\} = R$.
- The factor rings $\mathbb{Z}/(n)$ are exactly the rings $\mathbb{Z}_n$, the residue classes modulo n.
- The factor rings for $R = \mathbb{Z}_n$ and $I = (m)$ are equal to $\mathbb{Z}_{\gcd(m,n)}$.

4.4 Dedekind Domains

The aim of this section will be to prove that $\mathcal{O}_K$ is a Dedekind domain. Dedekind domains were invented by Dedekind precisely to show that $\mathcal{O}_K$ has unique prime ideal factorisation. We will show this in the last section.

Definition 4.27. A *Dedekind domain* is a domain R that satisfies the following three conditions:

- Every non-zero prime ideal of R is maximal,
- R is integrally closed,
- Every ideal I in R is finitely generated.

To fully understand the definition of a Dedekind domain we first need to know what integrally closed means.

Definition 4.28. A domain R is *integrally closed* if for all $\alpha \in Q(R)$ that are the root of some monic $f(X) \in R[X]$ we have $\alpha \in R$.

Examples.

- $\mathbb{Z}$ is integrally closed. To see this assume $\frac{p}{q} \in \mathbb{Q}$ with p and q coprime integers such that $f(X) \in \mathbb{Z}[X]$ is a monic polynomial with $f(\frac{p}{q}) = 0$. Then $f(X)$ has some degree n and can be written as $X^n + a_{n-1}X^{n-1} + \ldots + a_0$ with all $a_i \in \mathbb{Z}$. If we want to write $f(\frac{p}{q})$ as one fraction it will look like $\frac{p^n + a_{n-1}qp^{n-1} + \ldots + a_0q^n}{q^n}$. Obviously the denominator is divisible by q and because p and q are coprime the nominator is not. The only possibility is that $q = 1$ and thus that $\frac{p}{q} \in \mathbb{Z}$.
- Any field is integrally closed because they are their own quotient field.
- $\mathbb{Z}[\sqrt{5}]$ is not integrally closed. Its quotient field is $\mathbb{Q}(\sqrt{5})$, which contains $\frac{1+\sqrt{5}}{2}$. This element has minimal polynomial $X^2 - X - 1$, which is in $\mathbb{Z}[\sqrt{5}][X]$.

We will now show that $\mathcal{O}_K$ meets all three conditions of a Dedekind domain. To do this we check the three conditions separately. We start with showing that each prime ideal of $\mathcal{O}_K$ is also maximal. To do this we need some lemma's that will also be useful later.

Lemma 4.7. *An ideal I of R is maximal if and only if R/I is a field.*

Proof. First we assume that I is maximal and prove that then indeed R/I is a field.
Let $a \in R$ such that $a \notin I$. Because I is maximal we know that $I + (a)$ must equal the entire ring. In particular there have to exist some $i \in I$ and $b \in R$ such that $i + ba = 1$. This makes it clear that $ba \equiv 1 \mod I$ and thus that b is an inverse of a in R/I. So every element in R/I has an inverse and thus all elements are units and R/I is a field.
Second we will assume that R/I is a field, and prove that I has to be maximal.
Let J be an ideal such that $I \subset J$ and $I \neq J$. Then there exits some $a \in J$ such that $a \notin I$. Furthermore, because R/I is a field there is some $b \in R$ with $ab \equiv 1 \mod I$. Now obviously, because I is a subset of J, ab is also equivalent to 1 modulo J. But ab is an element of J, so 1 has to be an element of J. This shows that $J = R$. So there does not exist an ideal unequal to R or I that divides I and we may conclude that I is maximal. □

This lemma also nicely shows that indeed $(1 + \sqrt{5})$ is not maximal in $\mathbb{Z}[\sqrt{5}]$ even though it is prime. When we look at $\mathbb{Z}[\sqrt{5}]/(1 + \sqrt{5})$ we can find that $2 \in \mathbb{Z}[\sqrt{5}]/(1 + \sqrt{5})$ but it does not have an inverse. Also it becomes clear that in $\mathbb{Z}$ all prime ideals are maximal, because $\mathbb{Z}/(p)$ with p prime always equals $\mathbb{Z}_p$ which is a field.

Lemma 4.8. *For every non-zero ideal I of $\mathcal{O}_K$ we have that $\mathcal{O}_K/I$ is finite.*

Proof. We will prove this by showing that $\mathcal{O}_K/I$ is contained in the finite set $\{k_1\omega_1 + \ldots + k_n\omega_n \mid 1 \leq k_i \leq a_0\}$, where a_0 is some rational integer in I and $\{\omega_1, \ldots, \omega_n\}$ is a basis of integers of K.
First we show that I always contains a rational integer. Take $\alpha \in I$ to be any non-zero element. Then we know that $\alpha \in \mathcal{O}_K$, so it has an integer valued minimal polynomial $p(X) = \sum_{i=0}^{n} a_i x^i$. Using the properties of ideals and the fact that $\mathbb{Z}[\alpha] \subset \mathcal{O}_K$, we can easily

establish that a_0 must be in I. Also, because $p(X)$ is minimal we know that $a_0 \neq 0$ and thus a_0 is as required.
Next we take an arbitrary element β from $\mathcal{O}_K$ and prove that it is always equivalent to some element $k_1\omega_1 + \ldots + k_n\omega_n$ modulo I. β can be written as $m_1\omega_1 + \ldots + m_n\omega_n$ with $m_i \in \mathbb{Z}$. Also, $a_0\omega_i$ is in I for all elements ω_i of the basis. Thus if for each $1 \leq i \leq n$, we let k_i be the residue of m_i modulo a_0 it becomes clear that indeed $\beta \equiv k_1\omega_1 + \ldots + k_n\omega_n \mod I$ with $1 \leq k_i \leq a_0$.
In the set $\{k_1\omega_1 + \ldots + k_n\omega_n \mid 1 \leq k_i \leq a_0\}$ there are exactly a_0^n possibilities for the n-tuple $(k_1, \ldots, k_n)$, so the set is finite. We conclude that $\mathcal{O}_K/I$ is the subset of a finite set, which shows that $\mathcal{O}_K/I$ itself must be finite. □

Definition 4.29. The cardinality of $\mathcal{O}_K/I$ is also called the *norm* or *index of* I.
Notation: $N(I)$.

Note that we also already knew that Lemma 4.8 was true for $\mathbb{Z}$. In $\mathbb{Z}$ all the ideals are of the form (m) with $m \in \mathbb{Z}$. We know that $\mathbb{Z}/(m) = \mathbb{Z}_m$, which is finite. More specifically, $\mathbb{Z}_m$ is exactly the set $\{k_1 \cdot 1 \mid 1 \leq k_1 \leq m\}$ and $\{1\}$ is a basis for $\mathbb{Z}$. This also shows that the index of (m) in $\mathbb{Z}$ is m.
Now we know enough to prove the first property fo a Dedekind Domain.

Theorem 4.9. *Every non-zero prime ideal of $\mathcal{O}_K$ is maximal.*

Proof. We will prove this by showing that $\mathcal{O}_K/\wp$ is a field for all prime ideals $\wp$ of $\mathcal{O}_K$.
Let $\wp$ be some non-zero prime ideal. In the case that $\wp = \mathcal{O}_K$ we know that $\mathcal{O}_K/\mathcal{O}_K = \{0\}$, which is a field. Otherwise we can find some α in $\mathcal{O}_K$ that is not in $\wp$. Looking at the powers $\{\alpha, \alpha^2, \ldots\}$ of α and using that Lemma 4.8 implies that $\mathcal{O}_K/\wp$ is finite, we can find two integers $k > l$ such that $\alpha^k \equiv \alpha^l \mod \wp$. This is equivalent to saying that there is some element $p \in \wp$ with $\alpha^k - p = \alpha^l$. This expression can be rewritten to become $\alpha^l(\alpha^{k-l} - 1) \in \wp$. Because $\wp$ is prime this shows that either $\alpha^l \in \wp$ or $\alpha^{k-l} - 1 \in \wp$.
In the first case, that $\alpha^l \in \wp$, we can use again that $\wp$ is prime to find that either α^{l-1} or α must be in $\wp$. By an induction argument this will eventually lead to $\alpha \in \wp$. This is obviously in contradiction with our assumption so we find $\alpha^l \notin \wp$.
We are left with the second case that $\alpha^{k-l} - 1 \in \wp$. This can also be phrased as, $\alpha^{k-l} \equiv 1 \mod \wp$. Hence, α^{k-l-1} is an inverse of α modulo $\wp$. So, we have proved that every α that is not in $\wp$ but is in $\mathcal{O}_K$, has an inverse modulo $\wp$ and we may conclude that $\mathcal{O}_K/\wp$ is a field. Using Lemma 4.7 this means that $\wp$ is indeed maximal. □

Next we will show that $\mathcal{O}_K$ is also integrally closed. The most important idea of the proof is Lemma 4.11, that states a new way to check if some algebraic number is an integer. Hence, we will first work towards proving Lemma 4.11 and then use it to prove that $\mathcal{O}_K$ is indeed integrally closed.

