university of groningen / faculty of science and engineering / mathematics and applied mathematics

BACHELOR PROJECT

Proving special cases of Fermat's last theorem by using the classical approach of inspecting the ring $\mathbb{Z}[e^{\frac{2\pi i}{p}}]$ for primes p

Dylan de Jonge

Student Number: S5334349

June 27, 2025

First supervisor: prof. dr. J. Top

Second supervisor: dr. E. Özman

Contents

1 Introduction **3**

1.1 The case $n = 4$ using number theory 3

2 Important notions from ring theory and field theory **6**

3 The ring $\mathbb{Z}[\zeta_3]$ **13**

3.1 The units of $\mathbb{Z}[\zeta_3]$ 13

3.2 Unique factorization in $\mathbb{Z}[\zeta_3]$ 14

4 Proving Fermat's last theorem for $n = 3$ **17**

5 The ring $\mathbb{Z}[\zeta_4]$ **24**

5.1 The units of $\mathbb{Z}[\zeta_4]$ 24

5.2 Unique factorization in $\mathbb{Z}[\zeta_4]$ 25

6 Proving Fermat's last theorem for $n = 4$ **28**

7 The ring $\mathbb{Z}[\zeta_5]$ **34**

7.1 The units of $\mathbb{Z}[\zeta_5]$ 34

7.1.1 A useful map 35

7.1.2 The structure of the units 46

7.2 Unique factorization in $\mathbb{Z}[\zeta_5]$. 52

8 Proving Fermat's last theorem for $n = 5$ **58**

9 The ring $\mathbb{Z}[\zeta_n]$ and Fermat for general primes n **65**

9.1 The units of $\mathbb{Z}[\zeta_n]$ 65

9.2 The first case of Fermat's last theorem 74

9.3 Notable results 81

10 Conclusion **82**

11 Afterword **82**

Abstract

In this project we investigate the ring $\mathbb{Z}[\zeta_n]$ for certain small values of n. We determine the unit groups and show these rings take on unique factorization. These results allow us to prove Fermat's last theorem for these specific values of n. We also briefly discuss some key results for $\mathbb{Z}[\zeta_n]$ where n is any prime number and use those for the first case of Fermat's last theorem for suitable n.

1 Introduction

The goal of this project is to determine some properties about the ring $\mathbb{Z}[\zeta_n]$, where $\zeta_n = e^{\frac{2\pi i}{n}}$ is the n-th root of unity, and use those properties to prove that the equation $x^n + y^n = z^n$ has no solutions over the integers as long as $xyz \neq 0$. Such solutions are referred to as nontrivial solutions. This results is known as Fermat's last theorem. We start of by recalling and stating important results from ring theory and field theory. These prerequisites might be familiar to some however they are discussed to refresh them precisely so that the reader is put on point.

After this we investigate the ring $\mathbb{Z}[\zeta_n]$ for $n = 3, 4$ and 5 by determining the units in each ring and showing that these rings are Euclidean domains. These are very strong results and it is not something that can be done for $\mathbb{Z}[\zeta_n]$ for general n. The results we did find are used to prove Fermat's last theorem in these cases using classical methods from ring theory.

Lastly we discuss similar results in the ring $\mathbb{Z}[\zeta_n]$ where n is any prime greater than two and also discuss Fermat's last theorem for particular values of n. If one has a solution (a, b, c) of nontrivial integers to the equation $x^n + y^n = z^n$ and d is any divisor of n, one also has a solution to $x^{\frac{n}{d}} + y^{\frac{n}{d}} = z^{\frac{n}{d}}$ given by the triple (a^d, b^d, c^d). Therefore we restrict ourselves to prime numbers n, since showing no nontrivial solutions exist to $x^n + y^n = z^n$ means that there are also no solutions to $x^{kn} + y^{kn} = z^{kn}$ for any $k \in \mathbb{N}$. The only exception to restricting ourselves to prime exponents is when we take the exponent to be equal to 4 as it's only prime divisor is equal to 2 and there exist infinitely many nontrivial solutions to the equation $x^2 + y^2 = z^2$.

The main idea which we are aiming for is that for odd primes n, we can apply the factorization

$$x^n + y^n = (x + y)(x + (\zeta_n)y)(x + (\zeta_n)^2 y) \cdots (x + (\zeta_n)^{n-1} y) = z^n.$$

Up to certain units and irreducible elements, each term of the product is relatively prime with respect to another term of the product. In the case of unique factorization this allows us to give a nice form of each $x + (\zeta_n)^k y$ term from which we are able to show that there are no nontrivial solutions to the equation $x^n + y^n = z^n$.

1.1 The case $n = 4$ using number theory

We start of with a rather classical proof for Fermat's last theorem in the case $n = 4$ that relies solely on number theory strategies. We aim to show that the equation $x^4 + y^4 = z^4$ has no nontrivial solutions over the integers. First we would like to say something about the structure of solutions to the equation $x^2 + y^2 = z^2$ as this helps us with proving our desired result.

Definition 1.1 *A triple of three positive integers* (x, y, z) *satisfying* $x^2 + y^2 = z^2$ *is called a Pythagorean triple*

Definition 1.2 *A Pythagorean triple* (x, y, z) *is called a primitive Pythagorean triple if* x*,* y *and* z *have no common factor.*

Lemma 1.1 *If* (x, y, z) *is a primitive Pythagorean triple, then one of* x *and* y *is even while the other one is odd. In addition* z *is also odd*

Proof: Checking the equation $x^2 + y^2 = z^2$ modulo 4 yields the desired parity of x, y and z.

Q.E.D.

Now that the right terminology is established we continue to a classical results of describing all possible Pythagorean triples.

Theorem 1.1 (Primitive Pythagorean triples) *Let* (x, y, z) *be a primitive Pythagorean triple. Then there exist relatively prime positive integers* s *and* t*, one even and one odd, such that*

$$x = 2st, y = s^2 - t^2, z = s^2 + t^2$$

Proof: See Theorem 8.7 from [5]

Q.E.D.

Although a direct proof is not given, exercises leading up to this statement allows the reader to prove this result themselves. To now show that the equation $x^4 + y^4 = z^4$ has no nontrivial solutions, we actually prove a stronger result that the equation $x^4 + y^4 = z^2$ has no nontrivial solutions. Indeed if the triple (a, b, c) solves $x^4+y^4 = z^4$, then the triple (a, b, c^2) solves $x^4+y^4 = z^2$.

Theorem 1.2 *The equation* $x^4 + y^4 = z^2$ *has no nontrivial integer solutions.*

Proof: The proof relies on a method called infinite descent. How this works is by first assuming a certain solution with a property that is as small as possible exists. Then this solution is used to create a new solution where this property is smaller than in the solution given previously. This can be minimizing the sum of two terms or a number having a minimal divisor greater than 1. In this proof the minimal value of z is assumed. Suppose we find a triple of integers (x, y, z) such that $x^4 + y^4 = z^2$ and $xyz \neq 0$. This is indeed a nontrivial solution. By assumption of minimal z it means that no other triple (x^*, y^*, z^*) can exist where $z^* < z$. Because (x, y, z) satisfy $x^4+y^4 = z^2$, it follows that (x^2, y^2, z) is a Pythagorean triple. Since we could just divide by the common factors we can assume that without loss of generality it is a primitive Pythagorean triple. Also, without loss of generality let x be even and y, z be odd. This is allowed by Lemma 1.1.

From Theorem 1.1 we know that there exist positive coprime integers $a > b$ such that $x^2 = 2ab, y^2 = a^2 - b^2$ and $z = a^2 + b^2$. Observe the equation of y, rewriting yields $b^2 + y^2 = a^2$

which is again a Pythagorean triple. By choice of y being odd and a being on the right hand side of this equation, meaning it is also odd by Lemma 1.1, we find that b is even. Therefore we apply Theorem 1.1 again but now on the triple (b, y, a) to find that there exist positive coprime integers $p > q$ such that $b = 2pq, y = p^2 - q^2$ and $a = p^2 + q^2$. We choose this ordering as b is even. This is allowed since already a and b are coprime and since they form this relation with y, they are all coprime hence (b, y, a) is a primitive Pythagorean triple.

Notice then that $x^2 = 2ab = 4pq(p^2 + q^2)$ and since p and q are both coprime, so are p, q and $p^2 + q^2$. Therefore the numbers p, q and $p^2 + q^2$ are all perfect squares because their product is. Hence, since $p^2 + q^2$ is a perfect square, define $k^2 = p^2 + q^2$. Furthermore, since p and q are both also perfect squares, define $p = l^2$ and $q = m^2$. Combining these results then yields that

$$\begin{aligned} k^2 &= p^2 + q^2 \\ &= (l^2)^2 + (m^2)^2 \\ &= l^4 + m^4 \end{aligned}$$

So $k^2 = l^4 + m^4$, which gives us another solution to the equation $x^4 + y^4 = z^2$. Notice however that it is also true that

$$k^2 = p^2 + q^2 = a \leq a^2 < a^2 + b^2 = z \leq z^2.$$

Therefore we have the inequality $k < z$. We have hence found another triple of integers which is a solution to the equation $x^4 + y^4 = z^2$, namely $l^4 + m^4 = k^2$, where it is true that $k < z$. This however is a contradiction as we assumed no other solution (x^*, y^*, z^*) to exist where $z^* < z$. Hence a solution with z as small as possible does not exist which therefore proves that there are no solutions to the equation $x^4 + y^4 = z^2$. Hence it follows that there does not exist a nontrivial integer solution to the equation $x^4 + y^4 = z^4$ proving Fermat's equation for $n = 4$.

Q.E.D.

The above result follows from a solely number theory based approach. We now continue onward with an approach using ring theory that was very popular during the early 1800's. During this time, Fermat's last theorem was proven for some exponents n until Kummer found the biggest generalization. This is discussed in Chapter 9 near the end of this thesis. In chapter 6 we will discuss another proof of Fermat's last theorem for $n = 4$ using this new method.

2 Important notions from ring theory and field theory

Definition 2.1 *Let R be a ring with 1, then an element $a \in R$ is called a **unit** if there exists some $b \in R$ such that $ab = ba = 1$.*

The set of units in R is written as $R^\times$ and it is called the unit group of R. Some examples are $\mathbb{Z}^\times = \{-1, 1\}$ and $\mathbb{R}^\times = \mathbb{R}\backslash\{0\}$. In general finding units can be a tough task as in general it requires us to solve some difficult equations. Luckily there is a tool that can help, namely a so called norm-function.

Definition 2.2 *A map $\phi : R \to S$ between rings is called a ring homomorphism if it satisfies the following three properties:*

- $\phi(a +_R b) = \phi(a) +_S \phi(b)$.
- $\phi(a \cdot_R b) = \phi(a) \cdot_S \phi(b)$.
- $\phi(1_R) = 1_S$.

Definition 2.3 *Let R be a commutative ring. A norm is a function $N : R \to \mathbb{R}$ that satisfies the following properties.*

1. *$\forall \alpha, \beta \in R$ it holds that $N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta)$.*
2. *$N(0) = 0$.*
3. *$N(1) = 1$.*

In general depending on the ring R it can be possible to construct a norm that doesn't have to map into $\mathbb{R}$ but can map into $\mathbb{Z}$ which makes certain computations nicer. Now this norm function can be used to find units in our ring R. Namely if a is a unit of R then we know that there exists some $b \in R$ such that $ab = 1$. Applying the norm function on both sides of the equality yields

$$1 = N(1) = N(a \cdot b) = N(a) \cdot N(b).$$

Now this is just an equation that we have to solve in terms of what a and b are. Typically this is best demonstrated when the norm function maps into $\mathbb{Z}$ as then things turn out simple.

Example 2.1 *Take $R = \mathbb{Z}[\sqrt{m}]$ with m being an integer that is not a square, hence $R \neq \mathbb{Z}$. Note that we can write R as the following set. $R = \{a + b \cdot \sqrt{m} : a, b \in \mathbb{Z}\}$ and that therefore R is a commutative ring. We define the norm to be $N : R \to \mathbb{Z}$, $N(a+b\sqrt{m}) = (a+b\sqrt{m})(a-b\sqrt{m}) = a^2 - mb^2$. We verify that this is indeed a norm by checking the 3 properties given in Definition 2.3:*

1. *Let* $\alpha = a + b\sqrt{m}$ *and* $\beta = c + d\sqrt{m}$*, then* $\alpha \cdot \beta = (a + b\sqrt{m}) \cdot (c + d\sqrt{m}) = (ac + bdm) + (ad + bc)\sqrt{m}$*. Applying norms gives* $N(\alpha) = a^2 - mb^2$*,* $N(\beta) = c^2 - md^2$ *and* $N(\alpha \cdot \beta) = (ac + bdm)^2 - m(ad + bc)^2$*. From there one sees that*

$$\begin{aligned} N(\alpha) \cdot N(\beta) &= (a^2 - mb^2) \cdot (c^2 - md^2) \\ &= a^2c^2 - ma^2d^2 - mb^2c^2 + m^2b^2d^2 \\ &= a^2c^2 + 2mabcd + m^2b^2d^2 - ma^2d^2 - 2mabcd - mb^2c^2 \\ &= (ac + bdm)^2 - m(ad + bc)^2 \\ &= N(\alpha \cdot \beta) \end{aligned}$$

   Which is what was needed to be shown.

2. *Note that* $N(0) = N(0 + 0 \cdot \sqrt{0}) = 0 - 0 \cdot 0^2 = 0$*.*

3. *Note that* $N(1) = N(1 + 0 \cdot \sqrt{0}) = 1 - 0 \cdot 0^2 = 1$

Therefore our function N *is indeed a norm function. Because the norm function maps into the integers now finding units becomes relatively more simple. As seen if* α *is a unit then we can find some inverse* β *such that* $\alpha\beta = \beta\alpha = 1$ *and therefore also* $N(\alpha) \cdot N(\beta) = 1$*. Because both* $N(\alpha)$ *and* $N(\beta)$ *are integers we need to consider all possible cases where* $N(\alpha)$ *is a divisor* d *of* 1 *and where* $N(\beta) = \frac{1}{d}$*. Since the only divisors of* 1 *are* ± 1 *it remains to then solve the equation* $N(\alpha) = \pm 1$*. Letting* $\alpha = a + b\sqrt{m}$ *this becomes the quest of solving the equation* $a^2 - mb^2 = \pm 1$ *over the integers.*

Note that rings can have finitely but also infinitely many units. Taking the ring as described in the example above for $m = 2$ will yield infinitely many units, a results that will not be proven but can be looked up as Pell's equation. On the other hand taking just the ring $R = \mathbb{Z}$ with the norm $N : R \to \mathbb{Z}$, $N(a) = |a|$, one can follow along with the steps from Example 2.1 to get that $R^\times = \{1, -1\}$. These might look like two different cases but in fact there is some similarity between the two. In the case where $R = \mathbb{Z}$, the unit group is generated by only one element namely by -1. In other words $R^\times = \{1, -1\} = \langle -1 \rangle$. In Example 2.1, if one unit is found, say ϵ is a unit, then all powers of epsilon are also units. Hence it is true that $\{..., \epsilon^{-2}, \epsilon^{-1}, 1, \epsilon, \epsilon^2, ...\} = \langle \epsilon \rangle \subset \mathbb{Z}[\sqrt{m}]^\times$. The difference is that $\langle -1 \rangle$ is finite because $(-1)^2 = 1$, where on the other hand $\langle \epsilon \rangle$ is not because there does not exist a number n such that $\epsilon^n = 1$.

Definition 2.4 *A ring* R *is called a domain if* R *is commutative,* $1 \neq 0$ *and there are no* 0 *divisors in* R*.*

Definition 2.5 *A ring* R *is called a Euclidean domain if the ring* R *is a domain and moreover, that there exists a function*

$$g : R \backslash \{0\} \to \mathbb{Z}_{\geq 0}$$

with the property that for all $a, b \in R$ *with* $b \neq 0$*, there exist* $q, r \in R$ *such that* $a = qb + r$ *where either* $r = 0$ *or* $g(r) < g(b)$*.*

Definition 2.6 *A ring R is called a unique factorization domain if the ring R is a domain and moreover, for any $a \in R\backslash\{0\}$ we can write is as a product of a unit u and a finite number of irreducible elements p_i:*

$$a = u \cdot p_1 \cdot p_2 \cdots p_t.$$

The factorization is unique up to it's order and units.

Theorem 2.1 *If a ring R is a Euclidean domain, it is a unique factorization domain.*

Proof: The result of Theorem 6.1.4 and Theorem 5.3.4 from [3].

Definition 2.7 *A polynomial $f(x)$ of degree n over $\mathbb{Z}[x]$ is called irreducible if the only way for $f(x)$ to split up into two other polynomials $f(x) = g(x) \cdot h(x)$ is if either $g(x)$ or $h(x)$ is of degree 0, hence equal to a constant.*

In general the above definition has a more general setting, however we only need it on the ring $R = \mathbb{Z}$. Therefore we chose this simpler version.

Lemma 2.1 *Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial and $g(x), h(x) \in \mathbb{Q}[x]$ be also monic polynomials. If $f(x) = g(x) \cdot h(x)$, one has that $g(x), h(x) \in \mathbb{Z}[x]$.*

Now the reason that this matters to us is because we would like to find the so called minimal polynomial of the number ζ_n.

Definition 2.8 *The minimal polynomial of some complex number α is the polynomial $f(x)$ that has α as one of it's roots and furthermore $f(x)$ is irreducible.*

Definition 2.9 *The number $\zeta_n := e^{\frac{2\pi i}{n}}$ is called the n-th cyclotomic root of unity*

Using this notation we are able to state a first fundamental result about the roots of unity.

Theorem 2.2 *For all $n \in \mathbb{N}$, the minimal polynomial of the n-th root of unity is given by*

$$f_n(x) = \prod_{1 \leq j < n : \gcd(j,n)=1} (x - (\zeta_n)^j)$$

Proof: Observe that $x^n - 1 = \prod_{j=1}^{n}(x - (\zeta_n)^j)$ and define $f_n(x)$ to be the minimal polynomial of ζ_n. Note that $(\zeta_n)^n - 1 = 0$ and therefore $f_n(x)$ divides the polynomial $x^n - 1$. Due to the factorization $x^n - 1$ attains we just need to check which linear factors are in $x^n - 1$ but not in $f_n(x)$. First note that the only factors $f_n(x)$ can contain are the $x - (\zeta_n)^j$ where $\gcd(j, n) = 1$. Namely if

for a certain j such that $\gcd(j,n) = d > 1$ it holds that $f_n(x)$ contains $x - (\zeta_n)^j$ as a factor, then $f_n((\zeta_n)^j) = 0$. Furthermore $(\zeta_n)^j$ is also a root of $x^{\frac{n}{d}} - 1$ which means that $f_n(x)$ divides $x^{\frac{n}{d}} - 1$. Therefore $(\zeta_n)^{\frac{n}{d}} = 1$ which contradicts the fact that ζ_n is an n-th root of unity. Now it remains to show that every $x - (\zeta_n)^j$ where $\gcd(j,n) = 1$ is a factor of $f_n(x)$. We make the following claim:

Claim: If p is a prime not dividing n and $f_n(\alpha) = 0$, then $f_n(\alpha^p) = 0$ as well.

This claim can be used to show the desired result. To prove the claim we go by contradiction. Therefore suppose p is a prime not dividing n and $f_n(\alpha) = 0$ yet $f_n(\alpha^p) \neq 0$. Since $f_n(x)$ divides polynomial $x^n - 1$ there exists a polynomial $g(x) \in \mathbb{Z}[x]$ such that $x^n - 1 = f_n(x) \cdot g(x)$. Notice that

$$\begin{aligned} f_n(\alpha) = 0 &\Rightarrow \alpha^n - 1 = 0 \\ &\Rightarrow \alpha^n = 1 \\ &\Rightarrow \alpha^{pn} = 1 \\ &\Rightarrow \alpha^{pn} - 1 = 0 \\ &\Rightarrow (\alpha^p)^n - 1 = 0 \\ &\Rightarrow f_n(\alpha^p) \cdot g(\alpha^p) = 0 \Rightarrow g(\alpha^p) = 0. \end{aligned}$$

Since α^p is a root of $g(x)$, α is a root of $g(x^p)$. Since $f_n(x)$ is a minimal polynomial of some number which satisfies $f_n(\alpha) = 0$ it is also true that $f_n(x)$ divides polynomial $g(x^p)$. We find the relation

$$x^n - 1 = f_n(x) \cdot g(x) \Rightarrow x^{pn} - 1 = f_n(x^p) \cdot g(x^p)$$

where now $g(x^p)$ is divisible by $f_n(x)$. Because we work in $\mathbb{Z}[x]$, Lemma 2.1 tells us that $f_n(x^p) \cdot f_n(x)$ divides $x^{pn} - $‘1. Now observe that modulo p it is true that $(P(x))^p \equiv P(x^p) \pmod p$ for any polynomial $P(x) \in \mathbb{Z}[x]$. This follows from

$$\begin{aligned} P(x) = \sum_{i=0}^{n} a_i x^i \Rightarrow (P(x))^p &= \left(\sum_{i=0}^{n} a_i x^i \right)^p \\ &\equiv \sum_{i=0}^{n} (a_i)^p x^{ip} \pmod p \\ &\equiv \sum_{i=0}^{n} a_i x^{ip} \pmod p \\ &= \sum_{i=0}^{n} a_i (x^p)^i = P(x^p) \end{aligned}$$

where we used Fermat's little theorem which states that $a^p \equiv a \pmod{p}$ for all integers a and primes p. Using that modulo p, $P(x^p) \equiv (P(x))^p \pmod{p}$ we can find the following small relation using that $(x^n-1)^p \equiv x^{pn}-1 \pmod{p}$.

$$\begin{aligned}
&f_n(x^p)\cdot f_n(x) \text{ divides } x^{pn}-1\\
&\Rightarrow (f_n(x))^p \cdot f_n(x) \text{ divides } x^{pn-1}\\
&\Rightarrow (f_n(x))^{p+1} \text{ divides } x^{pn}-1=(x^n-1)^p.
\end{aligned}$$

Observe that x^n-1 only has simple roots, meaning roots of multiplicity 1. Since p does not divide n we find the multiplicity of all roots from $(x^n-1)^p$ to be equal to p. However since $(f_n(x))^{p+1}$ divides $(x^n-1)^p$, for roots both polynomials must be equal to zero. $(f_n(x))^{p+1}$ is a polynomial whose roots have multiplicity $\geq p+1$ which leads to a contradiction. Namely if two polynomials P and Q have a root α with respective multiplicites k and l where $k<l$, then $Q(x)$ does not divide $P(x)$ as in the ratio $\frac{P(x)}{Q(x)}$ there are more $x-\alpha$ terms in the denominator than in the numerator. This contradiction shows us that $f_n(\alpha^p)=0$ as well whenever $f_n(\alpha)=0$ for p a prime not dividing n which proves the claim.

Now suppose j is such that $\gcd(j,n)=1$ and $1\leq j<n$. We know $f_n(\zeta_n)=0$ and aim to show $f_n((\zeta_n)^j)=0$ as well as this implies $f_n(x)$ contains the factor $x-(\zeta_n)^j$. Write j as a product of prime numbers p_i where all p_i are not necessarily distinct. This being $j=\prod_{i=1}^{t} p_i$. Because $\gcd(j,n)=1$ it follows that $\gcd(p_i,t)=1$ for all $1\leq i\leq t$. It then follows using our claim that

$$\begin{aligned}
f_n(\zeta_n)=0 &\Rightarrow f_n((\zeta_n)^{p_1})=0\\
&\Rightarrow f_n(((\zeta_n)^{p_1})^{p_2})=f_n((\zeta_n)^{p_1p_2})=0\\
&\Rightarrow f_n(((\zeta_n)^{p_1p_2})^{p_3})=f_n((\zeta_n)^{p_1p_2p_3})=0\\
&\vdots\\
&\Rightarrow f_n((\zeta_n)^{p_1p_2p_3\cdots p_t})=f_n((\zeta_n)^j)=0.
\end{aligned}$$

Therefore $f_n((\zeta_n)^j)=0$ for all $1\leq j<n$ where $\gcd(j,n)$. Hence $f_n(x)$ can contain only and contains all $x-(\zeta_n)^j$ terms whenever $\gcd(j,n)=1$ and $1\leq j<n$. This proves that

$$f_n(x)=\prod_{1\leq j<n:\gcd(j,n)=1}(x-(\zeta_n)^j)$$

as desired.

Q.E.D.

As a consequence of Theorem 2.2, whenever n is a prime number one has

$$f_n(x) = \prod_{1 \leq j < n : \gcd(j,n)=1} (x - (\zeta_n)^j) = (x - (\zeta_n)^1)(x - (\zeta_n)^2) \cdots (x - (\zeta_n)^{n-1})$$

It might not be immediately obvious to one however it is possible to write this in a much neater way.

Lemma 2.2 ***The Eisenstein criterion*** *says that if a polynomial $f(x) = a_n x^n + ... + a_1 x + a_0$ over $\mathbb{Z}[x]$ satisfies the following properties with respect to some prime number p, then it is irreducible.*

- $p \nmid a_n$.
- $p \mid a_i$ *for* $i = 0, 1, ..., n-1$.
- $p^2 \nmid a_0$

Using this Lemma we obtain the following result.

Lemma 2.3 *For prime numbers n, one has that the minimal polynomial of ζ_n equals*

$$f_n(x) = \frac{x^n - 1}{x - 1} = x^{n-1} + ... + x + 1.$$

Proof: First one writes $g(x) = x^{n-1} + ... + x + 1 = \frac{x^n - 1}{x-1}$. Then after making the substitution $x = 1 + t$ we find

$$g(1+t) = \frac{(1+t)^n - 1}{(1+t) - 1} = \frac{1 + \sum_{k=1}^{n} \binom{n}{k} t^k - 1}{t} = \sum_{k=1}^{n} \binom{n}{k} t^{k-1}$$

Since each binomial coefficient $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ is divisible by the prime $p = n$, the polynomial $g(1+t)$ is irreducible by Lemma 2.2. Therefore, $g(x)$ is also irreducible. Because both $f_n(x)$ and $g(x)$ are irreducible polynomials of the same degree with the same root $x = \zeta_n$, they are in fact the same polynomial. Hence

$$f_n(x) = g(x) = x^{n-1} + ... + x + 1$$

which finishes the proof.

Q.E.D.

Now Lemma 2.3 allows us to write any number α in the ring $\mathbb{Z}[\zeta_n]$ as

$$\alpha = a_0 + a_1\zeta_n + ... + a_{n-1}(\zeta_n)^{n-1} \tag{2.1}$$

where each $a_i \in \mathbb{Z}$. This is useful as it then allows us to make computation within the ring $\mathbb{Z}[\zeta_n]$.

For a recap on Galois theory, the reader is encouraged to read Chapters 1 and 2 from [2] as going through the necessary definitions and theorems would take up too much space. Notions from Galois theory will appear during Chapters $7, 8$ and 9.

3 The ring $\mathbb{Z}[\zeta_3]$

In this section we define $\zeta := \zeta_3$ for notational convenience. Following Equation 2.1 we find that $\mathbb{Z}[\zeta] = \{a + b\zeta : a, b \in \mathbb{Z}\}$. For the readers interest, the exact value of ζ is given by

$$\zeta = \frac{-1 + i\sqrt{3}}{2}.$$

3.1 The units of $\mathbb{Z}[\zeta_3]$

To determine the units of $\mathbb{Z}[\zeta]$ we first aim to find a valid norm function from Definition 2.3. Then by following the logic of Example 2.1, when the norm function maps perfectly into $\mathbb{Z}$ all that we have to do is to solve the equation $N(\alpha) = \pm 1$. This then allows us to find all the units because

$$\mathbb{Z}[\zeta]^\times = \{\alpha : \exists \beta \in \mathbb{Z}[\zeta] \text{ such that } \alpha \cdot \beta = 1\} = \{\alpha : N(\alpha) = 1\}.$$

We define the following function:

$$N : \mathbb{Z}[\zeta] \to \mathbb{R}, N(\alpha) = \alpha \cdot \overline{\alpha}. \tag{3.1}$$

One easily determines that this function $N(\alpha)$ does satisfy the three conditions from Definition 2.3 and therefore this function is indeed a norm. Using that $\zeta^2 + \zeta + 1 = 0$ we can simplify this to become

$$\begin{aligned} N(\alpha) = \alpha \cdot \overline{\alpha} &= (a + b\zeta) \cdot \overline{(a + b\zeta)} \\ &= (a + b\zeta) \cdot (a + b\overline{\zeta}) = a^2 + ab(\zeta + \overline{\zeta}) + b^2\zeta\overline{\zeta} = a^2 - ab + b^2. \end{aligned}$$

This shows us that in fact $N : \mathbb{Z}[\zeta] \to \mathbb{Z}$.