Lemma 4.10. *Let $\alpha \in \overline{\mathbb{Q}}$ such that there exists some monic polynomial $f(X) \in \mathbb{Z}[X]$ with $f(\alpha) = 0$, then α is an algebraic integer.*

Proof. The aim of this proof will be to show that the minimal polynomial $p(X)$ of α also lies in $\mathbb{Z}[X]$. We will do this by first proving that $f(X)$ is divisible by $p(X)$, and then that any monic divisor of an integer valued polynomial must itself be integer valued.
Let $p(X)$ be the minimal polynomial of α. Certainly, we know that $p(X) \in \mathbb{Q}[X]$ and $\deg(f) \geq \deg(p)$. Thus we can rewrite $f(X)$ as, $f(X) = g(X)p(X) + r(X)$. Where $g(X), r(X) \in \mathbb{Q}[X]$ such that $r(X)$ has minimal degree. This means that the degree of $r(X)$ is less than the degree of $p(X)$. If this were not the case, and the leading coefficient of $r(X)$ is a, then $r'(X) = r(X) - aX^{\deg(r)-\deg(p)}p(X)$ would have a lower degree and still meet the equation with $g'(X) = g(X) + aX^{\deg(r)-\deg(p)}$.
Also noting that $r(\alpha) = 0$, because α is a root of both p and f, this only leaves the possibility that $r(X) = 0$. Thus, we see that $f(X) = g(X)p(X)$ for some polynomial $g(X) \in \mathbb{Q}[X]$.
Now define d_p and d_g to be the minimal rational integers such that $d_p p(X)$ and $d_g g(X)$ are in $\mathbb{Z}[X]$. If $p(X)$ itself is not integer-valued, then d_p must be greater than 1. In that case d_p is divisible by some prime factor q. Note that because d_p is minimal, the coefficients of $d_p p(X)$ cannot all be divisible by q. f and g are also not divisible by q because they are monic, but $d_p f$ is divisible by q. Now we will consider two cases. Either q does divide d_g or q does not divide d_g.
In the first case that q does divide d_g we know by a similar argument as before that q does not divide $d_g g$. This means that q does not divide $d_p d_g pg$, but this equals $d_p d_g f$ so is a contradiction.
In the second case that q does not divide d_g, we find that $d_g pg = d_g f$ contains no factors q. So $d_g g$ contains no factors q and neither may $d_p d_g pg$. But obviously $d_p d_g f$ does contain a factor q, and we have again a contradiction.
We conclude that in both cases d_p cannot contain a factor q and thus d_p must equal 1. This means that p is an integer-valued polynomial and α is an algebraic integer. □

The lemma shows us that the requirements for α to be an algebraic integer from Definition 4.14 can be slightly relaxed. Using this new less strict requirement we can also give a completely different description of algebraic integers.

Lemma 4.11. *Let $\alpha_1, \ldots, \alpha_m \in \overline{\mathbb{Q}}$, then $\mathbb{Z}[\alpha_1, \ldots, \alpha_m]$ is finitely generated in $\mathbb{Z}$ if and only if $\alpha_1, \ldots, \alpha_m$ are all algebraic integers.*

Proof. The lemma will be proved by induction to m. First we will prove that it is true for $m = 1$.
Assume that $\mathbb{Z}[\alpha_1]$ is finitely generated. To prove that α_1 is an algebraic integer we need to find some monic polynomial with coefficients in $\mathbb{Z}$ that has α_1 as a root.
We know that all powers of α_1 must be in $\mathbb{Z}[\alpha_1]$. But because $\mathbb{Z}[\alpha_1]$ is finitely generated there must be some $n \in \mathbb{N}$ such that α_1^n can be written as $\sum_{i=0}^{n-1} a_i \alpha_1^i$ with $a_i \in \mathbb{Z}$. Now we can easily check that α_1 is the root of $X^n - (a_{n-1}X^{n-1} + \ldots + a_1 X + a_0)$. This polynomial is integer-valued and monic thus by Lemma 4.10 we see that α_1 is an algebraic integer.
Next we assume that α_1 is an algebraic integer and prove that $\mathbb{Z}[\alpha_1]$ is finitely generated.
We know that $\mathbb{Z}[\alpha_1]$ is the smallest ring containing both $\mathbb{Z}$ and α_1, and that each element

can be written as $m_0 + m_1\alpha_1 + m_2\alpha_1^2 + \ldots$ with $m_i \in \mathbb{Z}$. Furthermore, because α_1 is an algebraic integer, we know that there exists some integer-valued minimal polynomial $p(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0$. We know that $p(\alpha_1) = 0$ and hence $\alpha_1^n = -(a_{n-1}\alpha_1^{n-1} + \ldots + a_0)$. So we see, for all $i \geq n$, that α_1^i is dependent on $(1, \ldots, \alpha_1^{n-1})$. This means that $\mathbb{Z}[\alpha_1]$ can be generated by the first n powers of α_1 and thus is finitely generated.
The lemma is now proved for $m = 1$. Let us assume that we know the lemma to be true up to some $m = k$. So $\mathbb{Z}[\alpha_1, \ldots, \alpha_k]$ is finitely generated if and only if $\alpha_1, \ldots, \alpha_k$ are all algebraic integers. We prove that the statement of the lemma is also true for $m = k + 1$.
First we assume that $\mathbb{Z}[\alpha_1, \ldots, \alpha_{k+1}]$ is finitely generated and prove that all α_i are algebraic integers. Let i be some integer between 1 and $k+1$. Then $\mathbb{Z}[\alpha_i]$ is a subset of $\mathbb{Z}[\alpha_1, \ldots, \alpha_{k+1}]$ which is finitely generated. This means that $\mathbb{Z}[\alpha_i]$ must also be finitely generated. We already proved that the statement is true for $m = 1$ so we easily see that then indeed, α_i is an algebraic integer for all $1 \leq i \leq k + 1$.
Now assume that $\alpha_1, \ldots, \alpha_{k+1}$ are all algebraic integers. By our induction hypothesis we already know that $\mathbb{Z}[\alpha_1, \ldots, \alpha_k]$ is finitely generated. Also all powers of α_{k+1} can be written as a finite combination of terms, because $\mathbb{Z}[\alpha_{k+1}]$ is finitely generated. So every element of $\mathbb{Z}[\alpha_1, \ldots, \alpha_{k+1}]$ can be written as $a_0 + a_1\alpha_{k+1} + \ldots + a_{n-1}\alpha_{k+1}^{n-1}$ where n is the degree of α_{k+1} and $a_i \in \mathbb{Z}[\alpha_1, \ldots, \alpha_k]$. If we assume that $\mathbb{Z}[\alpha_1, \ldots, \alpha_k]$ is generated in $\mathbb{Z}$ by l elements, we can write every a_i in a basis of l elements. So we can write every element in $\mathbb{Z}[\alpha_1, \ldots, \alpha_{k+1}]$ in a basis of at most ln elements which means that it is finitely generated, as wished.
By induction we may now conclude that the lemma is true for all $m \in \mathbb{N}$, as wished. □

Examples.

- To get a better intuition about why $\mathbb{Z}[\alpha]$ is not finitely generated if α is not an algebraic integer you may look at $\alpha = \frac{1}{2}$. If the basis is finite there has to be some biggest n such that $\frac{1}{2}^n$ is in the basis. We can then never make $\frac{1}{2}^{n+1}$ using this basis, because the sum over smaller powers than $n + 1$ always has a denominator of maximally 2^n. So we see that $\mathbb{Z}[\frac{1}{2}]$ is cannot be finitely generated.

Now we have all the tools we need to prove that $\mathcal{O}_K$ is integrally closed. However, we are also finally ready to show that $\mathcal{O}_K$ is a ring. This is obviously another important property that a set must have before it can be a Dedekind domain.

Theorem 4.12. *Every ring of integers $\mathcal{O}_K$ is a ring.*

Proof. It is obvious that $0, 1 \in \mathcal{O}_K$ and that $+$ and $\cdot$ meet the requirements. All that is left to prove is that $\mathcal{O}_K$ is closed under multiplication and addition. Let α and β be two arbitrary elements of $\mathcal{O}_K$, then obviously they are both in $\mathbb{Z}[\alpha, \beta]$. Lemma 4.11 tells us that this ring must be finitely generated because α and β are both algebraic integers. Furthermore, the sets $\mathbb{Z}[\alpha \cdot \beta]$ and $\mathbb{Z}[\alpha + \beta]$ are subsets of $\mathbb{Z}[\alpha, \beta]$ and thus, also finitely generated. Using Lemma 4.11 for a second time we see that $\alpha\beta$ and $\alpha + \beta$ must be algebraic integers in $\mathcal{O}_K$. We may now conclude that $\mathcal{O}_K$ is indeed closed under multiplication and addition and so that $\mathcal{O}_K$ is a ring. □

Theorem 4.13. *$\mathcal{O}_K$ is integrally closed.*

Proof. For every ring of integers there must be some field $F \subset \overline{\mathbb{Q}}$ such that $Q(\mathcal{O}_K) = F$ and $\mathcal{O}_K = \mathcal{O}_F$. This is easily seen by remarking that $\mathcal{O}_K \subset F \subset K$, so $\mathcal{O}_K \subset \mathcal{O}_F \subset \mathcal{O}_K$. Thus we may assume that $Q(\mathcal{O}_K) = K$.
Now, let $\alpha \in K$ such that there exists some monic polynomial $f(X)$ in $\mathcal{O}_K[X]$ with $f(\alpha) = 0$. We want to prove that $\alpha \in \mathcal{O}_K$, which is equivalent to showing that α is an algebraic integer. We can write $f(X)$ as $X^n + a_{n-1}X^{n-1} + \ldots + a_0$, with $a_i \in \mathcal{O}_K$. From Lemma 4.11 we know that $\mathbb{Z}[a_0, \ldots, a_{n-1}]$ is finitely generated. Furthermore with the help from $f(X)$ it is clear that α^n can be written as $-(a_{n-1}\alpha^{n-1} + \ldots + a_0)$. So α^i with $i \geq n$ is a linear combination of $(\alpha, \ldots, \alpha^{n-1})$ in $\mathbb{Z}[a_0, \ldots a_{n-1}]$. This shows that $\mathbb{Z}[a_0, \ldots, a_{n-1}, \alpha]$ is finitely generated and thus that α must be an algebraic integer. This proves that $\alpha \in \mathcal{O}_K$ and thus that $\mathcal{O}_K$ is integrally closed. □

Finally we need to show that every ideal of $\mathcal{O}_K$ is finitely generated. This is fortunately not very hard and we can state the theorem immediately.

Theorem 4.14. *Every ideal of $\mathcal{O}_K$ is finitely generated.*

Proof. Let $I \subset \mathcal{O}_K$ be some ideal of $\mathcal{O}_K$. We know that $\mathcal{O}_K = \{m_1\omega_1 + \ldots + m_n\omega_n \mid m_i \in \mathbb{Z}\}$ for some basis of integers $\{\omega_i \mid 0 \leq i \leq n\}$. Hence, there do not exist $n+1$ independent elements in $\mathcal{O}_K$. Because I is a subset of $\mathcal{O}_K$ this also means that there do not exist $n+1$ independent elements in I, and we can easily conclude that I must be finitely generated. □

The Theorems 4.9, 4.13 and 4.14 show that $\mathcal{O}_K$ is indeed a Dedekind domain.

4.5 Unique prime ideal factorisation

For I an ideal of $\mathcal{O}_K$ we will prove in this section that I has a unique factorisation in prime ideals of $\mathcal{O}_K$ up to ordering of factors. We already mentioned that any Dedekind domain has this property. The proof for an arbitrary Dedekind domain is similar to the proof for $\mathcal{O}_K$ but less intuitive.
The setup of this section will that we first prove some of the harder steps of the proof of Theorem 4.19 in the form of lemma's and then end with the actual proof.

Lemma 4.15. *Every non-zero prime ideal I in $\mathcal{O}_K$ contains a finite product of non-zero prime ideals.*

Proof. We will prove this by contradiction. So first assume that there exist some ideals such that the lemma does not hold. Then there must also exist an ideal I with smallest index or norm $N(I)$ such that the lemma does not hold. We may assume that I is not prime itself and that I does not equal $\mathcal{O}_K$ entirely, because we know that $\mathcal{O}_K$ contains prime ideals.

This implies that there exist $a, b \in \mathcal{O}_K$ such that neither is in I but their product ab is in I. Thus $I + (a)$ and $I + (b)$ are both ideals that are unequal to I but do contain I. Now this gives us that $\mathcal{O}_K/(I + (a)) \subset \mathcal{O}_K/I$ but they can't be equal, because a is an element of $\mathcal{O}_K/I$ but it equals 0 in $\mathcal{O}_K/(I + (a))$. The same argument holds for the ideal $I + (b)$ and we may conclude that $N(I + (a)) < N(I)$ and $N(I + (b)) < N(I)$. Because we chose I to be the ideal with the smallest index such that the lemma does not hold we see that the lemma does hold for $I + (a)$ and $I + (b)$. Let $\wp_1 \cdots \wp_n \subset I + (a)$ and $\wp_{n+1} \cdots \wp_m \subset I + (b)$ for two integers $m > n$. Then we see taht $\wp_1 \cdots \wp_m \subset (I + (a))(I + (b)) = I^2 + aI + bI + (ab) \subset I$, where the last step follows because $ab \in I$. Thus I contains the product of prime ideals $\wp_1 \cdots \wp_m$. This is in contradiction with our assumption and we see that all ideals must contain a product of prime ideals. □

The Lemma 4.15 shows that every ideal divides some product of prime ideals but does not yet show that every ideal equals a product of prime ideals.

Lemma 4.16. *Let I be an ideal of an integrally closed domain R such that I is finitely generated. Then for all $x \in Q(R)$ such that $xI \subset I$ we have that x is integral in R.*

Proof. The proof we will give is unfortunately rather technical. We will start with expressing some elements in xI in the generating elements of I. Then we will show that these expressions can be combined to find a polynomial with root x in $R[X]$. Thus using that R is integrally closed we will find that $x \in R$.
First we want to be able to write elements of I in a unique way. Because I is finitely generated in R we know that all elements can be written as $\{a_1\omega_1 + \cdots + a_n\omega_n \mid a_i \in R\}$ where $\{\omega_i \mid 1 \leq i \leq n\}$ is some subset of R. We may also assume that n is minimal, hence, all ω_i are independent of each other. Now because $x\omega_i \in xI \subset I$ for all i this means that we have the following equalities:

$$\begin{aligned} x\omega_1 =& a_{1,1}\omega_1 + \ldots + a_{n,1}\omega_n \\ & \ldots \\ x\omega_n =& a_{1,n}\omega_1 + \ldots + a_{n,n}\omega_n. \end{aligned}$$

For some $a_{i,j} \in R$.
We make the following more general claim. Let $m \geq 2$ a rational integer such that we have the m equations:

$$\begin{aligned} f_1(x)\omega_1 =& g_{1,1}(x)\omega_1 + \ldots + g_{m,1}(x)\omega_m \\ & \ldots \\ f_m(x)\omega_m =& g_{1,m}(x)\omega_1 + \ldots + g_{m,m}(x)\omega_m \end{aligned}$$

with $f_i, g_{i,j} \in R[X]$ and $\deg(f_i) > \max_{j \leq m}(\deg(g_{i,j}))$ for all $1 \leq i \leq m$. Then we can find $m - 1$ such equations with the same properties in $\omega_1, \ldots, \omega_{m-1}$ and x.
To see this we rewrite the last equation as,

$$h(x)\omega_m = g_{1,m}(x)\omega_1 + \ldots + g_{m-1,m}(x)\omega_{m-1}. \tag{4.1}$$

Where we define $h(x) := (f_m(x) - g_{m,m}(x))$. Note that the degree of $h(x)$ is the degree of $f_m(x)$.
Now we multiply all other $m-1$ equations by $h(x)$ and get:

$$\begin{aligned} h(x)f_1(x)\omega_1 &= g_{1,1}(x)h(x)\omega_1 + \ldots + g_{m,1}(x)h(x)\omega_m \\ &\ldots \\ h(x)f_{m-1}(x)\omega_{m-1} &= g_{1,m-1}(x)h(x)\omega_1 + \ldots + g_{m,m-1}(x)h(x)\omega_m. \end{aligned}$$

If we then substitute the last term of each equation by equation (4.1), we see that ω_m disapears. The polynomial on the left side of the i-th equation will have the degree of f_m times the degree of f_i. And the polynomial in front of each ω_j on the right side will have a degree of $\deg(g_{i,j})\deg(f_m)$ or $\deg(g_{m,j})\deg(g_{j,m})$ depending on which is greater. However it is obvious that the degree of the polynomial on the left side is greater than the degrees of all polynomials on the right side. Thus we have found $m-1$ equations that have the same properties as the previous m equations. And we have proved our claim.
The equations for $x\omega_i$ that we found before, also meet the conditions of the claim. Thus using induction we can reduce these n equation to one equation of the form,

$$f(x)\omega_1 = g(x)\omega_1.$$

Here $f(X), g(X) \in R[X]$ and $f(X)$ has a greater degree than $g(X)$.
We can now easily see that $f(X) - g(X)$ is a non-zero polynomial in $R[X]$ with root x, and we are done. □

Lemma 4.17. *For each non-zero prime ideal $\wp$ of $\mathcal{O}_K$, the fractional ideal $\wp^{-1} = \{\alpha \in K \mid \alpha\wp \subset \mathcal{O}_K\}$ satisfies:*

- $\mathcal{O}_K \subsetneq \wp^{-1}$
- $\wp\wp^{-1} = \mathcal{O}_K$.

In particular every prime ideal of $\mathcal{O}_K$ is invertible.

Proof. Let $\wp$ be some non-zero prime ideal of $\mathcal{O}_K$. For any ideal of $\mathcal{O}_K$ we know that it must be a subset of $\mathcal{O}_K$, so in particular $\wp \subset \mathcal{O}_K$. This also implies that for each $\alpha \in \mathcal{O}_K$ we have $\alpha\wp \subset \mathcal{O}_K$ and by the definition of $\wp^{-1}$ that $\alpha \in \wp^{-1}$. Hence all element of $\mathcal{O}_K$ are in $\wp^{-1}$ and $\mathcal{O}_K \subset \wp^{-1}$.
To see the equation is also strict we need to find some α in $\wp^{-1}$ that is not in $\mathcal{O}_K$. We do this by considering some $x \in \wp$ and finding an element $y \cdot x^{-1} \in \wp^{-1}$ which cannot be in the ring of integers.
Let $x \in \wp$, then $(x) \subset \wp$ and from Lemma 4.15 we know that there exist $\wp_1 \cdots \wp_n \subset (x) \subset \wp$, where $\wp_i$ for $1 \leq i \leq n$ are all prime ideals. Assume that n is the minimal integer such that such prime ideals exist. If $n = 1$ we find that $\wp_1$ must equal $\wp$ by maximality of prime ideals. Thus then $\wp = (x)$ and $x^{-1} \in \wp^{-1}$ but $x^{-1} \notin \mathcal{O}_K$ because if it would be in $\mathcal{O}_K$ we would have $\wp = \mathcal{O}_K$, which is not a prime ideal.