Lemma 3.1 *The units of* $\mathbb{Z}[\zeta]$ *are given by* $\{\pm 1, \pm\zeta, \pm\zeta^2\}$.

Proof: Because the norm function maps into $\mathbb{Z}$, for units it is true that $N(\alpha) = \pm 1$. Therefore to find all the units, we solve the equation $N(\alpha) = \pm 1$ where $\alpha \in \mathbb{Z}[\zeta]$. This is the same as solving $a^2 + b^2 - ab = \pm 1$ for $a, b \in \mathbb{Z}$. To solve this we are going to complete the square, rewriting our equation to be

$$a^2 - ab + b^2 = a^2 - 2 \cdot a \cdot \frac{b}{2} + \frac{b^2}{4} + \frac{3b^2}{4}$$
$$= (a - \frac{b}{2})^2 + \frac{3b^2}{4} = \pm 1.$$

It follows that the -1 case is impossible because squares are always positive numbers. Therefore we now look at the $+1$ case. Because $(a - \frac{b}{2})^2 \geq 0$, we obtain that $\frac{3b^2}{4} \leq 1$ and therefore we obtain three possible values for b namely $b \in \{-1, 0, 1\}$.

1. The case $b = -1$ gives us $(a + \frac{1}{2})^2 = \frac{1}{4}$ and so $a = 0$ or $a = -1$. Therefore $\alpha = -\zeta$ or $\alpha = -1 - \zeta$.
2. The case $b = 0$ gives us $a^2 = 1$ and so $a = -1$ or $a = 1$. Therefore $\alpha = -1$ or $\alpha = 1$.
3. Lastly, the case $b = 1$ gives us $(a - \frac{1}{2})^2 = \frac{1}{4}$ and so $a = 0$ or $a = 1$. Therefore $\alpha = \zeta$ or $\alpha = 1 + \zeta$.

Hence we obtain $\mathbb{Z}[\zeta]^\times = \{-\zeta, -1 - \zeta, 1, -1, \zeta, 1 + \zeta\}$. Using that $\zeta^2 = -1 - \zeta$ we obtain $\mathbb{Z}[\zeta]^\times = \{-\zeta, \zeta^2, -1, \zeta, -\zeta^2, 1\}$. This indeed shows us that

$$\mathbb{Z}[\zeta] = \{\pm 1, \pm\zeta, \pm\zeta^2\}$$

which is what we intended to show.

Q.E.D.

3.2 Unique factorization in $\mathbb{Z}[\zeta_3]$

Next up we would like to determine whether or not we have unique factorization up to units in the ring $\mathbb{Z}[\zeta]$. Following Theorem 2.1 it is enough to show that $\mathbb{Z}[\zeta]$ is a Euclidean domain.

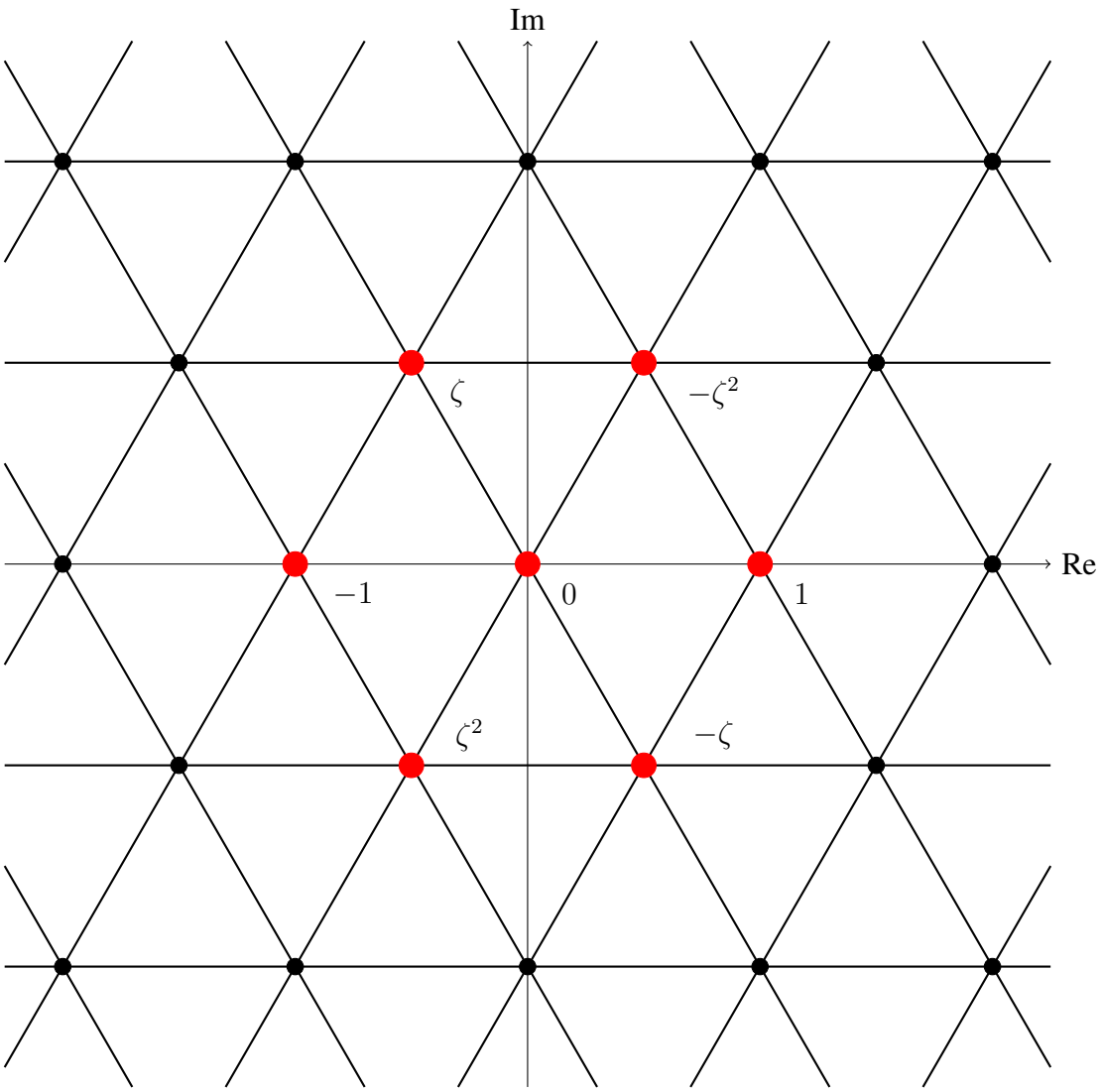
Theorem 3.1 *The ring $\mathbb{Z}[\zeta]$ is a euclidean domain, hence a unique factorization domain.*

Proof: According to Definition 2.5 we need to show that there exists a map $\Phi : \mathbb{Z}[\zeta]\backslash\{0\} \to \mathbb{N}$ such that given any $m, n \in \mathbb{Z}[\zeta]$, there exists q and r in $\mathbb{Z}[\zeta]$ such that $m = nq + r$ where either $r = 0$ or $\Phi(r) < \Phi(n)$. The claim that we make is that this works if we take the map $\Phi = N$ where N was the norm as described in Equation 3.1. Now a key observation is to note that $N(\alpha) = \alpha\overline{\alpha} = |\alpha|^2$ is just the standard Euclidean norm squared. This will come in handy later. Suppose we are given any $m, n \in \mathbb{Z}[\zeta]$, let $q \in \mathbb{Z}[\zeta]$ be such that there is some $r^* \in \mathbb{Q}[\zeta]$ with

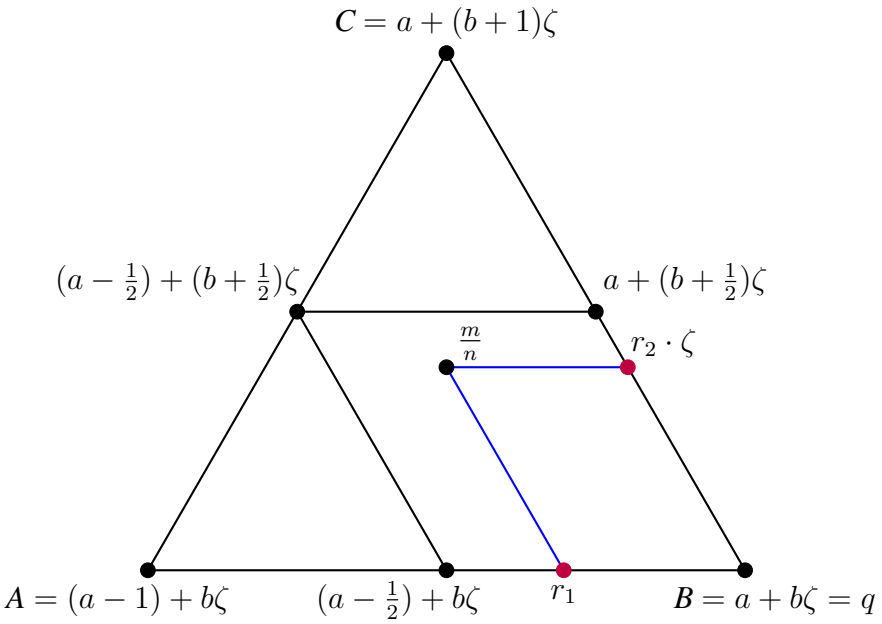
$$\frac{m}{n} = q + r^*.$$

First we need to define an extension of N into $\mathbb{Q}[\zeta]$, we pick the natural one where $N(\frac{a}{b}) := \frac{N(a)}{N(b)}$. This extension is well defined due to the multiplicity of N. We would then like to show that we can pick a certain value of q such that $N(\frac{m}{n} - q) < 1$, as then we can conclude the proof. Namely for the defined q we can write $m = nq + r$ and rewrite to $\frac{m}{n} - q = \frac{r}{n}$. Note that if it happens to be that $\frac{m}{n} \in \mathbb{Z}[\zeta]$, then we let it be equal to q yielding that $r = 0$. Therefore we now suppose that $\frac{m}{n} \notin \mathbb{Z}[\zeta]$ and hence $r \neq 0$. If the left hand side has norm < 1 then so does the right hand side which gives us that $N(\frac{r}{n}) < 1 \Rightarrow \frac{N(r)}{N(n)} < 1 \Rightarrow N(r) < N(n)$. This is precisely the desired result so it remains to show that $N(\frac{m}{n} - q) < 1$ and since the norm function is the euclidean norm squared, in words it means that q is at most distance 1 away from the point $\frac{m}{n}$.

For this we will observe the triangular structure of all the points in $\mathbb{Z}[\zeta]$. Namely if we draw all the points that lay in $\mathbb{Z}[\zeta]$, we observe that they basically form a bunch of horizontal lines parallel to the real axis, each of them spaced apart by a vertical distance of $\frac{\sqrt{3}}{2}$, the points of two lines next to each other are spaced out by a distance of $\frac{1}{2}$ which combined yields that each point has exactly six neighbors of distance 1 from it. This becomes clear in the following diagram.



Now that we have all these triangles we can see that all the corners of each triangle are precisely those points that are in $\mathbb{Z}[\zeta]$. Because we supposed that $\frac{m}{n} \notin \mathbb{Z}[\zeta]$ we know that it lies either on the edge or inside one of these triangles. We look closer into the triangle that contains the point $\frac{m}{n}$ and let one of the three corners be q to ensure that $q \in \mathbb{Z}[\zeta]$ and sort of close to $\frac{m}{n}$. Now we are going to define the following. We said that $\frac{m}{n}$ lies in $\mathbb{Q}[\zeta]$, therefore we will define numbers $r_1, r_2 \in \mathbb{Q}$ such that $\frac{m}{n} = r_1 + r_2\zeta$. The geometrical interpretation of q was that it is one of the corners of the triangle containing $\frac{m}{n}$ but with our new way of writing we can pick the optimal corner. Namely we can find a and b in $\mathbb{Z}$ such that $q = a + b\zeta$ and where $|r_1 - a| \leq \frac{1}{2}, |r_2 - b| \leq \frac{1}{2}$. Looking at the following picture motivates this reasoning and shows that we are indeed allowed to make this choice.



The point $\frac{m}{n}$ is located in one of the three regions enclosed in black lines. Whatever region it lies in, we take q to be the vertex of the main triangle that lies on the boundary of this region containing $\frac{m}{n}$. Now using all of the above one concludes the following key result.

$$\begin{aligned} N(\frac{m}{n} - q) &= N(r_1 + r_2\zeta - a - b\zeta) \\ &= N((r_1 - a) + (r_2 - b)\zeta) \\ &= (r_1 - a)^2 - (r_1 - a)(r_2 - b) + (r_2 - b)^2 \\ &\leq \left(\frac{1}{2}\right)^2 + \frac{1}{2} \cdot \frac{1}{2} + \left(\frac{1}{2}\right)^2 = \frac{3}{4} < 1. \end{aligned}$$

Here we used that $-\frac{1}{2} \leq r_1 - a, r_2 - b \leq \frac{1}{2}$. The result we obtain is then that for any $m, n \in \mathbb{Z}[\zeta]$ where n is nonzero there exists some $q \in \mathbb{Z}[\zeta]$ such that $N\left(\frac{m}{n} - q\right) < 1$. Therefore, there exists an $r \in \mathbb{Z}[\zeta]$ such that $m = nq + r$ where $r = 0$ or $N(r) < N(n)$. This shows that $\mathbb{Z}[\zeta]$ is indeed a Euclidean domain and hence a unique factorization domain by Theorem 2.1.

Q.E.D.

4 Proving Fermat's last theorem for $n = 3$

We have shown what the units of $\mathbb{Z}[\zeta]$ are and have also shown that this ring has unique factorization. Now we are ready to tackle Fermat's equation. Typically Fermat's equation is split up into two cases. When proving that $x^3 + y^3 = z^3$ has no nontrivial solutions in $\mathbb{Z}$, the first case concerns the situation where xyz is not divisible by 3 and the second case concerns the situation where xyz is divisible by 3. Typically this difference is made because of the following irreducible element.

Lemma 4.1 *The number $1 - \zeta$ is irreducible in $\mathbb{Z}[\zeta]$. That is the only divisors of $1 - \zeta$ are itself, units and itself multiplied by units.*

Proof: Note that $N(1 - \zeta) = N(1 + (-1)\zeta) = (1)^2 + (-1)^2 - (1)(-1) = 3$. Therefore if $1 - \zeta = A \cdot B$ for some $A, B \in \mathbb{Z}[\zeta]$ then it holds that $3 = N(1 - \zeta) = N(A \cdot B) = N(A) \cdot N(B)$ showing that either $N(A) = 1$ or $N(B) = 1$ and so respectively either A or B is a unit, showing that $1 - \zeta$ is indeed irreducible in $\mathbb{Z}[\zeta]$.

Q.E.D.

Now notice that in the ring $\mathbb{Z}[\zeta]$, it is true that $1-\zeta$ divides 3. Indeed one can check by computation that $3 = -\zeta^2 \cdot (1 - \zeta)^2$. We start of by proving the first case of Fermat;s last theorem for $n = 3$.

Lemma 4.2 *The equation $x^3 + y^3 = z^3$ has no solution over the integers whenever xyz is not divisible by 3.*

Proof: The proof of this statement requires some simple modular arithmetic. Since xyz is not divisible by 3 it then means that x, y and z are also not divisible by 3, because 3 is a prime number in $\mathbb{Z}$. Hence $x \equiv 1$ or $2 \pmod 3$, $y \equiv 1$ or $2 \pmod 3$ and $z \equiv 1$ or $2 \pmod 3$. Looking at the equation $x^3 + y^3 = z^3$ modulo 9 then reveals the following.

$$\begin{cases} x \equiv 1 \pmod 3 \Rightarrow x^3 \equiv 1 \pmod 9 \\ x \equiv 2 \pmod 3 \Rightarrow x^3 \equiv -1 \pmod 9 \end{cases}$$

These are then also all the possible values of $y^3 \pmod 9$ and $z^3 \pmod 9$. Therefore after reducing $\pmod 9$ in $x^3 + y^3 = z^3$ the left side satisfies $x^3 + y^3 \equiv -2, 0$ or $2 \pmod 9$ whereas the right side satisfies $z^3 \equiv \pm 1 \pmod 9$. Since the two sides are never equal $\pmod 9$ they are also never equal in general, hence the equation $x^3 + y^3 = z^3$ has no solutions when xyz is not divisible by 3.

Q.E.D.

Now that the first case is proven it is time to move to the second case, namely where xyz is divisible by 3. Without loss of generality we are going to actually assume that z is divisible by 3 and both x and y are not because of respective coprimality. The reason that we can take z to be divisible

by 3 is because the equation can be rewritten such that x, y and z can swap roles, for example $x^3 + (-z)^3 = (-y)^3$ over the integers. Because of this symmetry we can just say that z is divisible by 3. We furthermore assume that the $\gcd(x, y, z) = 1$ because any common divisors can be divided out, hence xyz divisible by 3 implies that only one out of the x, y and z is divisible by 3.

To then prove the second case of Fermat's last theorem for $n = 3$ we are actually going to prove a stronger statement out of which the result will follow. What we are going to prove is that the equation

$$x^3 + y^3 = u((1-\zeta)^k z)^3 \tag{4.1}$$

has no solution in $\mathbb{Z}[\zeta]$ where u is a unit, $k \geq 1$ is an integer, x, y and z are pairwise coprime and xyz is not divisible by $1 - \zeta$. If this equation has no solution in $\mathbb{Z}[\zeta]$, then $x^3 + y^3 = z^3$ also has no solution in $\mathbb{Z}$ where x, y and z are pairwise coprime and z is divisible by 3. The reason for this has to do with the following. Namely if (x, y, z) solves $x^3 + y^3 = z^3$, then the triple $(x^*, y^*, z^*) = (x, y, \frac{z}{(1-\zeta)^k})$ solves $(x^*)^3 + (y^*)^3 = u((1-\zeta)^k(z^*))^3$ for $u = 1$ and k being equal to twice the exponent of 3 in the prime decomposition of z. In other words because z is a multiple of 3, we can write $z = 3^p q$ where q is not divisible by 3 and then take $k = 2p$. Note that $3 = (1-\zeta)^2(-\zeta^2)$ and so $\frac{z}{(1-\zeta)^k}$ is well defined in $\mathbb{Z}[\zeta]$ and leaves no factor of $1 - \zeta$. Also note that x^* and y^* are not divisible by $1 - \zeta$ because x and y are not divisible by 3, but 3 is divisible by $1 - \zeta$. Furthermore because every factor of 3 is divided out in how z^* was picked, it is also not divisible by $1 - \zeta$. Therefore this new triple (x^*, y^*, z^*) is a valid solution to equation 4.1

Theorem 4.1 *The equation $x^3 + y^3 = u((1-\zeta)^k z)^3$ for u a unit, $k \geq 1$ an integer, x, y and z relatively co-prime and xyz is not divisible by $1 - \zeta$ has no solution for $x, y, z \in \mathbb{Z}[\zeta]$.*

Proof: We follow along the proof that was published in a paper with unknown author [4]. We start of by giving the structure of the proof, as we are going to do a proof by infinite descent. We aim to show the following two statements from which we can conclude no solution exists.

1. If a solution does exist, then $k \geq 2$
2. If there is a solution for $k \geq 2$, then there is also a solution for k being replaced by $k - 1$.

If these statements hold, then we can indeed conclude that there are no solutions to $x^3 + y^3 = u((1-\zeta)^k z)^3$. We begin with the proof of the first statement, hence suppose a solution exists for some $k \geq 1$ and satisfactory x, y, z and u. Typically we wrote elements of $\mathbb{Z}[\zeta]$ as $\alpha = a + b\zeta$ however we will now opt for a different style of writing, namely $x = a_0 + a_1(1-\zeta)$ and $y = b_0 + b_1(1-\zeta)$ where $a_0, a_1, b_0, b_1 \in \mathbb{Z}$. Now both x and y are such that they are not divisible by $1 - \zeta$. Suppose that a_0 is divisible by 3, then a_0 is also divisible by $1 - \zeta$ which would give that x is divisible by $1 - \zeta$ however we assumed it not to be. The same reasoning applies for b_0 and y. Therefore both a_0 and b_0 are not divisible by 3.

Note that replacing y by $\zeta^j y$ still yields a valid solution to the Equation 4.1 because $y^3 = (\zeta y)^3$. This motivates to look into $\zeta^j y$. For any $j \geq 0$ we have the following relation.

$$\begin{aligned}\zeta^j y = (1-(1-\zeta))^j(b_0+b_1(1-\zeta)) &\equiv (1-j(1-\zeta))(b_0+b_1(1-\zeta)) \pmod{(1-\zeta)^2} \\ &\equiv b_0 + (b_1 - jb_0)(1-\zeta) \pmod{(1-\zeta)^2}\end{aligned}$$

Now observe that $(1-\zeta)^2 = -3\zeta$ which implies that $\zeta^j y = b_0 + (b_1 - jb_0)(1-\zeta) - 3\zeta K$ for some $K \in \mathbb{Z}[\zeta]$. Next we pick j such that $a_1 + b_1 - jb_0 \equiv 0 \pmod 3$. This j always exists because b_0 is not a multiple of 3 so this equation can be solved for $j \pmod 3$. For this specific j we then see that

$$\begin{aligned}x + \zeta^j y &= a_0 + a_1(1-\zeta) + b_0 + (b_1 - jb_0)(1-\zeta) - 3\zeta K \\ &= a_0 + b_0 + (a_1 + b_1 - jb_0)(1-\zeta) - 3\zeta K \\ &\equiv a_0 + b_0 \pmod 3\end{aligned}$$

Here in the last line we used that $-3\zeta K \equiv 0 \pmod 3$ and that j was picked such that $a_1 + b_1 - jb_0 \equiv 0 \pmod 3$. Now there exist integers c_0, c_1, d_0, d_1 such that $\zeta y = c_0 + c_1(1-\zeta)$ and $\zeta^2 y = d_0 + d_1(1-\zeta)$. We could express them in terms of b_0 and b_1, however, that is not of our interest. Instead, we aim for the result $b_0 \equiv c_0 \equiv d_0 \pmod 3$. From the expression $\zeta^j y = b_0 + (b_1 - jb_0)(1-\zeta) - 3\zeta K$ we see that the only terms that can influence the values of c_0 and d_0 are b_0 and $-3\zeta K$. Reducing $\pmod 3$ will cancel the latter term leaving just b_0 and therefore $b_0 \equiv c_0 \equiv d_0 \pmod 3$. This then implies that

$$\begin{aligned}x + \zeta^j y &\equiv a_0 + b_0 \pmod 3 \\ &\equiv a_0 + c_0 \pmod 3 \\ &\equiv a_0 + d_0 \pmod 3\end{aligned}$$

which means that after replacing y by $\zeta^j y$, we can find a representation of $x + \zeta^j y \pmod 3$ that uses a_0 from how x was written and one of b_0, c_0, d_0 depending on what our value of j is, as we can pick the term corresponding to the value of a where $\zeta^j y = a + b(1-\zeta)$. Hence replacing y by $\zeta^j y$ allows us to write $x + \zeta^j y \pmod 3$ using only coefficients that were used in it's own representation in $\mathbb{Z}[\zeta]$. This replacement allows us to assume that $x + y \equiv a_0 + b_0 \pmod 3$ where we know $a_0, b_0 \in \mathbb{Z}$, as after replacing y by $\zeta^j y$ we can find a suitable representation $\pmod 3$. Now using that $\frac{1-\zeta^i}{1-\zeta} = 1 + \zeta + ... + \zeta^{i-1}, \forall i \geq 0$ we obtain that

$$\begin{aligned}x + \zeta^i y = x + y - (1-\zeta^i)y = x + y - (1-\zeta)(1+\zeta+...+\zeta^{i-1})y \\ &\equiv x + y \pmod{1-\zeta} \\ &\equiv a_0 + b_0 \pmod{1-\zeta}\end{aligned}$$

Note that the last line follows from $x + y \equiv a_0 + b_0 \pmod 3$ and that $1 - \zeta$ is a divisor of 3.

Returning to our original equation $x^3 + y^3 = u((1-\zeta)^k z)^3$ we see that the left side can factor as $x^3+y^3 = (x+y)(x+\zeta y)(x+\zeta^2 y)$ inside $\mathbb{Z}[\zeta]$. As the right-hand side of $x^3+y^3 = u((1-\zeta)^k z)^3$ is divisible by $1-\zeta$, so is the left-hand side. After combining all these results, one finds the following equivalences.

$$\begin{aligned} 0 &\equiv x^3 + y^3 \pmod{1-\zeta} \\ &\equiv (x+y)(x+\zeta y)(x+\zeta^2 y) \pmod{1-\zeta} \\ &\equiv (a_0+b_0)(a_0+b_0)(a_0+b_0) \pmod{1-\zeta} \\ &\equiv (a_0+b_0)^3 \pmod{1-\zeta} \end{aligned}$$

Because $1-\zeta$ is irreducible and divides $(a_0+b_0)^3$, it is actually also the case that it divides a_0+b_0. Now I make the following claim:

$$\mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}[\zeta]/(1-\zeta)\mathbb{Z}[\zeta] \tag{4.2}$$

This can be proven by defining the following map, $\Phi : \mathbb{Z}[\zeta]/(1-\zeta)\mathbb{Z}[\zeta] \to \mathbb{Z}/3\mathbb{Z}$ by $\Phi(a+b\zeta) = \overline{a+b}$. This works as $a+b\zeta = a+b-b+b\zeta = a+b-(1-\zeta)b \equiv a+b \pmod{1-\zeta}$ so this is in fact the natural map between the two objects. Because both 3 and $1-\zeta$ are irreducible elements in $\mathbb{Z}$ respectively $\mathbb{Z}[\zeta]$, both the domain and co-domain of Φ are fields. Combined with the observation that Φ is a surjective it follows that both of the fields are isomorphic. The important thing is then that zeroes in $\mathbb{Z}[\zeta]/(1-\zeta)\mathbb{Z}[\zeta]$ correspond to zeroes in $\mathbb{Z}/3\mathbb{Z}$. So since a_0+b_0 is a multiple of $1-\zeta$, it corresponds to $\overline{0}$ in $\mathbb{Z}[\zeta]/(1-\zeta)\mathbb{Z}[\zeta]$ and therefore it also corresponds to $\overline{0}$ in $\mathbb{Z}/3\mathbb{Z}$. We combine this with the fact that $\Phi|_{\mathbb{Z}} = id|_{\mathbb{Z}}$ to show that $a_0+b_0 \in \mathbb{Z}$ is also a multiple of 3, hence $a_0+b_0 \equiv 0 \pmod 3$.

Because we had the equivalence $x+y \equiv a_0+b_0 \pmod 3$ it also shows that $x+y$ is divisible by 3. In fact because $(1-\zeta)^2 = -3\zeta$ and since $-\zeta$ is a unit it follows that $x+y$ is divisible by $(1-\zeta)^2$. This is important to us for the following reason. Since $x^3+y^3 = (x+y)(x+\zeta y)(x+\zeta^2 y)$ we are able to say the following thing about x^3+y^3

- We have $x+y \equiv 0 \pmod{(1-\zeta)^2}$.
- We have $x+\zeta y \equiv a_0+b_0 \pmod{1-\zeta} \equiv 0 \pmod{1-\zeta}$ because 3 is divisible by $1-\zeta$.
- We have $x+\zeta^2 y \equiv a_0+b_0 \pmod{1-\zeta} \equiv 0 \pmod{1-\zeta}$ because 3 is divisible by $1-\zeta$.

So after multiplying everything we find that x^3+y^3 is divisible by $(1-\zeta)^4$. Returning to $x^3+y^3 = u((1-\zeta)^k z)^3$, we now see that the left side is divisible by $(1-\zeta)^4$. Therefore also the right side should be divisible by $(1-\zeta)^4$. Since u is a unit and z was assumed to not be divisible by $1-\zeta$, we must have that $k \geq 2$. This is because if k were to equal 1, the right side is divisible by $(1-\zeta)^3$ but not the fourth power. This proves the first statement which said that if a solution exists, then $k \geq 2$.