Thus we may assume that $n \geq 2$. Now because $\wp$ is prime there must be some $\wp_i \subset \wp$. Without loss of generality we may assume this to be $\wp_1$. Also because all prime ideals are maximal we find that $\wp_1 = \wp$. However we know that x does not contain $\wp_2 \cdots \wp_n$ because then n wouldn't be minimal. So there exists some $y \in \wp_2 \cdots \wp_n$ such that $y \notin (x)$. This also implies that $y \cdot x^{-1} \notin \mathcal{O}_K$. If $y \cdot x^{-1}$ was in $\mathcal{O}_K$, then $x \cdot y \cdot x^{-1} = y$ would be in (x). However, we do have that $y \cdot x^{-1}\wp \subset x^{-1}\wp\wp_2 \cdots \wp_n \subset \mathcal{O}_K$. Thus we see that $y \cdot x^{-1}$ is an element of $\wp^{-1}$. This proves the first statement of the lemma.
For the second part of the lemma we use the first part and Lemma 4.16. From the first we know that there exists some x in $\wp^{-1}$ that x is not in $\mathcal{O}_K$. This implies that $x\wp$ is a subset of $\mathcal{O}_K$ and because $\wp$ is also a subset of $\mathcal{O}_K$ itself we know that $\wp + x\wp \subset \mathcal{O}_K$. Now, because $\wp$ is maximal and a subset of $\wp + x\wp$, we see that there are two possibilities. Either $\wp + x\wp = \wp$ or $\wp + x\wp = \mathcal{O}_K$. In the first case $x\wp \subset \wp$ and by Lemma 4.16 we see that x is integral which is a contradiction with the fact that $x \notin \mathcal{O}_K$. Thus we are left with the case that $\wp + x\wp = \mathcal{O}_K$. Then it is obvious that $\wp(\mathcal{O}_K + x\mathcal{O}_K) = \mathcal{O}_K$ and we see that $\mathcal{O}_K + x\mathcal{O}_K = \wp^{-1}$ which has indeed the property that $\wp\wp^{-1} = \mathcal{O}_K$. Now we have proved the second statement and thus the entire lemma. □

Lemma 4.18. *Let R be a ring such that all its ideals are finitely generated. Then for all ideals I of R there exists some maximal ideal J of R such that $I \subset J$.*

Proof. If I is maximal, the lemma is obviously true by choosing $J = I$. If I is not maximal we know that there exists some ideal I_1 such that $I \subsetneq I_1 \subsetneq \mathcal{O}_K$. Now, either I_1 is maximal and a good choice for J or there exists some ideal I_2 such that $I \subsetneq I_1 \subsetneq I_2 \subsetneq \mathcal{O}_K$. In this manner we may construct a chain of ideals $(I_n)_{n\in\mathbb{N}}$ with the property that either for all $i \in \mathbb{N}$ we have $I_i \subsetneq I_{i+1} \subsetneq \mathcal{O}_K$, or there is some $n \in \mathbb{N}$ such that I_n is maximal. In the second case we are done because we may choose $J = I_n$. In the first case we have an infinitely long chain of non-maximal ideals. We will prove that this is not possible.
It is easily shown that $\cup_{i\in\mathbb{N}} I_i$ is an ideal of R as well. This ideal must be finitely generated because all ideals of R are. But because it is finite there must be some smallest index $j \in \mathbb{N}$ such that I_j contains all generators of the union ideal. However then for all $i \geq j$ we have that $I_i = I_j$ which contradicts the fact that $I_j \subsetneq I_{j+1}$. It follows that such an infinite chain is not possible and thus that there must exist some maximal ideal J such that $I \subset J$. □

Theorem 4.19. *Every non-trivial ideal of $\mathcal{O}_K$ is uniquely a product of non-zero prime ideals in $\mathcal{O}_K$.*

Proof. To prove this theorem we have to show two things. We have to show that there exists a factorisation of every ideal in $\mathcal{O}_K$ and we have to show that this factorisation is unique.
To prove existence we use Lemma 4.15 to find a product of prime ideals $\wp_1 \cdots \wp_m$ that is divided by I and then do induction on m.
First we assume that $m = 1$ which gives us $\wp_1 \subset I$. By maximality it directly follows that I must equal $\wp_1$, which gives us a trivial factorisation in prime ideals.
Next we assume the induction hypothesis: if I divides a product of $m = k$ non-zero prime ideals, then I can be written as the product of non-zero prime ideals. We will prove that

this implies that it is also true for $m = k + 1$.
Let I be a non-zero prime ideal such that it divides $\wp_1 \cdots \wp_{k+1}$. We may assume that I itself is not prime and thus not maximal. Using the fact that all ideals in $\mathcal{O}_K$ are finitely generated and Lemma 4.18 this means we can find some maximal ideal $\wp$ such that $\wp_1 \cdots \wp_{k+1} \subset I \subset \wp \subset \mathcal{O}_K$. From the definition of prime ideals it follows that there must be some $\wp_i$ in the product that is contained in $\wp$ and by maximality even equal to $\wp$. Without loss of generality we may assume this to be $\wp_{k+1}$. Furthermore, Lemma 4.17 tells us that $\wp$ has some inverse $\wp^{-1}$ such that $\wp\wp^{-1} = \mathcal{O}_K$. This gives us the following expression: $\wp_1 \cdots \wp_k \subset I\wp^{-1} \subset \wp\wp^{-1} = \mathcal{O}_K$.
Note that $I\wp^{-1}$ is a fractional ideal which is contained in $\mathcal{O}_K$, and thus it is an actual ideal. It is even an ideal that contains a product of k prime ideals. By our induction hypothesis this means that it can be written as a product of prime ideals. If we multiply the factorisation of $I\wp{-}1$ again by $\wp$ we get I and hence I equals some product of prime ideals. From the notion of induction it now follows that for all m such that I divides a product of m prime ideals we have that I equals a product of prime ideals. This finishes the proof of existence.
To show that the factorisation for each ideal I is also unique we will first assume the contrary. Suppose we have some ideal I that does not have a unique factorisation. Then there exist at least two products of prime ideals, $\wp_1 \cdots \wp_m$ and $\wp'_1 \cdots \wp'_r$, that both equal I. Because all $\wp$ and $\wp'$ have inverses we may assume that for all i, j we have $\wp_i \neq \wp'_j$. We also know that $\wp_1 \cdots \wp_n \subset \wp_1$, so that $\wp'_1 \cdots \wp'_r$ is a subset of $\wp_1$. However because $\wp_1$ is prime this means that there is some j such that $\wp'_j \subset \wp_1$, and by maximality they are even equal. This is in contradiction with our previous statement and we conclude that no such I can exist. So every I can be factored uniquely into non-zero prime ideals. □

Chapter 5

Lower bounds using algebraic number theory

To be able to use Theorem 3.1, given some polynomial f, we need to find an integer m such that m meets the requirements as stated in Theorem 3.1. To make this more precise we have the following definition.

Definition 5.1. Consider a polynomial $f = \sum_{i=k}^{d} a_i X^i \in \mathbb{Z}[X]$. We will say that an integer m *meets the requirements of Theorem 3.1 with regard to* f if it is square-free, $\gcd(m, a_k) = 1$ and if for all $x \in \mathbb{Z}$ such that $f(x) \equiv 0 \mod m$ we have that $x \equiv 0 \mod m$.

The aim of this chapter will be to find such m and to even find m such that we can estimate γ to be strictly greater than $\frac{d-1}{d}$. (Note that this is exactly the case if we can find a set $R \subset [m]$ with $|R| \geq 2$ such that $(R - R) \cap \{x^k \mod m | x \in [m]\} = \{0\}$.)

A useful tool in finding m that meet the requirements of Theorem 3.1 is Dedekind's criterion. In the first section we will discuss the theory behind this criterion. In the second section we will apply the criterion to give a condition for m to check if m might be a good choice. There we will also show that for all monic f there are arbitrary big m that meet the requirements of Theorem 3.1. For this we use Chebotarev's density Theorem. In the third section we will find m for some f such that $|R| \geq 2$ and thus $\gamma > \frac{d-1}{d}$.

5.1 Dedekind's criterion

In this section we will prove Dedekind's criterion. The proof will use the theory that has been discussed in Chapter 4 and is based on [4]. We start with stating the criterion.

Theorem 5.1 (Dedekind's criterion)**.** *Let p be a prime in $\mathbb{Z}$ and $\alpha \in \mathcal{O}_K$ such that $K = \mathbb{Q}(\alpha)$ and p does not divide the index of α. Let $g(X)$ be the minimal polynomial of α and let*

$g(X) \equiv g_1(X)^{e_1} \dots g_r(X)^{e_r} \mod p$ *be its factorisation into distinct irreducible factors* $g_i(X)$ *modulo* p. *Then the ideals* $\wp_i = (p, g_i(\alpha))$ *are prime ideals and we have* $(p) = \wp_1^{e_1} \dots \wp_r^{e_r}$.