To now prove the second statement, we take a solution for a certain $k \geq 2$ and try to construct a solution where k is now replaced by $k-1$. Because x and y were said to be co-prime, it also follows that the numbers $\frac{x+\zeta^a y}{1-\zeta}$ and $\frac{x+\zeta^b y}{1-\zeta}$ are co-prime where without loss of generality $0 \leq a < b < 3$. Suppose by contradiction that $\frac{x+\zeta^a y}{1-\zeta}$ and $\frac{x+\zeta^b y}{1-\zeta}$ are not co-prime, then there exists some $d \in \mathbb{Z}[\zeta]$ that is not a unit and divides them both. However, then also d divides their difference which equates to

$$\frac{x+\zeta^a y}{1-\zeta} - \frac{x+\zeta^b y}{1-\zeta} = \frac{\zeta^a - \zeta^b}{1-\zeta} y = \zeta^a \cdot \frac{1-\zeta^{b-a}}{1-\zeta} \cdot y.$$

Note however that ζ^a is a unit and that $\frac{1-\zeta^{b-a}}{1-\zeta}$ is also a unit, the latter can be checked using a standard computation. Therefore the d we picked should divide y itself and since it divides $x+\zeta^i y$, d also divides x. This however contradicts the fact that x and y were picked to be coprime.

Returning to the equation $x^3 + y^3 = u((1-\zeta)^k z)^3$, one factors the left side like we did before to be $(x+y)(x+\zeta y)(x+\zeta^2 y) = u((1-\zeta)^k z)^3$. Because the product of three numbers with only one common divisor equals a cube, it allows us to make the following factorization which is unique because we showed in Theorem 3.1 that $\mathbb{Z}[\zeta]$ is a Euclidean domain and therefore a unique factorization domain.

$$\begin{aligned} x + y &= u_0 \cdot (1-\zeta) \cdot (1-\zeta)^{3(k-1)} \cdot (t_0)^3 \\ x + \zeta y &= u_1 \cdot (1-\zeta) \cdot (t_1)^3 \\ x + \zeta^2 y &= u_2 \cdot (1-\zeta) \cdot (t_2)^3 \end{aligned}$$

Here the numbers u_0, u_1 and u_2 are units, the numbers t_0, t_1 and t_2 are pairwise co-prime and not divisible by $1-\zeta$. The coprimality comes from the result that the numbers $\frac{x+\zeta^a y}{1-\zeta}$ and $\frac{x+\zeta^b y}{1-\zeta}$ are co-prime for all suitable a and b. Furthermore none of t_0, t_1 and t_2 are divisible by $1-\zeta$. This is because $x+\zeta y$ and $x+\zeta^2 y$ are not divisible by $(1-\zeta)^2$ and so t_1 and t_2 are not divisible by $1-\zeta$. Furthermore because $x+y$ is divisible by a higher power of $1-\zeta$, all remaining factors of $1-\zeta$ are actually there which gives us the $(1-\zeta)^{3(k-1)}$ term there. As now all required $1-\zeta$ powers are there, t_0 is also not divisible by $1-\zeta$.

Observe the following equation:

$$\begin{aligned} (x+\zeta y) + \zeta(x+\zeta^2 y) &= x + \zeta y + \zeta x + \zeta^3 y \\ &= x + \zeta x + y + \zeta y \\ &= (1+\zeta)x + (1+\zeta)y \\ &= (1+\zeta)(x+y). \end{aligned}$$

Plugging in the new ways of writing we found for $x+y$, $x+\zeta y$ and $x+\zeta^2 y$ this line becomes

$$u_1 \cdot (1-\zeta) \cdot (t_1)^3 + \zeta \cdot u_2 \cdot (1-\zeta) \cdot (t_2)^3 = (1+\zeta) \cdot u_0 \cdot (1-\zeta) \cdot (1-\zeta)^{3l} \cdot (t_0)^3.$$

After dividing both sides by $1 - \zeta$ we obtain

$$u_1 \cdot (t_1)^3 + \zeta \cdot u_2 \cdot (t_2)^3 = (1 + \zeta) \cdot u_0 \cdot (1 - \zeta)^{3l} \cdot (t_0)^3.$$

Next we can divide by the unit u_1 to get the equation

$$(t_1)^3 + \zeta \cdot \frac{u_2}{u_1} \cdot (t_2)^3 = (1 + \zeta) \cdot \frac{u_0}{u_1} \cdot (1 - \zeta)^{3l} \cdot (t_0)^3.$$

Finally to make the reading better, we replace $\zeta \cdot \frac{u_2}{u_1}$ by A and $\frac{u_0}{u_1} \cdot (1 + \zeta)$ by B where now A and B are both units because they are a product and quotient of units.

$$(t_1)^3 + A \cdot (t_2)^3 = B \cdot (1 - \zeta)^{3l} \cdot (t_0)^3. \tag{4.3}$$

Now because k was said to be ≥ 2 and $l = k - 1$, we have $l \geq 1$. Therefore

$$(1 - \zeta)^{3l} = (1 - \zeta)^{3l-2} \cdot (1 - \zeta)^2 \equiv 0 \pmod 3.$$

It then follows that the right side of Equation 4.3 is equivalent to $0 \pmod 3$ which means also that $(t_1)^3 + A \cdot (t_2)^3 \equiv 0 \pmod 3$. Notice that any $\alpha = a + b\zeta$ satisfies

$$\alpha^3 = a^3 + 3a^2b\zeta + 3ab^2\zeta^2 + b^3\zeta^3 \equiv a^3 + b^3 \pmod 3.$$

We apply this observation on the t_i's. We have that each $t_i^3 \not\equiv 0 \pmod 3$, because if 3 divides t_i, then so does $1-\zeta$ which contradicts the definition of each t_i. Setting $t_2 = a_2+b_2\zeta$ makes $(t_2)^3 \equiv 1 \pmod 3$ or $\equiv 2 \pmod 3$. Therefore there exists some integer n such that $n \cdot (t_2)^3 \equiv 1 \pmod 3$. After multiplying Equation 4.3 by n we see that the unit A is a rational integer $\pmod 3$ because $n(t_1)^3 + An(t_2)^3 \equiv n(t_1)^3 + A \equiv 0 \pmod 3$. We can check the list of units found in Lemma 3.1 and find that the only two possible such units are ± 1. This shows us that $A = \pm 1$. Because t_2 can be replaced by $-t_2$ for a solution, we only have to look at $A = 1$ which yields

$$\begin{aligned}(t_1)^3 + (t_2)^3 &= B \cdot (1 - \zeta)^{3l} \cdot (t_0)^3 \\ &= B((1 - \zeta)^l t_0)^3\end{aligned}$$

where we have that B is a unit, $l \geq 1$ is an integer, t_0, t_1 and t_2 are relatively co-prime and $t_0t_1t_2$ is not divisible by $1 - \zeta$. This is exactly our Equation 4.1 from before again, however we have now constructed a solution from a given one where k was replaced with $k - 1 = l$. This proves the

second statement which said that if there is a solution for $k \geq 2$, then there is also a solution for k being replaced by $k - 1$.

Therefore we have proven that the equation $x^3+y^3 = u((1-\zeta)^k z)^3$ with u a unit, $k \geq 1$ an integer, x, y and z relatively coprime and xyz not a multiple of $1 - \zeta$ has no solution for $x, y, z \in \mathbb{Z}[\zeta]$.

Q.E.D.

We have therefore managed to prove Fermat's last theorem for the case $n = 3$. Our proof used a bit of number theory yet relied on two main ring theory statements. Namely having an exact description of the unit group $\mathbb{Z}[\zeta]^\times$ and knowing that the ring $\mathbb{Z}[\zeta]$ adheres to unique factorization. In addition to that we used a proof by infinite descent, something that is quite commonly used in number theory to disprove existence of a certain solution.

5 The ring $\mathbb{Z}[\zeta_4]$

In this section we define $\zeta := \zeta_4$ for notational convenience. One can actually compute to see that

$$\zeta_4 = e^{\frac{2\pi i}{4}} = i$$

and that therefore. $\zeta^2 = -1$ and $\zeta^3 = -i$. Following Equation 2.1 we then find that

$$\mathbb{Z}[\zeta] = \{a + b\zeta + c\zeta^2 + d\zeta^3 : a, b, c, d \in \mathbb{Z}\} = \{a + bi : a, b \in \mathbb{Z}\}$$

5.1 The units of $\mathbb{Z}[\zeta_4]$

To determine the units of $\mathbb{Z}[\zeta]$ we first aim to find a valid norm function from Definition 2.3. Then by following the logic of Example 2.1, when the norm function maps perfectly into $\mathbb{Z}$ all that we have to do is to solve the equation $N(\alpha) = \pm 1$. This then allows us to find all the units because

$$\mathbb{Z}[\zeta]^\times = \{\alpha : \exists \beta \in \mathbb{Z}[\zeta] \text{ such that } \alpha \cdot \beta = 1\} = \{\alpha : N(\alpha) = 1\}.$$

We define the following function:

$$N : \mathbb{Z}[\zeta] \to \mathbb{R}, N(\alpha) = \alpha \cdot \overline{\alpha}. \tag{5.1}$$

One easily determines that this function $N(\alpha)$ does satisfy the three conditions from Definition 2.3 and therefore this function is indeed a norm. We can simplify this to become

$$N(\alpha) = \alpha \cdot \overline{\alpha} = (a + bi)(a - bi) = a^2 + b^2 = |\alpha|^2$$

showing that in fact $N : \mathbb{Z}[\zeta] \to \mathbb{Z}$

Lemma 5.1 *The units of $\mathbb{Z}$ are given by $\{\pm 1, \pm i\}$.*

Proof: Because the norm function maps into $\mathbb{Z}$, for units it is true that $N(\alpha) = \pm 1$. Therefore to find all the units, we solve the equation $N(\alpha) = \pm 1$ where $\alpha \in \mathbb{Z}[\zeta]$. This is the same as solving $a^2 + b^2 = \pm 1$ for $a, b \in \mathbb{Z}$. It follows that the -1 case is impossible because squares are always positive numbers. Therefore we now look at the $+1$ case. Because $a^2 \geq 0$, we obtain that $b^2 \leq 1$ and therefore we obtain three possible values for b namely $b \in \{-1, 0, 1\}$.

1. The case $b = -1$ gives us $a^2 = 0$ and so $a = 0$. Therefore $\alpha = -i$.

2. The case $b = 0$ gives us $a^2 = 1$ and so $a = 1$ or $a = -1$. Therefore $\alpha = 1$ or $\alpha = -1$.
3. Lastly, the case $b = 1$ gives us $a^2 = 0$ and so $a = 0$. Therefore $\alpha = i$.

Hence we obtain that $\mathbb{Z}[\zeta]^\times = \{-i, 1, -1, i\} = \{\pm 1, \pm i\}$ which is what we intended to show.

Q.E.D.

5.2 Unique factorization in $\mathbb{Z}[\zeta_4]$

Next up we would like to determine whether or not we have unique factorization up to units in the ring $\mathbb{Z}[\zeta]$. Again by following Theorem 2.1, it is enough to show that $\mathbb{Z}[\zeta] = \mathbb{Z}[i]$ is a Euclidean domain.

Theorem 5.1 *The ring $\mathbb{Z}[\zeta] = \mathbb{Z}[i]$ is a Euclidean domain, hence a unique factorization domain.*

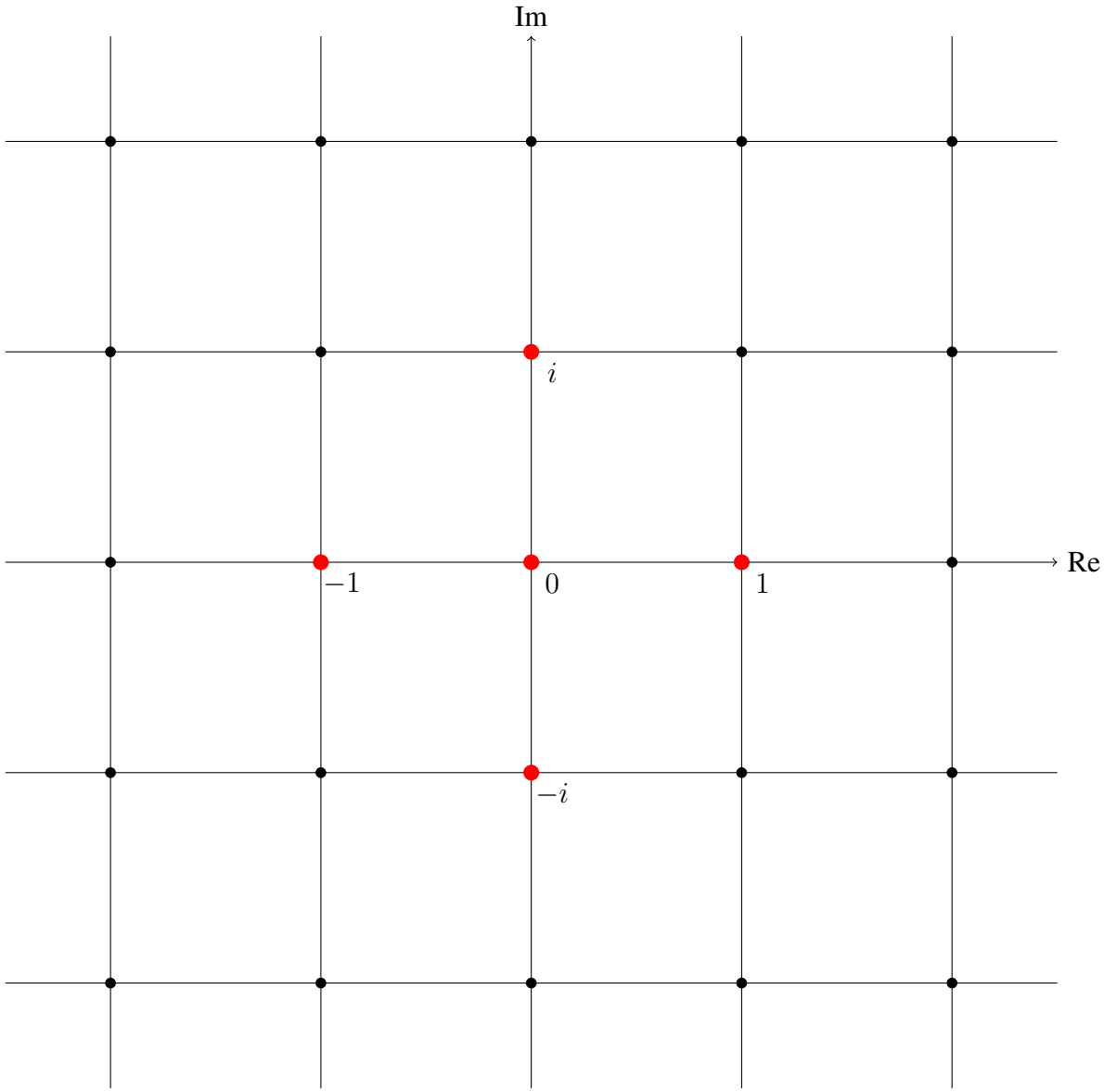
Proof: We work in similar fashion as for proving Theorem 3.1 which states that $\mathbb{Z}[\zeta_3]$ is a Euclidean domain. According to Definition 2.5 we need to show that there exists a map $\Phi : \mathbb{Z}[i]\backslash\{0\} \to \mathbb{N}$ such that given any $m, n \in \mathbb{Z}[i]$, there exists q and r such that $m = nq + r$ where either $r = 0$ or $\Phi(r) < \Phi(n)$. The claim that we make is that this works if we take the map $\Phi = N$ where N was the norm as described before.