Similar to the proof of unique factorisation of ideals, we will first prove some steps in between and end with the proof of Theorem 5.1. The idea of the proof of this theorem will be to first show that all $(p, g_i(\alpha))$ are prime ideals, then that their product is contained in (p) and finally that the index of this product equals the index of (p).
To show that $\wp_i$ are prime ideals it will be enough to show that they are maximal ideals. To do this the next three theorems will be useful.

Theorem 5.2. *Let* $K = \mathbb{Q}(\alpha)$ *for some algebraic integer* α *and let* $p \in \mathbb{Z}$ *be prime that does not divide the index of* α. *Then* $\mathcal{O}_K/(p) = \mathbb{Z}[\alpha]/(p)$. *Here* $(p) = p\mathcal{O}_K$.

Proof. We defined the index of α to be the product of the denominators of the elements in the basis of $\mathcal{O}_K$. Because p does not divide this index and p is prime we know that the greatest common divisor of each denominator and p is always 1. Let ω_i be some element of the basis $\mathcal{O}_K$ that is not in $\mathbb{Z}[\alpha]$. Then ω_i has a denominator $d \neq 1$ and $d\omega_i \in \mathbb{Z}[\alpha]$. Also $\gcd(p, d) = 1$ so there exist integers x, y such that $yd = 1 - xp$. Multiplying both sides with ω_i gives us $yd\omega_i = \omega_i - xp\omega_i$. But in the ring $\mathcal{O}_K/(p)$ the element $xp\omega_i = 0$, so we see that $\omega_i \equiv yd\omega_i \mod (p)$. Thus every element in $\mathcal{O}_K/(p)$ is also represented in $\mathbb{Z}[\alpha]/(p)$. Because we already knew that $\mathbb{Z}[\alpha] \subset \mathcal{O}_K$ this is enough to show that $\mathbb{Z}[\alpha]/(p) = \mathcal{O}_K/(p)$. □

Theorem 5.3. *Let* α *be some algebraic number with minimal polynomial* $f(X)$ *and let* p *a prime number. Assume that* $f(X) \equiv g(X)h(X) \mod p$, *then,*

$$\mathbb{Z}[\alpha]/(p, g(\alpha)) = \mathbb{Z}[X]/(p, g(X)).$$

Proof. The only difference between $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[X]$ is that the first has the extra relation $f(\alpha) = 0$ but the second does not have the relation $f(X) = 0$. Thus $\mathbb{Z}[\alpha]$ is equivalent to $\mathbb{Z}[X]/(f(X))$. However $f(X) \equiv g(X)h(X) \mod p$, which shows that $(f(X))$ is divided by the ideal $(p, g(X))$. Now we can easily see that,

$$\mathbb{Z}[X]/(p, g(X)) = (\mathbb{Z}[X]/(f(X)))/(p, g(X)) = \mathbb{Z}[\alpha]/(p, g(\alpha)).$$

□

Theorem 5.4. *Let* $g(X)$ *be some irreducible polynomial in* $R[X]$ *where* R *is a field. Then* (g) *is a maximal ideal in* $R[X]$.

Proof. We will prove this by first showing that $R[X]$ is a principal ideal domain and then that (g) cannot be contained in some other ideal (f) if $g(X)$ is irreducible.
To prove that $R[X]$ is a PID we take an arbitrary ideal I of $R[X]$. Let $g(X)$ be the polynomial in I of smallest degree, then obviously the ideal (g) is contained in I. Now take any $f(X)$ that is an element of I. Using the algorithm of Euclides we find $f(X) = h(X)g(X)+r(X)$ for some $h(X), r(X) \in R[X]$ with $\deg(r(X)) < \deg(g(X))$. (Also see the proof of Lemma 4.10.) However, this implies that $r(X) = f(X) - h(X)g(X)$ must also be in I, but we assumed

$g(X)$ to be the polynomial of lowest degree. The only possibility is that $r(X) = 0$ and thus $f(X) \in (g)$. This shows that for every ideal I of $R[X]$ we can find some $g(X)$ such that $(g) \subset I \subset (g)$ and thus that I is generated by the single element $g(X)$. We may conclude that $R[X]$ is a PID.
Now let $g(X)$ be some irreducible element of $R[X]$. If (g) is not maximal there exists some $f(X) \in R[X]$ such that $(g) \subset (f)$. This also implies that we can write $g(X)$ as $f(X)h(X)$ for some $h(X) \in R[X]$. This is in contradiction with the fact that $g(X)$ is irreducible and thus we see that (g) is a maximal ideal. □

To be able to say something about which ideals divide the product defined in the criterion we need the following theorem.

Theorem 5.5. *Let $m \in \mathbb{Z}$ and $f_1(X), \ldots, f_s(X) \in \mathbb{Z}[X]$ and $\alpha \in \overline{\mathbb{Q}}$, then in $\mathbb{Z}[X]$ we have,*

$$\prod_{i=1}^{s}(m, f_i(\alpha)) \subset (m, \prod_{i=1}^{s} f_i(\alpha)).$$

Proof. We will prove this by induction to $s \in \mathbb{N}$.
In the case that $s = 1$, we do not have to take any product and thus the two ideals are equal. So it is clear that the claim is true for $s = 1$.
Now assume that we know the claim to be true for a certain $s = k$ with $k \in \mathbb{N}$. We will prove that the claim is also true for $s = k + 1$.
First of all, note that, by our assumption,

$$\prod_{i=1}^{k+1}(m, f_i(\alpha)) = (m, f_{k+1}(\alpha)) \prod_{i=1}^{k}(m, f_i(\alpha)) \subset (m, f_{k+1}(\alpha))(m, \prod_{i=1}^{k} f_i(\alpha)).$$

Note that we can write $\prod_{i=1}^{k} f_i(X) = g(X)$ for some $g(X) \in \mathbb{Z}[X]$. Thus we are left to prove that $(m, f_{k+1}(\alpha))(m, g(\alpha))$ is contained in $(m, f_{k+1}(\alpha)g(\alpha))$.
Take $h(X)$ to be some arbitrary element in $(m, f_{k+1}(X))(m, g(X))$. Then we can write $h(\alpha)$ as,

$$h(\alpha) = \sum_{i=1}^{n}(ma_{1,i}(\alpha) + f_{k+1}(\alpha)a_{2,i}(\alpha))(mb_{1,i}(\alpha) + g(\alpha)b_{2,i}(\alpha)),$$

where $a_{1,i}, a_{2,i}, b_{1,i}, b_{2,i}$ are polynomials in $\mathbb{Z}[X]$ and n is some natural number. Thus,

$$h = \sum_{i=1}^{n} m^2 a_{1,i}b_{1,i} + ma_{1,i}b_{2,i}g + ma_{2,i}b_{1,i}f_{k+1} + a_{2,i}b_{2i}f_{k+1}g.$$

It can now be seen that $h(\alpha) \in (m, f_{k+1}(\alpha)g(\alpha))$. Because $h(X)$ was arbitrary this shows that indeed,

$$\prod_{i=1}^{k+1}(m, f_i(\alpha)) \subset (m, \prod_{i=1}^{k+1} f_i(\alpha)),$$

and by the principle of induction we now know the claim to be true for all $s \in \mathbb{N}$, as wished. □

For the last step in the proof, where we want to show that the indices are equal, we need to be able to calculate these indices. To do this we use three theorems of which we will not prove the first one. A proof can be found in [7].

Theorem 5.6. *Let I and J be two ideals in $\mathcal{O}_K$, then $N(IJ) = N(I)N(J)$.*

Theorem 5.7. *Let $K = \mathbb{Q}(\alpha)$ with α some algebraic number with degree n. Then the norm or index of (p) in $\mathcal{O}_K$ is p^n, where p is some prime in $\mathbb{N}$.*

Proof. Recall that the index of an ideal I is the cardinality of the set $\mathcal{O}_K/I$. Now let $\{\omega_1, \ldots, \omega_n\}$ be some basis of integers of $\mathcal{O}_K$. We can then write each element of $\mathcal{O}_K$ as $\sum_{i=1}^n m_i\omega_i$ and each element of (p) as $\sum_{i=1}^n pm_i\omega_i$, where all $m_i \in \mathbb{Z}$. Now take two elements $x, y \in \mathcal{O}_K$ and write $x = \sum_{i=1}^n m_i\omega_i$ and $y = \sum_{i=1}^n k_i\omega_i$. Then it is obvious that $x \equiv y \mod (p)$ if and only if p divides $m_i - k_i$ for all $1 \leq i \leq n$. Thus, x and y are equivalent if and only if $m_i \equiv k_i$ modulo p. So for all $1 \leq i \leq n$ we have p choices for m_i if we want x to be a unique element in $\mathcal{O}_K/(p)$. This gives a total of p^n choices and thus the index of (p) in $\mathcal{O}_K$ is p^n. □

Theorem 5.8. *For α, $g_i(X)$ and p as in Dedekind's criterion, the cardinality of $\mathbb{Z}[\alpha]/(p, g_i(\alpha))$ equals $p^{\deg(g_i)}$.*

Proof. We know that $\mathbb{Z}[\alpha]$ can be written as $\{m_1 + m_2\alpha + \ldots + m_n\alpha^{n-1} \mid m_i \in \mathbb{Z}\}$. By dividing $\mathbb{Z}[\alpha]$ by the ideal $(g_i(\alpha))$ we get the extra relation that $g_i(\alpha) = 0$. Thus we see that $\alpha^{\deg(g_i)}$ is no longer independent of the α^j with $0 \leq j < \deg(g_i)$. However, because $g_i(x)$ is irreducible all α^j for j smaller than $\deg(g_i)$, wíll stay independent of each other. This leaves us with exactly $\deg(g_i)$ independent powers of α. Now analogue to the proof of Theorem 5.7 we easily find that $|\mathbb{Z}[\alpha]/(p, g_i(\alpha))| = p^{\deg(g_i)}$. □

Now we have all the setup we need and we can give the proof.

Theorem 5.1 (Dedekind's criterion)**.** *Let p be a prime in $\mathbb{Z}$ and $\alpha \in \mathcal{O}_K$ such that $K = \mathbb{Q}(\alpha)$ and p does not divide the index of α. Let $g(X)$ be the minimal polynomial of α and let $g(X) \equiv g_1(X)^{e_1} \ldots g_r(X)^{e_r} \mod p$ be its factorisation into distinct irreducible factors $g_i(X)$ modulo p. Then the ideals $\wp_i = (p, g_i(\alpha))$ are prime ideals and we have $(p) = \wp_1^{e_1} \ldots \wp_r^{e_r}$.*

Proof of Dedekind's Criterion. From Theorem 5.2 we find that $\mathcal{O}_K/(p) = \mathbb{Z}[\alpha]/(p)$ and because $(p) \subset (p, g_i(\alpha)) = \wp_i$ this also implies that $\mathcal{O}_K/\wp_i = \mathbb{Z}[\alpha]/\wp_i = \mathbb{Z}[X]/(p, g_i(X))$. Here the last equality follows from Theorem 5.3. In Theorem 5.4 we saw that $(g_i(X))$ was maximal in $\mathbb{Z}_p[X]$ which means that $\mathbb{Z}[X]/(p, g_i(X))$ is a field. Thus $\mathcal{O}_K/\wp_i$ is also a field, and $\wp_i$ is maximal. We know that every maximal ideal is also prime ideal, so we have now proved that $\wp_i$ is prime for all $1 \leq i \leq r$.
To show that $(p) = \wp_1^{e_1} \cdots \wp_r^{e_r}$ we use Theorem 5.5 to show that the product of prime ideals

is contained in (p) and then compare their indices.
By taking $m = p, s = e_i$ and $f_1(X) = \ldots = f_{e_i}(X) = g_i(X)$ for all $1 \leq i \leq r$ in Theorem 5.5, we find that $\wp_i^{e_i} \subset (p, g_i(\alpha)^{e_i})$. Similar taking $m = p, s = r$ and $f_i(X) = g_i(X)^{e_i}$ for all $1 \leq i \leq r$ we get:

$$\prod_{i=1}^{r} \wp_i^{e_i} \subset \prod_{i=1}^{r} (p, g_i(\alpha)^{e_i}) \subset (p, g(\alpha)) = (p).$$

Where the last step follows from the fact that $g(\alpha) = 0$. Hence, we have found that $\wp_1^{e_1} \cdots \wp_r^{e_r} \subset (p)$.
From Theorem 5.7 we know that the index of (p) is p^n. From Theorem 5.8 and the fact that $\mathcal{O}_K/\wp_i = \mathbb{Z}[\alpha]/\wp_i$ we find that the index of each $\wp_i$ is $p^{\deg(g_i)}$. Now using Theorem 5.6 this implies that $N(\wp_1^{e_1} \cdots \wp_r^{e_r}) = \prod_{i=1}^{r} p^{e_i \deg(g_i)}$ which is easily seen to be $p^{\deg(g)} = p^n$. One can also check that two ideals are equal if and only if one divides the other and their indices are equal. We conclude that $(p) = \wp_1^{e_1} \cdots \wp_r^{e_r}$. □

5.2 Applications

The reason that Dedekind's criterion is relevant in the polynomial Szemerédi Theorem is because it says something about how a monic primitive polynomial $g(X)$ factors modulo p. The factorisation of a polynomial modulo p gives us again information about the existence of roots modulo p. Thus Dedekind's criterion gives us a way to express an algebraic condition to check if some prime meets the requirements of Theorem 3.1.
Before we will state this condition explicitely it is important to remark something about general integers that meet the requirements of Theorem 3.1. Since Dedekind's criterion is about primes it will not be possible to directly get a condition for all square-free $m \in \mathbb{Z}$. This is, however, relevant as the following example shows.

Examples.

- The polynomial $15x^5 + x^4$ can use $m = 3$, $m = 5$ and $m = 3 \cdot 5 = 15$. This gives us respectively $R_3 = \{0\}$, $R_5 = \{0, 2\}$ and $R_{15} = \{0, 3, 7, 11\}$ and thus $\gamma_3 = 0.8$, $\gamma_5 = 0.88613\ldots$ and $\gamma_{15} = 0.90238\ldots$. Note that all these sets R_m are maximal, so it is possible to find a bigger γ for a composite number than for its prime divisors.

In the next theorem it is stated that it is sufficient to know for all primes whether they meet the conditions of Theorem 3.1 to know for all m whether they meet the requirements of Theorem 3.1.

Theorem 5.9. *Let $f = \sum_{i=k}^{d} a_i X^i \in \mathbb{Z}[X]$. Let m be a square-free integer, then m meets the requirements of Theorem 3.1 with regard to f if and only if for all primes p that divide m we know that p meets the requirements of Theorem 3.1 with regard to f.*

Proof. Because m is square-free we can write m as $p_1 \cdots p_n$ with all p_i for $1 \leq i \leq n$ different

primes. We first assume that all these p_i meet the requirements of Theorem 3.1. and prove that in this case so does m.
It is obvious that $\gcd(a_k, m)$ equals 1 because $\gcd(a_k, p_i) = 1$ for all i. Now assume there is some root x of f modulo m, then x must also be a root of f modulo p_i for all $0 \leq i \leq n$. By our assumption this means that $x \equiv 0 \mod p_i$ for all i. We can now use the Chinese remainder theorem to see that x is also equivalent to 0 modulo m and thus m meets the requirements as wished.
Secondly we assume that m meets the requirements and we will prove that all p_i do as well. Again it is obvious that if $\gcd(a_k, m) = 1$ then $\gcd(a_k, p_i) = 1$ for all i. Now suppose there is some $1 \leq j \leq n$ and integer $a \not\equiv 0 \mod p_j$ such that $f(a)$ modulo p_j is equivalent to 0. Then all integers that are equivalent to a modulo p_j are also roots of f modulo p_j. Besides, we know that for all i and $x \equiv 0 \mod p_i$, x is a root of f modulo p_i. Thus any integer x that is $0 \mod p_i$ for all $i \neq j$ and $a \mod p_j$ has that $f(x) \equiv 0 \mod p_i$ for all $1 \leq i \leq n$ (including $i = j$). In particular we then know that $f(x) \equiv 0 \mod m$. However, from the Chinese remainder theorem we know that $x \not\equiv 0 \mod m$ which contradicts our assumption. We conclude that such a j cannot exist and thus that all p_i must meet the requirements of Theorem 3.1. □

It is now clear that all we really want to know is if there exist primes p that meet the requirements of Theorem 3.1. The most important idea of the following theorem is that a polynomial does not have a root modulo p if it cannot be facotred into a linear polynomial modulo p.

Theorem 5.10. *Let $f(X)$ be equal to $X^k g(X)$ where $g(X)$ is the minimal polynomial of α and $k \geq 2$. Furthermore, let p be a prime number which does not divide the index of α. Then p meets the requirements of Theorem 3.1 if and only if $\gcd(a_k, p) = 1$ and (p) cannot be factored into any prime ideal $\wp$ with $N(\wp) = p$ in $\mathcal{O}_{\mathbb{Q}(\alpha)}$.*

Proof. First we assume that $\gcd(a_k, p) = 1$ and that (p) cannot be factored into any prime ideal $\wp$ with norm p. We show that then p must meet the requirements of Theorem 3.1.
It is clear that $f(X)$ can be written as $\sum_{i=k}^{d} a_i X^i$ with $a_d \neq 0$ and $k \geq 2$ as required by Theorem 3.1. Furthermore, we note that $g(X)$ cannot have any roots modulo p which are 0 mod p. Because if this were the case, that would mean that $g(0) = a_k$ is divisible by p. But we assumed that $\gcd(a_k, p) = 1$ so this cannot be true. Now we look at the factorisation of $g(X)$ modulo p. Dedekind's criterion tells us that $g(X) = g_1(X)^{e_1} \cdots g_r(X)^{e_r} \mod p$ where $g_i(X)$ are distinct irreducible factors modulo p. Also, we know that $(p) = (p, g_1(\alpha))^{e_1} \cdots (p, g_r(\alpha))^{e_r}$ where all $(p, g_i(\alpha))$ are prime ideals. For all prime ideals that divide (p) we assumed that their indices do not equal p. We know as well that $N((p, g_i(\alpha))) = p^{\deg(g_i)}$. So every g_i must have a degree of at least 2. However, if $g(X)$ would have a root a modulo p we would be able to write $g(X)$ modulo p as $(x - a)h(X)$ where $h(X) \in \mathbb{Z}[X]$. Thus, we conclude that $g(X)$ does not have a root modulo p and also f does not have any roots modulo p which are unequal to $0 \mod p$. Together with the fact that $\gcd(a_k, p) = 1$ this is exactly what is required for p to meet the requirements of Theorem 3.1, as wished.