Now a key observation is to note that $N(\alpha) = \alpha\overline{\alpha} = |\alpha|^2$ is just the standard Euclidean norm squared. This will come in handy later. Suppose we are given any $m, n \in \mathbb{Z}[i]$, let $q \in \mathbb{Z}[i]$ be such that there is some $r^* \in \mathbb{Q}[i]$ with

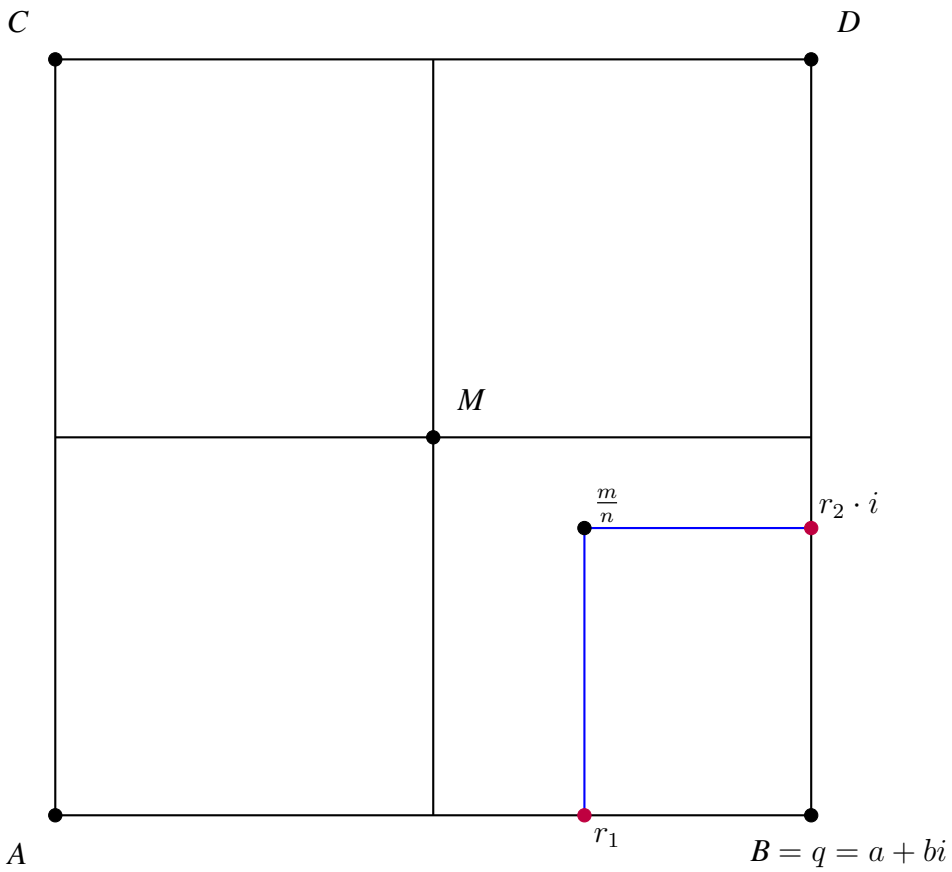
$$\frac{m}{n} = q + r^*.$$

First we need to define an extension of N into $\mathbb{Q}[\zeta]$, we pick the natural one where $N(\frac{a}{b}) := \frac{N(a)}{N(b)}$. This extension is well defined due to the multiplicity of N. We would then like to show that we can pick a certain value of q such that $N(\frac{m}{n} - q) < 1$, as then we can conclude the proof in similar style as we did for showing $\mathbb{Z}[\zeta_3]$ is Euclidean. Therefore it remains to show that $N(\frac{m}{n} - q) < 1$ and since the norm function is the euclidean norm squared, in words it means that q is at most distance 1 away from the point $\frac{m}{n}$.

For this we will observe the square structure of all the points in $\mathbb{Z}[i]$. Namely if we draw all the points that lay in $\mathbb{Z}[i]$, we observe that they basically form a bunch of horizontal lines parallel to the real axis spaced out by distance 1 and a bunch of vertical lines parallel to the imaginary axis spaced out by distance 1.



Now that we have all these squares we can see that all the corners of each square are precisely those points that are in $\mathbb{Z}[i]$. Note that if it happens to be that $\frac{m}{n} \in \mathbb{Z}[\zeta]$, then we let it be equal to q yielding that $r = 0$. Therefore we now suppose that $\frac{m}{n} \notin \mathbb{Z}[\zeta]$ and hence $r \neq 0$. Since $\frac{m}{n} \notin \mathbb{Z}[\zeta]$, we know that it lies either on the edge or inside one of these squares. We look closer into the square that contains the point $\frac{m}{n}$ and let one of the four corners be q to ensure that $q \in \mathbb{Z}[\zeta]$ and sort of close to $\frac{m}{n}$. Now we are going to define the following. We said that $\frac{m}{n}$ lies in $\mathbb{Q}[i]$, therefore we will define numbers $r_1, r_2 \in \mathbb{Q}$ such that $\frac{m}{n} = r_1 + r_2 i$. The geometrical interpretation of q was that it is one of the corners of the square containing $\frac{m}{n}$ but with our new way of writing we can pick the optimal corner. Namely we can find a and b in $\mathbb{Z}$ such that $q = a + bi$ and where $|r_1 - a| \leq \frac{1}{2}, |r_2 - b| \leq \frac{1}{2}$. Looking at the following picture motivates this reasoning and shows that we are indeed allowed to make this choice.



The point $\frac{m}{n}$ is located in one of the four regions enclosed in black lines. Whatever region it lies in, we take q to be the vertex of the main square that lies on the boundary of this region containing $\frac{m}{n}$. Now using all of the above one concludes the following key result.

$$\begin{aligned} N(\frac{m}{n} - q) &= N(r_1 + r_2 i - a - bi) \\ &= N((r_1 - a) + (r_2 - b)i) \\ &= (r_1 - a)^2 + (r_2 - b)^2 \\ &\leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2} < 1. \end{aligned}$$

Here we used that $-\frac{1}{2} \leq r_1 - a, r_2 - b \leq \frac{1}{2}$. The result we obtain is then that for any $m, n \in \mathbb{Z}[i]$ where n is nonzero there exists some $q \in \mathbb{Z}[i]$ such that $N\left(\frac{m}{n} - q\right) < 1$. Therefore there exists an $r \in \mathbb{Z}[i]$ such that $m = nq + r$ where $r = 0$ or $N(r) < N(n)$. This shows that $\mathbb{Z}[i]$ is indeed a Euclidean domain and hence a unique factorization domain by Theorem 2.1.

Q.E.D.

6 Proving Fermat's last theorem for $n = 4$

Now we are ready to tackle Fermat's equation. Just as in Theorem 1.2, we opt for proving a stronger result. Namely we prove that there are no nontrivial solutions to the equation $x^4 + y^4 = z^2$ over the ring $\mathbb{Z}[i]$. Just like the $n = 3$ case, we have two cases that we need to consider due to the following irreducible element.

Lemma 6.1 *The number $1 - i$ is irreducible in $\mathbb{Z}[i]$. That is the only divisors of $1 - i$ are itself, units and itself multiplied by units.*

Proof: Note that $N(1 + i) = N(1 + (-1) \cdot i) = 1^2 + (-1)^2 = 2$. Therefore if $1 - i = A \cdot B$ for some $A, B \in \mathbb{Z}[i]$ then it holds that $2 = N(1-i) = N(A \cdot B) = N(A) \cdot N(B)$ showing that either $N(A) = 1$ or $N(B) = 1$ and so respectively either A or B is a unit, showing that $1 - i$ is indeed irreducible in $\mathbb{Z}[i]$.

Q.E.D.

The importance from this irreducible element comes from that we are working with exponents 2 and 4 and that $2 = (1 - i)^2 \cdot i$. We start of with a small lemma checking some congruences that might seem random, however they will come back in the proof of the main theorem.

Lemma 6.2 *If $1 - i$ does not divide α where $\alpha \in \mathbb{Z}[i]$, then the following congruences hold.*

1. $\alpha^2 \equiv \pm 1 \pmod 4$
2. $\alpha^4 \equiv 1 \pmod 8$
3. $\alpha^4 \equiv 1 \pmod{(1 - i)^6}$

Proof: Let $\alpha = a + bi$ such that α is not divisible by $1 - i$. In total there are 4 equivalence classes $\pmod 2$ and they are $\overline{0}, \overline{1}, \overline{i}$ and $\overline{1 - i}$. Indeed one can check that these are distinct and together they form the whole set $\mathbb{Z}[i]$. Because α is not divisible by $1 - i$, α is also not divisible by 2 because $2 = i(1 - i)^2$. Therefore $\alpha \equiv 1 \pmod 2$ or $\alpha \equiv i \pmod 2$. It then follows that $\alpha^2 \equiv 1 \pmod 4$ or $\alpha^2 \equiv -1 \pmod 4$ after squaring α knowing the possible residues $\pmod 2$. This shows statement 1.

After squaring again and checking the possible classes now $\pmod 8$ we find that the only valid solution is $\alpha^4 \equiv 1 \pmod 8$. This is precisely the second statement. Finally the last statement instantly follows because $8 = -i(1 - i)^6$ and therefore $\alpha^4 \equiv 1 \pmod{(1 - i)^6}$.

Q.E.D.

Now that we have shown these important congruences, we can begin proving Fermat's last theorem for the case $n = 4$. We work along notes from the book[6]. We start of with the first case.

Lemma 6.3 *The equation $x^4+y^4 = z^2$ where xy is not divisible by $1-i$ has no nontrivial solutions in $\mathbb{Z}[i]$*

Proof: Because $1 - i$ is irreducible and xy is not divisible by it, we know that both x and y are not divisible by $1 - i$. From Lemma 6.2 we then know that $x^4 \equiv 1 \pmod{(1-i)^6}$ and also $y^4 \equiv 1 \pmod{(1-i)^6}$. Therefore, after reducing $x^4 + y^4 = z^2 \pmod{(1-i)^6}$ we find

$$z^2 = x^4 + y^4 \equiv 1 + 1 \pmod{(1-i)^6} \equiv 2 \pmod{(1-i)^6}.$$

Therefore, $z^2 = 2 + L \cdot (1-i)^6$ for some $L \in \mathbb{Z}[i]$. Because $2 = i(1-i)^2$ and i was found to be a unit we see that $(1-i)^2$ divides z^2. Therefore $1-i$ divides z because $1-i$ is irreducible. However, it also holds that $(1-i)^2$ does not divide z because $(1-i)^4$ does not divide 2, while 2 does divide z^2. This then allows us to write $z = (1-i)z^*$ where z^* is not divisible by $1 - i$. Because of this, from Lemma 6.2 it follows that $(z^*)^4 \equiv 1 \pmod{(1-i)^6}$.

Going back to our result where $z^2 \equiv 2 \pmod{(1-i)^6}$, using this new form of z and that $2 = i(1-i)^2$ results into

$$(1-i)^2(z^*)^2 = z^2 \equiv i(1-i)^2 \pmod{(1-i)^6}.$$

This means the following lines of equations:

$$\begin{aligned}
&(1-i)^2(z^*)^2 \equiv i(1-i)^2 \pmod{(1-i)^6} \\
&\Rightarrow (1-i)^2(z^*)^2 = i(1-i)^2 + K(1-i)^6 \\
&\Rightarrow (z^*)^2 = i + K(1-i)^4 \\
&\Rightarrow (z^*)^4 = (-1) + 2 \cdot i \cdot K(1-i)^4 + K^2(1-i)^8 \\
&\Rightarrow (z^*)^4 = -1 + (i(1-i)^2) \cdot i \cdot K(1-i)^4 + K^2(1-i)^8 \\
&\Rightarrow (z^*)^4 = -1 - K(1-i)^6 + K^2(1-i)^8 \\
&\Rightarrow (z^*)^4 \equiv -1 \pmod{(1-i)^6}.
\end{aligned}$$

So we previously obtained the expression $(z^*)^4 \equiv 1 \pmod{(1-i)^6}$ and now we also find $(z^*)^4 \equiv -1 \pmod{(1-i))^6}$. Subtracting these two lines results in $2 \equiv 0 \pmod{(1-i)^6}$ which is a contradiction because $(1-i)^6$ does not divide 2. This then proves the statement that the equation $x^4 + y^4 = z^2$ where xy is not divisible by $1 - i$ has no nontrivial solution in $\mathbb{Z}[i]$.

Q.E.D.

To now prove the second case, just like for $n = 3$ we are actually going to prove a stronger result out of which the desired result follows. This time we look at the equation

$$u(1-i)^{4n}x^4 + y^4 = z^2 \tag{6.1}$$

where $n \geq 1$ is an integer, u is a unit and x, y, z are pairwise relatively prime where none of them is divisible by $1 - i$. Notice that it is quite similar in form to Equation 4.1 we investigated during the

$n = 3$ case. If this equation has no solutions over $\mathbb{Z}[i]$ then we are done because of the following. Note that in Lemma 6.3 we looked at the case where xy is not divisible by $1 - i$. For the second case we then need to look at the case where xy is divisible by $1 - i$. Because $1 - i$ is irreducible and we want to preserve relative coprimality between x, y and z we assume x to be divisible by $1 - i$, allowing us to write $x = (1 - i)^k \cdot x^*$ where x^* is not divisible by $1 - i$. Putting this new form into the equation $x^4 + y^4 = z^2$, where we will put $n = k \geq 1$ and $u = 1$, will result in $1 \cdot (1 - i)^{4k}(x^*)^4 + y^4 = z^2$ which attains the form of Equation 6.1. Hence showing this has no solutions is satisfactory.

Theorem 6.1 *The equation $u(1 - i)^{4n}x^4 + y^4 = z^2$ for u a unit, $n \geq 1$ an integer, x, y and z relatively co-prime and xyz not divisible by $1 - i$ has no solution for $x, y, z \in \mathbb{Z}[i]$.*

Proof: Just like the proof of Theorem 6.1, we are going to follow a similar strategy of infinite descent. We aim to prove the following two statements from which we can conclude that no solution exists.