Now we prove that if p meets the requirements of Theorem 3.1 then (p) cannot be factored by a prime ideal with index p.
This follows almost directly from Dedekind's criterion and the fact that every ideal can be uniquely factored into its prime ideals. First we note that with Dedekind's criterion we find the unique factorisation of (p). Let us assume that this factorisation does contain some prime ideal $\wp$ with index p. Then we know that this prime ideal can also be written as $(p, g_i(\alpha))$ where g_i is an irreducible factor modulo p of $g(X)$. Because the index of $\wp$ is p we also know that g_i has degree 1. But this means that g_i can be written as $X - a$ for some $a \in \mathbb{Z}_p$. And thus that $g_i(a) \equiv 0 \mod p$ which gives that $g(a) \equiv 0 \mod p$. The only possibility left for p to meet the requirements of Theorem 3.1 is if a is equivalent to 0 modulo p. However, we also know that $\gcd(a_k, p) = 1$ because p meets the requirements. So, by the same proof as in the first part we know that $g(X)$ cannot have any roots modulo p which are $0 \mod p$. This clearly leads to a contradiction. We conclude that $\wp$ cannot have index p and thus that (p) cannot be factored into any prime ideal with index p. □

We have now stated and proved an algebraic condition for prime numbers to meet the requirements of Theorem 3.1 with regard to some polyomials f. It is important to realise that we have not proved this condition for all f that we are interested in. This is because not all such polynomials can be written as a product of X^k and a minimal polynomial. For instance, if $f(X) = X^2(X^2+1)^2 = X^2(X^4+2X^2+1) = X^6+2X^4+X^2$ it is obvious that X^4+2X^2+1 is not a minimal polynomial. Thus, we also want to look at what happens if f is a product of several minimal polynomials and X^k.
Fortunately for us we can generalise Theorem 5.10 to these cases. However, we still have to demand that $f(X)$ is monic.

Theorem 5.11. *Let $f(X)$ be equal to $X^k g_1(X) \cdots g_n(X)$ where $g_i(X)$ are minimal polynomials of α_i for all $1 \leq i \leq n$ and $k \geq 2$. Furthermore, let p be a prime number which does not divide the index of α_i for any $1 \leq i \leq n$. Then p meets the requirements of Theorem 3.1 if and only if $\gcd(a_k, p) = 1$ and (p) cannot be factored into any prime ideal $\wp$ with $N(\wp) = p$ in $\mathcal{O}_{\mathbb{Q}(\alpha_i)}$ for all $1 \leq i \leq n$.*

Proof. This theorem will be proved using induction to n.
It should be obvious that Theorem 5.10 exactly states the theorem for the case $n = 1$, so we do not need to prove that anymore.
Now, suppose that the statement is known for a certain $n = r$. We will prove this implies that the statement is also true for $n = r + 1$.
Let $f(X)$ be some polynomial that can be written as $X^k g_1(X) \cdots g_{r+1}(X)$ with all g_i minimal polynomials for certain α_i and $k \geq 2$. Furthermore, assume p to be some prime that does not divide the indices of α_i for $1 \leq i \leq r+1$. We will prove that p meets the requirements of Theorem 3.1 if and only if $\gcd(a_k, p) = 1$ and (p) cannot be factored into any prime ideal $\wp$ with $N(\wp) = p$ in any $\mathcal{O}_{\mathbb{Q}(\alpha_i)}$
If we consider the polynomials $a(X) = X^k g_1(X) \cdots g_r(X)$ and $b(X) = X^k g_{r+1}(X)$ we can see by our induction hypothesis that the if-and-only-if-statement holds for p with regard to

a and b. Furthermore, note that a_k of f is the product of the last coefficient of a and the last coefficient of b. So $\gcd(a_k, p) = 1$ if and only if the greatest common divisor of the last coefficients of a and p equals 1 and the greatest common divisor of the last coefficient of b and p equals 1. We will call this our 'gcd-argument'.
Now, assume that p meets the requirements of 3.1 with regard to f. Then there are no $x \not\equiv 0$ modulo p such that $f(x)/x^k$ is 0 modulo p. Because $a(X)/X^k$ and $b(X)/X^k$ both divide $f(X)/X^k$ this also implies that there are no such x such that $a(x)/x^k$ or $b(x)/x^k$ are 0 modulo p. Together with the gcd-argument this shows that p meets the requirements of 3.1 for a and b. Thus, we see that for all $1 \leq i \leq r+1$ we have that in $\mathcal{O}_{\mathbb{Q}(\alpha_i)}$ we cannot factor (p) with a prime ideal with index p.
To prove the other side we assume that (p) cannot be factored into a prime ideal $\wp$ with index p in $\mathcal{O}_{\mathbb{Q}(\alpha_i)}$ for all $1 \leq i \leq r+1$ and that $\gcd(a_k, p) = 1$. Because a and b consist of the same primitive polynomials as f they also rely on the same α_i. Using our induction hypothesis and gcd-argument we see that this implies that p meets the requirements of Theorem 3.1 with regard to a and b. Thus, there are no $x \not\equiv 0$ modulo p such that either $a(x)/x^k$ or $b(x)/x^k$ is 0 modulo p. Now, because p is prime and $f(X)/X^k = a(X)/X^k \cdot b(X)/X^k$ this also implies that there are no such x such that $f(x)/x^k$ is 0 modulo p. We may conclude that p also meets the requirements of Theorem 3.1 with regard to f.
By induction it should now be clear that for all $n \in \mathbb{N}$ the statement of the theorem holds and we are done. □

Now that we have found a condition for such a large class of polynomials, a logical follow-up question is if this condition is ever met. Nicely enough we can answer this question positively, by using Chebotarev's denisty Theorem. This theorem estimates the density of primes p such that (p) factors in a ceratain way in Galois extensions. So, it also says something about when a polynomial (p) can be factored in a prime ideal $\wp$ with index p. In particular, this leads to the following application of Chebotarev's density Theorem.

Theorem 5.12. *Let $g(X)$ be the minimal polynomial of some $\alpha \in \overline{\mathbb{Q}}$ with degree $n \geq 2$, and let $P(g)$ be the set of primes such that all $p \in P(g)$ meet the requirements of Theorem 3.1. Then the density $d(P(g))$ is greater or equal to $\frac{1}{n}$.*

Theorem 5.13. *Let n and a be two integers such that $\gcd(n, a) = 1$ and let P be the set of primes p such that $p \equiv a \mod n$. Then the density $d(P)$ equals $\frac{1}{\phi(n)}$.*

Proves of these theorems can be found in [22].
From Theorem 5.12 it directly follows that there must be infinitely many and arbritray big primes p that meet the requirements of Theorem 3.1. From Theorem 5.13 it similary follows that there are infinitely many primes such that $p \equiv a \mod n$. More fore it is even true that in the case that the Galois extensions of these two cases only intersect in $\mathbb{Q}$, there are infinitely many primes that meet both conditions.

5.3 Finding R

In the previous section we proved that there exist square-free m that meet the requirements of Theorem 3.1. But Theorem 3.1 becomes more useful if we can find an m such that $\log_m |R| > 0$. This is the case when R contains at least 2 elements. In this section we prove the main result of this thesis, namely, that for certain polynomials f we can always find a set R with cardinality at least 2.

Theorem 5.14. *Let $f = \sum_{i=k}^{d} a_i X^i \in \mathbb{Z}[X]$ such that $k \geq 2$, $a_d \neq 0$ and $f = X^k g(X)$ where $g(X)$ is the minimal polynomial for some $\alpha \in \overline{\mathbb{Q}}$. Furthermore let E be the Galois extension of $\mathbb{Q}[X]/g(X)$ and assume that $\mathbb{Q}(\zeta_k) \cap E = \mathbb{Q}$ where ζ_k is a kth root of unity if k is odd and $\zeta_k = i$ if k is even. Then there exists a prime p such that for all $N \in \mathbb{N}$ the number $\alpha(f, N) \gg_{p,f} N^{\gamma}$ with:*

$$\gamma = \frac{d - 1 + \log_p |R|}{d}$$

such that $|R| \geq 2$.

Proof. From Section 5.2 we already know that there exist arbitrary large p that meet the requirements of Theorem 3.1. We are left to show that we can even find a p such that $|R| \geq 2$.
We will prove this separately for k is odd and k is even. First we assume that k is odd.
Because the intersection of $\mathbb{Q}(\zeta_k)$ and E equals $\mathbb{Q}$ we know that the density of the set of primes p such that p meets the requirements of Theorem 3.1 and p is equivalent to 1 modulo k is positive. This implies that there are infinitely many p with both these properties, and we can choose one. For this p we know that k divides $p - 1$ and thus, by Fermat, that the set $C := \{a^k \mid a \in \{0, 1, \ldots p - 1\}\}$ cannot equal all the residual classes of p. Now, because k is odd, we also know that $(-1)^k \equiv -1 \mod p$. Let $b \in C$, then there exists an a such that $a^k \equiv b \mod k$, thus $(-a)^k \equiv (-1)(a)^k \equiv -b \mod k$ and $-b \in C$. Because C does not equal all the residual classes of p and b in C implies that $-b$ is in C, there must also be a pair b and $-b$ that are both not in C. For this b we may take $R = \{0, b\}$ and it is easy to check that $(R - R) \cap C = \{0\}$, as wished. Hence, we have found a set R with $|R| = 2$. Now using Theorem 3.1 itself we find that $\gamma \geq \frac{d-1+\log_p(2)}{d}$ which is strictly larger than $\frac{d-1}{d}$.
Next, we assume that k is even and thus that $\zeta_k = i$.
Similar to the odd case we have that the intersection of $\mathbb{Q}(i)$ and E equals $\mathbb{Q}$ and thus, that there are infinitely many primes p such that $p \equiv 1 \mod 4$ and p meets the requirements of Theorem 3.1. If we choose such a p we know that p must have -1 as a quadratic residue. We will show that this means that either there is an $a \in \{0, 1, \ldots, p - 1\}$ such that $a^k \equiv -1 \mod p$ or that there are three distinct a such that $a^k \equiv 1 \mod p$.
It is obvious that $\frac{k}{2}$ is an integer because k is even. Let a be in the residual class of p such that $a^2 \equiv -1 \mod p$. If $\frac{k}{2}$ is odd we have that $a^k \equiv (-1)^{\frac{k}{2}} = -1 \mod p$. If $\frac{k}{2}$ is even we have that $a^k \equiv (-1)^{\frac{k}{2}} = 1 \mod p$. Because we also know that $a \neq 1, -1$ from the fact that $a^2 \not\equiv 1 \mod p$ we see that for even $\frac{k}{2}$ all three residual classes $1, a$ and -1 have a kth power

that is 1 modulo p.
Now because k is even we also know that $a^k \equiv (p-a)^k \mod p$. So we have at most $\frac{p+1}{2}$ different k-th powers modulo p. Assume now, that there does not exist a suitable set R with $R = \{0, b\}$. This implies that for all $b \in \{0, 1, \ldots, p-1\}$ either b or $-b$ equals a kth power modulo p. Including 0 there are exactly $\frac{p+1}{2}$ pairs b and $-b$, thus we can only have that all b or $-b$ can be written as a k-th power if there is is exactly one pair $(a, -a)$ such that $a^k \equiv \pm b$ for each b. However, we have just shown that $1, a$ and -1 all have a k-th power that is equivalent to either -1 or 1. This implies that there must also be a b such that no k-th power is equivalent to b or $-b$ modulo p. We may conclude that for this b the set $R = \{0, b\}$ is suitable and thus that we can find a set R with at least two elements. Using Theorem 3.1 again we find $\gamma = \frac{d-1+\log_p(2)}{d} > \frac{d-1}{d}$. □

It is again important to realise that the previous theorem does not apply for all f in which we are interested. Specifically we ask f to be a monic polynomial that is the product of X^k and some minimal polynomial $g(X)$. It would be interesting to see if it would be possible to extend Theorem 5.14 using Theorem 5.11.

Chapter 6

Further Research

While working on my thesis I encountered a lot of interesting ideas and questions about lower bounds in the polynomial Szemerédi theorem. In this chapter I would like to mention some of them. In some cases these ideas are extensions of the ones I did treat in the previous chapters. In other cases they stand on their own and take a completely different direction.

6.1 Different Domains

In Section 3.2 I proved a theorem about the lower bound for $\alpha(f, N)$ if the domain of f was $n\mathbb{Z}$ instead of $\mathbb{Z}$. It would also be interesting to look at bounds for $\alpha(f, N)$ if the domain of f were some other subset of $\mathbb{Z}$. For instance if we take the natural numbers as domain, the (absolute) image of $f(x) = x^3$ stays the same but the image of $f(x) = x^3 + x^2$ does not. Does this affect how $\alpha(f, N)$ grows?
In a similar way one could limit the domain to the prime numbers or any arbitrary subset S of $\mathbb{Z}$. One nice aspect is that an upper bound of $\alpha(f, N)$ with domain S is always the value that $\alpha(f, N)$ would take if $S = \mathbb{Z}$.

6.2 Linear polynomials

Theorem 3.1 requires that $k \geq 2$. It would be nice to look if we can find some estimates for γ if $k = 1$ or $k = 0$.
One interesting polynomial for $k = 1$ is $X^2 + X$. The image of $X^2 + X$ consists solely of even numbers. Thus, the odd integers and the even integers in $A_{X^2+X}[N]$ do not interact. Furthermore for $z \leq 30$ I calculated that there are twice as many solutions to $f(x) + f(y) = f(z)$ where $x, y, z \in \mathbb{Z}$ if $f(X) = X^2 + X$ than if $f(X) = X^2$. Whenever $f(x) + f(y) = f(z)$ we have for each $a \in \mathbb{N}$ the triplet $(a, a + f(x), a + f(x) + f(y))$ such that at most one of

these can be in $A_f[N]$, whereas usually there is only a pair $(a, a + f(x))$ where we have to choose from. Thus, one might suspect that if the number of solutions of $f(x) + f(y) = f(z)$ is bigger that the value of $\alpha_f[N]$ is smaller.

6.3 Better lower bounds

In Theorem 5.14 we found that there exist square-free integers m such that $|R| \geq 2$. However, it is still unclear how big these integers have to be. To get a strict lower bound for $\alpha(f, N)$, it is necessary to give an upper bound for the first p such that $|R| \geq 2$. This would require a quantative version of Chebotarev's density Theorem.
Another way to improve the lower bound would be to find bigger sets R. In [17], Ruzsa proved that for $f(X) = X^k$ one can find a set R with $|R| \geq k$ if m equals the smallest prime that is equivalent to 1 modulo $2k$. I think his techniques might also work in our case, if tweaked a little.
It has also been mentioned a couple of times that Theorem 5.14 is only for one class of polynomials. For all non-monic polynomials we still have to find any m at all. For polynomials that contain a product of minimal polynomials we do know that there exist m, but do not have a estimation of $|R|$ yet.

6.4 Multiple polynomials

In Chapter 2 we learned that the polynomial Szemerédi Theorem is a much more general theorem than the cases that I have discussed. For instance, we have seen that Younis himself found lower bounds for two other cases in Theorems 3.2 and 3.3. Perhaps it is also possible to use algebraic number theory to find more explicit bounds in these cases, or even more general cases where we also consider some $f_3, \ldots, f_k$.

Bibliography

[1] A. Balog, J. Pelikán, J. Pintz and E. Szemerédi, *Difference sets without k-th powers*, Acta. Math. Hung. **65 (2)** (1994), 165–187.

[2] R. Beigel and W. Gasarch, *Square-difference-free sets of size* $\Omega(n^{0.7334\ldots})$, Preprint, arXiv:0804.4892, 2008.

[3] V. Bergelson and A. Leibman, *Polynomial extensions of van der Waerden's and Szemerédi's Theorems*, J. Amer. Math. Soc. **9** (1996), no. 3, 725–753.

[4] F. Beukers, *Algebraic Number Theory, a crash course*, Leiden, 2011.

[5] F. Beukers, *Rings and Galois Theory*, Department of Mathematics UU, Utrecht, 2018.

[6] T. F. Bloom, *A quantitative improvement for Roth's theorem on arithmetic progressions*, J. London Math. Soc. **93** (2016), 643–663.

[7] K. Conrad, *Ideal Factorisation*, UCONN, `https://kconrad.math.uconn.edu/blurbs/gradnumthy/idealfactor.pdf`. Consulted in December 2019.

[8] H. Furstenberg, *Ergodic behaviour of diagonal measures and a theorem of Szemerédi on arithmetic progressions*, J. Analyse Math. **31** (1977), 204–256.

[9] T. Gowers, *A new proof of Szemerédi's Theorem*, Geom. Func. Anal. **11** (2001), 465–588.

[10] B. Green and T. Tao, *New bounds for Szemerédi's theorem, III: A polylogarithmic bound for* $r_4(N)$, Preprint, arXiv:1705.01703, 2017.

[11] T. Kamae and M. Mendès France, *Van der corput's difference Theorem*, Israel J. Math. **31** (1978), no. 3-4, 335–342.

[12] M. Lewko, *An improved lower bound related to the Furstenberg-Sárközy Theorem*, Electro. J. Comb. **22** (2015), no. 1, 32.

[13] K. O'Bryant, *Sets of integers that do not contain long arithmetic progressions*, The Electronic J. Combinatorics **18** (2011), 59.

[14] J. Pintz, W. L. Steiger, E. Szemerédi, *On sets of natural numbers whose difference set contains no squares*, J. London Math. Soc. **37** (1988), no. 2, 219–231.

[15] A. Rice, *A maximal extension of the best-known bounds for the Furstenberg-Sárközy theorem*, Acta Arith. **187** (2019), no. 1, 1–41.

[16] K. F. Roth, *On certain sets of integers*, J. London Math. Soc. **28** (1953),245–252.

[17] I. Z. Ruzsa, *Difference sets without squares*, Period. Math. Hung. **15** (1984), no.3, 205–209.

[18] P. Stevenhagen, *Number Rings*, Universiteit Leiden, 2017.

[19] E. Szemerédi, *On sets of integers containing no k elements in arithmetic progression*, Acta Arith. **27** (1975), 299–345.

[20] T. Tao and T. Ziegler, *The primes contain arbitrarily long arithmetic progressions*, Annals of Math. **167** (2008), 481–547.

[21] V. Taranchuk, *A constructive lower bound on Szemerédi's Theorem*, Preprint, arXiv:1711.04183v2, 2017.

[22] N. G. Triantafillou, *Chebotarev's Density Theorem*, MIT, (2016).

[23] K. Younis, *Lower bounds in the polynomial Szemerédi Theorem*, Preprint, arXiv:1908.06058v1, 2019.