1. If a solution exists, then $n \geq 2$.
2. If there is a solution for $n \geq 2$, then there is also a solution for n being replaced by $n - 1$.

If these statements hold, then we can indeed conclude that there are no solutions to $u(1-i)^{4n}x^4 + y^4 = z^2$ over $\mathbb{Z}[i]$. We begin with the proof of the first statement, hence suppose a solution exists for some $n \geq 1$ and suitable x, y, z and u. Then we of course have the equation $u(1-i)^{4n}x^4+y^4 = z^2$ holding. Then it is also true that $u(1 - i)^{4n}x^4 + y^4 - 1 = z^2 - 1$. Since we assumed that y is not divisible by $1 - i$. From Lemma 6.2, it holds that $y^4 \equiv 1 \pmod{(1 - i)^6}$. Therefore we see that

$$u(1 - i)^{4n}x^4 + y^4 - 1 \equiv 0 \pmod{(1 - i)^4}$$

because $u(1 - i)^{4n}x^4 \equiv 0 \pmod{(1 - i)^4}$ and $y^4 - 1 \equiv 0 \pmod{(1 - i)^6} \Rightarrow y^4 - 1 \equiv 0 \pmod{(1 - i)^4}$. This then implies that $z^2 - 1 \equiv 0 \pmod{(1 - i)^4} \Rightarrow z^2 \equiv 1 \pmod{(1 - i)^4}$. Now because we also assumed z to not be divisible by $1 - i$, from the proof of Lemma 6.2 it holds that $z \equiv i \pmod{(1 - i)^2}$ or $z \equiv 1 \pmod{(1 - i)^2}$. In the first case it means that $z^2 \equiv -1 \pmod{(1 - i)^4}$ which combined with the result $z^2 \equiv 1 \pmod{(1 - i)^4}$ yields that $2 \equiv 0 \pmod{(1 - i)^4}$ which is a contradiction because 2 is not divisible by $(1 - i)^4$. Therefore it holds that $z \equiv 1 \pmod{(1 - i)^2}$ which means that $z = 1 + K(1 - i)^2$ for some $K \in \mathbb{Z}[i]$. One then observes that adding 1 to both sides yields

$$z + 1 = 2 + K(1 - i)^2 = (K + i)(1 - i)^2.$$

We now aim for the result that $1 - i$ divides $K(K + i)$ for all $K \in \mathbb{Z}[i]$. If K is such that it is divisible by $1 - i$ then we are done, if however K is not divisible by $1 - i$ then

$$K \equiv 1 \pmod{1 - i} \equiv i \pmod{1 - i} \equiv i - 2i \pmod{1 - i} \equiv -i \pmod{1 - i}.$$

Therefore $K + i$ is divisible by $1 - i$, which proves that $K(K + i)$ is divisible by $1 - i$ for all $K \in \mathbb{Z}[i]$. Therefore we can see that the following holds

$$\begin{aligned} &z - 1 = K(1 - i)^2, z + 1 = (K + i)(1 - i)^2 \\ &\Rightarrow (z - 1)(z + 1) = (K(1 - i)^2)((K + i)(1 - i)^2) \\ &\Rightarrow z^2 - 1 = K(K + i)(1 - i)^4 \\ &\Rightarrow z^2 - 1 \equiv 0 \pmod{(1 - i)^5} \end{aligned}$$

The last line holds because $K(K + i)$ was shown to be a multiple of $1 - i$.

Since $u(1 - i)^{4n}x^4 + y^4 - 1 = z^2 - 1$ and the right hand side was shown to be congruent to $0 \pmod{(1-i)^5}$, the left side must satisfy the same. However note that it was shown that $y^4 - 1 \equiv 0 \pmod{(1 - i)^6}$ which implies that $u(1 - i)^{4n}x^4 \equiv 0 \pmod{(1 - i)^5}$. Now since u is a unit and x is not divisible by $1 - i$, it means that $(1 - i)^{4n}$ should be divisible by $(1 - i)^5$, this then shows that indeed $n \geq 2$ because if n were to equal 1, the left side is only divisible by $(1 - i)^4$ but not by the fifth power. This proves the first statement which said that if a solution exists, then $n \geq 2$.

To now proof the second statement, we take a solution for a certain $n \geq 2$ and try to construct a solution where n is now replaced by $n - 1$. Going back to our equation, we see that we can rewrite it as

$$u(1 - i)^{4n}x^4 + y^4 = z^2 \Rightarrow u(1 - i)^{4n}x^4 = z^2 - y^4 = (z - y^2)(z + y^2).$$

Because the left side is divisible by $1-i$, so must at least one of the terms of $(z-y^2)(z+y^2)$ be then. Now observe that $z + y^2 - (z - y^2) = 2y^2$ is a multiple of $(1 - i)^2$, since $2 = i(1 - i)^2$, but not of a higher power of $1-i$. Therefore both $z-y^2$ and $z+y^2$ should be divisible by $1-i$. As $u(1-i)^{4n}x^4$ is divisible by $(1 - i)^4$ it then necessarily means that both $z - y^2$ and $z + y^2$ are actually multiples of $(1 - i)^2$. Notice however that $z - y^2$ and $z + y^2$ can not have a higher greatest common divisor because this greatest common divisor should divide their difference too which is equal to $2y^2$ as seen above. However y and z are relatively prime, therefore the gcd$(z - y^2, z + y^2) = (1 - i)^2$.

Using this, without loss of generality, we rewrite $z - y^2$ and $z + y^2$ in the following way:

- $z - y^2 = (1 - i)^2 a$
- $z + y^2 = (1 - i)^{4n-2} b$

Here $a, b \in \mathbb{Z}[i]$ such that they are relatively co-prime and not divisible by $1 - i$. Looking back at our original equation yields then that

$$u(1 - i)^{4n}x^4 = (z - y^2)(z + y^2) = (1 - i)^{4n}ab \Rightarrow ux^4 = ab.$$

From Theorem 5.1 it followed that $\mathbb{Z}[i]$ is a unique factorization domain. Therefore we notice that if the product of two relatively co-prime numbers is a fourth power, each of those two numbers individually equals a fourth power multiplied by a unit. We therefore define

- $a := vp^4$
- $b := wq^4$

where v, w are units in $\mathbb{Z}[i]$ and p, q are numbers in $\mathbb{Z}[i]$ that are relatively co-prime and are not divisible by $1 - i$. Using this way of writing we obtain the following equations.

1. $z - y^2 = (1 - i)^2 a = v(1 - i)^2 p^4$
2. $z + y^2 = (1 - i)^{4n-2} b = w(1 - i)^{4n-2} q^4$

If we take the second equation and subtract the first equation from it we obtain

$$\begin{aligned}
&(z + y^2) - (z - y^2) = w(1 - i)^{4n-2} q^4 - v(1 - i)^2 p^4 \\
&\Rightarrow 2y^2 = w(1 - i)^{4n-2} q^4 - v(1 - i)^2 p^4 \\
&\Rightarrow i(1 - i)^2 y^2 = w(1 - i)^{4n-2} q^4 - v(1 - i)^2 p^4 \\
&\Rightarrow iy^2 = w(1 - i)^{4n-4} q^4 - vp^4 \\
&\Rightarrow y^2 = -iw(1 - i)^{4(n-1)} q^4 + ivp^4.
\end{aligned}$$

After making the substitution $-iw = w^*$ and $iv = v^*$, note since v and w are units then also v^* and w^* are, just for writing it simpler we obtain the equation

$$w^*(1 - i)^{4(n-1)} q^4 + v^* p^4 = y^2. \tag{6.2}$$

This looks a lot like our original equation $u(1 - i)^{4n} x^4 + y^4 = z^2$ already where n is now replaced by $n - 1$. All that is left to show is then that $v^* = 1$.

Because $n \geq 2$ it is true that $(1-i)^4$ divides $w^*(1-i)^{4(n-1)} q^4$ and therefore it also divides $y^2 - v^* p^4$. However as $1 - i$ does not divide y, it can also not divide p. From Lemma 6.2 we see that then $p^4 \equiv 1 \pmod{(1 - i)^6}$. Therefore $p^4 = 1 + L(1 - i)^6$ for some $L \in \mathbb{Z}[i]$. Using this we find that $(1 - i)^4$ divides $y^2 - v^* p^4 = y^2 - v^*(1 + L(1 - i)^6) = y^2 - v^* - v^* L(1 - i)^6$. Therefore $y^2 - v^*$ is divisible by $(1 - i)^4$. However since y is not divisible by $1 - i$, from Lemma 6.2 it follows that $y^4 \equiv 1 \pmod{(1 - i)^6}$. Therefore, $(1 - i)^6$ divides $y^4 - 1 = (y^2 - 1)(y^2 + 1)$. From the same reasoning that was used to determine that $\gcd(z - y^2, z + y^2) = (1 - i)^2$ one finds that $\gcd(y^2 - 1, y^2 + 1) = (1 - i)^2$. Hence we conclude that, since the product of these two terms is divisible by $(1 - i)^6$ and since one of the two terms only contains an $(1 - i)^2$ factor, the other term contains an $(1 - i)^4$ factor. So either $y^2 - 1 \equiv 0 \pmod{(1 - i)^4}$ or $y^2 + 1 \equiv 0 \pmod{(1 - i)^4}$. This then implies that $y^2 \equiv \pm 1 \pmod{(1-i)^4}$. Combining with $y^2 \equiv v^* \pmod{(1-i)^4}$ and that v^* is a unit it means that $v^* = \pm 1$.

If $v^* = 1$ we are done, if it equals -1 we can multiply the whole Equation 6.2 by -1 to obtain

$$-w^*(1-i)^{4(n-1)}q^4 + 1 \cdot p^4 = -y^2 = (iy)^2$$

which is still in valid form of our original equation. Therefore we can indeed say that $v^* = 1$ meaning that we have found the relation that

$$w^*(1-i)^{4(n-1)}q^4 + p^4 = y^2$$

where w^* is a unit, $n - 1 \geq 1$ an integer, p, q and y relatively coprime and pqy not divisible by $1 - i$. This is exactly equal to Equation 6.1, however we have now constructed a valid solution from a given one where n was replaced with $n - 1$. This proves the second statement which said that if there is a solution for $n \geq 2$, then there is also a solution for n being replaced by $n - 1$.

Therefore we have proven that the equation $u(1-i)^{4n}x^4 + y^4 = z^2$ with u a unit, $n \geq 1$ an integer, x, y and z relatively co-prime and xyz not a multiple of $1 - i$ has no solution for $x, y, z \in \mathbb{Z}[i]$.

Q.E.D.

We have now proven Fermat's last theorem for the $n = 4$ again. Just like in the first proof done in Theorem 1.2, we used a method of infinite descent of some sorts. The difference is that adapting the method from ring theory to other exponents is simpler than adapting the method that relies purely on number theory. This is because for the ring theory approach we only have to change a few parts. Notice the similarity of to the proof of Fermat's last theorem for $n = 3$ done in Theorem 4.1. During the proof of Theorem 6.1 we relied on our clear description of the unit group $\mathbb{Z}[\zeta]^\times$ and on the fact that $\mathbb{Z}[\zeta]$ adheres to unique factorization.

7 The ring $\mathbb{Z}[\zeta_5]$

In this section we define $\zeta := \zeta_5$ for notational convenience. Following Equation 2.1 we find that $\mathbb{Z}[\zeta] = \{a + b\zeta + c\zeta^2 + d\zeta^3 : a, b, c, d \in \mathbb{Z}\}$. For the readers interest, the exact value of ζ is given by

$$\zeta = \frac{-1 + \sqrt{5}}{2} + i\sqrt{\frac{5 + \sqrt{5}}{8}}.$$

7.1 The units of $\mathbb{Z}[\zeta_5]$

To determine the units of $\mathbb{Z}[\zeta]$ we first aim to find a valid norm function from Definition 2.3. Then by following the logic of Example 2.1, when the norm function maps perfectly into $\mathbb{Z}$ all that we have to do is to solve the equation $N(\alpha) = \pm 1$. This then allows us to find all the units because

$$\mathbb{Z}[\zeta]^\times = \{\alpha : \exists \beta \in \mathbb{Z}[\zeta] \text{ such that } \alpha \cdot \beta = 1\} = \{\alpha : N(\alpha) = 1\}.$$

By looking at our previous results with ζ_3 and ζ_4 we are motivated to try the following norm function:

$$N : \mathbb{Z}[\zeta] \to \mathbb{R}, N(\alpha) = \alpha \cdot \overline{\alpha}.$$

One can check that the function $N(\alpha)$ indeed satisfies the three properties from Definition 2.3 and therefore this function is indeed a norm. The problem however now is that this function N does not map into $\mathbb{Z}$ but actually into something bigger. We can compute, for example, that $N(\zeta^2 + 1) \approx 0.6180$ or another example $N(\zeta^4 + 2\zeta^2 - \zeta + 2) \approx 0.8208$. There are a lot of other examples like this. This shows that, unlike in the cases for ζ_3 and ζ_4, our norm function does not map perfectly into $\mathbb{Z}$. Therefore we can not say that α is a unit if and only if $N(\alpha) = \pm 1$. Hence for ζ_5 we need a different norm function.

We skip some of the computations as they require a lot of algebraic manipulations but one can verify by doing the computations themselves. Define the linear function

$$\sigma_i : \mathbb{Z}[\zeta] \to \mathbb{Z}[\zeta], \sigma_i(\zeta) = \zeta^i.$$

It is linear in the sense that $\sigma_i(a + b\zeta + c\zeta^2 + d\zeta^3) = a + b\sigma_i(\zeta) + c\sigma_i(\zeta)^2 + d\sigma_i(\zeta)^3 = a + b\zeta^i + c\zeta^{2i} + d\zeta^{3i}$. We define our norm to be

$$N : \mathbb{Z}[\zeta_5] \to \mathbb{Z}, N(\alpha) = \sigma_1(\alpha) \cdot \sigma_2(\alpha) \cdot \sigma_3(\alpha) \cdot \sigma_4(\alpha). \tag{7.1}$$

One can determine that this function $N(\alpha)$ now does satisfy the three conditions from Definition 2.3 and therefore, this function is indeed a norm. Given a number $\alpha = a + b\zeta + c\zeta^2 + d\zeta^3$ where $a, b, c, d \in \mathbb{Z}$ we define the following numbers:

$$\begin{cases} q = a^2 + b^2 + c^2 + d^2 \\ r = \quad ab + bc + cd \\ s = \quad ac + ad + bd \end{cases}$$

Then, after expanding and simplifying, one finds the following expression for the norm:

$$N(\alpha) = N(a + b\zeta + c\zeta^2 + d\zeta^3) = \frac{1}{4}\left((2q - r - s)^2 - 5(r - s)^2\right). \tag{7.2}$$

This is indeed a number in $\mathbb{Z}$ so in fact $N : \mathbb{Z}[\zeta] \to \mathbb{Z}$ this time. Now to find units we would like to solve the equation $N(\alpha) = \pm 1$ like we did before. This time unfortunately it is very unpractical due to the difficulty of this equation. Instead we therefore aim for a different approach using methods from group theory to describe the group $\mathbb{Z}[\zeta]^\times$.

7.1.1 A useful map

To figure out what the units are we construct a series of ring homomorphisms that are going to help us determine all of the units in $\mathbb{Z}[\zeta]$. We saw that any element in the ring $\beta \in \mathbb{Z}[\zeta]$ can be written as $\beta = a + b\zeta + c\zeta^2 + d\zeta^3$ for some integers a, b, c, d. Therefore we have the isomorphic relation $\mathbb{Z}^4 \cong \mathbb{Z}[\zeta]$ as addition groups. To make things simpler instead of writing each element $\beta \in \mathbb{Z}[\zeta]$ as $\beta = a + b\zeta + c\zeta^2 + d\zeta^3$, we will write our elements as $g(\zeta)$ where $g(x)$ is some polynomial of degree 3 with integer coefficients. This is just for our notational convenience as now we start with constructing the homomorphisms. Define

$$\Phi : \mathbb{Z}[\zeta] \to \mathbb{C} \times \mathbb{C}, \Phi(g(\zeta)) := (g(\zeta), g(\zeta^2)).$$

Note that the function g stays the same but we do replace ζ by ζ in the first coordinate and by ζ^2 in the second coordinate. For example, $\Phi(1 + 2\zeta + \zeta^3) = (1 + 2\zeta + \zeta^3, 1 + 2\zeta^2 + \zeta^6) = (1 + 2\zeta + \zeta^3, 1 + \zeta + 2\zeta^2)$ as $\zeta^5 = 1$.

Lemma 7.1 *The map Φ defined above is a ring homomorphism.*

Proof: We prove this by using the Definition of a ring homomorphism 2.2, namely by showing the three properties it must satisfy.

1. To show is $\Phi(a+b) = \Phi(a) + \Phi(b), \forall a, b \in \mathbb{Z}[\zeta]$. Since $a, b \in \mathbb{Z}[\zeta]$, let g_1 and g_2 be such that $g_1(\zeta) = a, g_2(\zeta) = b$. Define the function $h_1(\zeta) = g_1(\zeta) + g_2(\zeta)$, this is just the number $a + b$ but then written with the function notation. Then

$$\begin{aligned}\Phi(a+b) &= \Phi(g_1(\zeta) + g_2(\zeta)) \\ &= \Phi(h_1(\zeta)) = (h_1(\zeta), h_1(\zeta^2)) \\ &= (g_1(\zeta) + g_2(\zeta), g_1(\zeta^2) + g_2(\zeta^2)) \\ &= (g_1(\zeta), g_1(\zeta^2)) + (g_2(\zeta), g_2(\zeta^2)) \\ &= \Phi(g_1(\zeta)) + \Phi(g_2(\zeta)) = \Phi(a) + \Phi(b).\end{aligned}$$

   This shows that $\Phi(a+b) = \Phi(a) + \Phi(b), \forall a, b \in \mathbb{Z}[\zeta]$.

2. To show is $\Phi(a \cdot b) = \Phi(a) \cdot \Phi(b), \forall a, b \in \mathbb{Z}[\zeta]$. Define the function $h_2(\zeta) = g_1(\zeta) \cdot g_2(\zeta)$, this is just the number $a \cdot b$ but then written with the function notation. Then

$$\begin{aligned}\Phi(a \cdot b) &= \Phi(g_1(\zeta) \cdot g_2(\zeta)) \\ &= \Phi(h_2(\zeta)) = (h_2(\zeta), h_2(\zeta^2)) \\ &= (g_1(\zeta) \cdot g_2(\zeta), g_1(\zeta^2) \cdot g_2(\zeta^2)) \\ &= (g_1(\zeta), g_1(\zeta^2)) \cdot (g_2(\zeta), g_2(\zeta^2)) \\ &= \Phi(g_1(\zeta)) \cdot \Phi(g_2(\zeta)) = \Phi(a) \cdot \Phi(b).\end{aligned}$$

   This shows that $\Phi(a \cdot b) = \Phi(a) \cdot \Phi(b), \forall a, b \in \mathbb{Z}[\zeta]$. Note that in $\mathbb{C}^2$ the multiplication is defined as $(a, b) \cdot (c, d) := (a \cdot c, b \cdot d)$ which is why the fourth line holds.

3. To show is $\Phi(1_{\mathbb{Z}[\zeta]}) = 1_{\mathbb{C}^2}$. Note that $1_{\mathbb{Z}[\zeta]} = 1$ and that $1_{\mathbb{C}^2} = (1, 1)$. Then by our notation we have that $g(\zeta) = 1$ and so

$$\begin{aligned}\Phi(1_{\mathbb{Z}[\zeta]}) &= \Phi(1) = \Phi(g(\zeta)) \\ &= (g(\zeta), g(\zeta^2)) = (1, 1) = 1_{\mathbb{C}^2}\end{aligned}$$

   This shows that $\Phi(1_{\mathbb{Z}[\zeta]}) = 1_{\mathbb{C}^2}$.

Therefore the map $\Phi : \mathbb{Z}[\zeta] \to \mathbb{C} \times \mathbb{C}, \Phi(g(\zeta)) := (g(\zeta), g(\zeta^2))$ is indeed a ring homomorphism.

Q.E.D.

Lemma 7.2 *The map Φ defined above is injective*

Proof: To prove this we show that the kernel of the map Φ is equal to $\{0\}$. Recall that the kernel is defined as

$$\ker(\Phi) := \{\beta \in \mathbb{Z}[\zeta] : \Phi(\beta) = 0_{\mathbb{C}^2} = (0, 0)\}.$$

So suppose $\beta \in \ker(\Phi)$, since $\beta \in \mathbb{Z}[\zeta]$ we can find some function g again such that $\beta = g(\zeta)$. Because β is in the kernel of Φ it is true that $\Phi(\beta) = 0$, therefore $(g(\zeta), g(\zeta^2)) = (0,0) \Rightarrow g(\zeta) = g(\zeta^2) = 0$. However note that ζ and ζ^2 have the same minimal polynomial over the integers, namely $f(x) = x^4 + x^3 + x^2 + x + 1$. Because g is of degree ≤ 3 and has integer coefficients, it is impossible for a nonzero polynomial of this degree to have ζ and ζ^2 as a root. Therefore there is only one polynomial of degree ≤ 3 that has ζ and ζ^2 as roots and it is $g(\zeta) = 0 \Rightarrow \beta = 0$. So if $\beta \in \ker(\Phi)$, then $\beta = 0$ which shows that $\ker(\Phi) = \{0\}$. Hence Φ is an injective ring homomorphism.

Q.E.D.

We defined the norm on $\mathbb{Z}[\zeta]$ as in Equation 7.1. We can also see that this map on $\mathbb{Z}[\zeta]$ rotates through the powers of ζ, replacing it by ζ^i for each σ_i. Writing β as $g(\zeta)$ shows the following due to the linearity of each σ_i:

$$\sigma_i(\beta) = \sigma_i(g(\zeta)) = g(\sigma_i(\zeta)) = g(\zeta^i).$$

Therefore we obtain the relation that

$$\begin{aligned} N(g(\zeta)) &= g(\zeta) \cdot g(\zeta^2) \cdot g(\zeta^3) \cdot g(\zeta^4) \\ &= g(\zeta) \cdot g(\zeta^2) \cdot g(\overline{\zeta^2}) \cdot g(\overline{\zeta}) \\ &= g(\zeta) \cdot g(\zeta^2) \cdot \overline{g(\zeta^2)} \cdot \overline{g(\zeta)} \\ &= |g(\zeta)|^2 \cdot |g(\zeta^2)|^2 \end{aligned}$$

Note that finding units in $\mathbb{Z}[\zeta]$ equals solving the equation $N(g(\zeta)) = |g(\zeta)|^2 \cdot |g(\zeta^2)|^2 = \pm 1$. Because the left side is a square of a real number, it is never equal to a negative number. Therefore $N(\beta) = -1$ has no solutions so we only need to look at $N(\beta) = 1$. We shall define the following maps that help us with this goal and ultimately allows us to describe all the units in $\mathbb{Z}[\zeta]$.

- $\phi_1 : \mathbb{Z}[\zeta]^\times \to \mathbb{C}^\times \times \mathbb{C}^\times, \phi_1(\beta) = \phi_1(g(\zeta)) := (g(\zeta), g(\zeta^2))$.
- $\phi_2 : \mathbb{C}^\times \times \mathbb{C}^\times \to \mathbb{R}_{>0} \times \mathbb{R}_{>0}, \phi_2((z,w)) := (|z|, |w|)$.
- $\phi_3 : \mathbb{R}_{>0} \times \mathbb{R}_{>0} \to \mathbb{R} \times \mathbb{R}, \phi_3((p,q)) := (\ln(p), \ln(q))$.

First note that each of these maps are well defined. Maps ϕ_2 and ϕ_3 are clearly well defined and because $\phi_1 = \Phi|_{\mathbb{Z}[\zeta]^\times}$, ϕ_1 is also a well defined group homomorphism because Φ is an injective ring homomorphism by Lemma 7.2. Now suppose some element β is given in $\mathbb{Z}[\zeta]^\times$, observe that after putting it into ϕ_1, ϕ_2 and ϕ_3 respectively we obtain

$$\begin{aligned}\phi_3(\phi_2(\phi_1(\beta))) &= \phi_3(\phi_2(\phi_1(g(\zeta))))\\ &= \phi_3(\phi_2((g(\zeta), g(\zeta^2))))\\ &= \phi_3((|g(\zeta)|, |g(\zeta^2)|))\\ &= (\ln(|g(\zeta)|), \ln(|g(\zeta^2)|)).\end{aligned}$$

Now because β is a unit in $\mathbb{Z}[\zeta]$ it holds that $N(\beta) = 1$. Therefore $N(\beta) = N(g(\zeta)) = |g(\zeta)|^2 \cdot |g(\zeta^2)|^2 = 1$. Taking logarithms on both sides yields

$$\begin{aligned}&|g(\zeta)|^2 \cdot |g(\zeta^2)|^2 = 1\\ \Rightarrow &\ln(|g(\zeta)|^2 \cdot |g(\zeta^2)|^2) = \ln(1) = 0\\ \Rightarrow &2 \cdot \ln(|g(\zeta)|) + 2 \cdot \ln(|g(\zeta^2)|) = 0\\ \Rightarrow &\ln(|g(\zeta)|) = -\ln(|g(\zeta^2)|).\end{aligned}$$

Observe then that for units β, we have that

$$\phi_3(\phi_2(\phi_1(\beta))) = (\ln(|g(\zeta)|), \ln(|g(\zeta^2)|)) = (\ln(|g(\zeta)|), -\ln(|g(\zeta)|)).$$

This means that all the units of $\mathbb{Z}[\zeta]$ are located on the line $x + y = 0$ in $\mathbb{R}^2$. For notational convenience let $\psi : \mathbb{Z}[\zeta]^\times \to \mathbb{R} \times \mathbb{R}$ be equal to the composition $\phi_3 \circ \phi_2 \circ \phi_1$.

Lemma 7.3 *The map $\psi : \mathbb{Z}[\zeta]^\times \to \mathbb{R} \times \mathbb{R}$ is a group homomorphism.*

Proof: First we start by giving the group laws of the groups in question such that all operations are clear. The maps in question look like the following:

$$\mathbb{Z}[\zeta]^\times \xrightarrow{\phi_1} (\mathbb{C}^\times \times \mathbb{C}^\times) \xrightarrow{\phi_2} (\mathbb{R}_{>0} \times \mathbb{R}_{>0}) \xrightarrow{\phi_3} (\mathbb{R} \times \mathbb{R}).$$

These groups come with the following structures on them:

1. The group structure on $\mathbb{Z}[\zeta]^\times$ is standard multiplication where the unit element is 1.
2. The group structure on $\mathbb{C}^\times \times \mathbb{C}^\times$ is elementwise standard multiplication, so $(a, b) \times (c, d) = (ac, bd)$, and the unit element is $(1, 1)$.
3. The group structure on $\mathbb{R}_{>0} \times \mathbb{R}_{>0}$ is elementwise standard multiplication, so $(a, b) \times (c, d) = (ac, bd)$, and the unit element is $(1, 1)$.
4. The group structure on $\mathbb{R} \times \mathbb{R}$ is elementwise standard addition, so $(a, b) \times (c, d) = (a + c, b + d)$, and the unit element is $(0, 0)$.

Knowing this we can proceed. In order to show that ψ is a homomorphism it is enough to show that $\psi(a \times_{\mathbb{Z}[\zeta]^\times} b) = \psi(a) \times_{\mathbb{R}\times\mathbb{R}} \psi(b)$ for all elements $a, b \in \mathbb{Z}[\zeta]^\times$. For notational convenience we now write $\times_{\mathbb{Z}[\zeta]^\times}$ as $\cdot$ and $\times_{\mathbb{R}\times\mathbb{R}}$ as $+$ since these are the structures on the respective groups. Let a, b we arbitrary in $\mathbb{Z}[\zeta]^\times$. From our notation from before it is possible to write $a = g_1(\zeta)$ and $b = g_2(\zeta)$ where g_1 and g_2 are polynomials of degree ≤ 3 in ζ with integer coefficients. We also define $h(\zeta) := g_1(\zeta) \cdot g_2(\zeta)$. This is just the number $a \cdot b$ with the function notation. It then follows that we have

$$\begin{aligned}
\psi(a \cdot b) &= \psi(g_1(\zeta) \cdot g_2(\zeta)) \\
&= \psi(h(\zeta)) = \phi_3(\phi_2(\phi_1(h(\zeta)))) \\
&= (\ln(|h(\zeta)|), \ln(|h(\zeta^2)|)) \\
&= (\ln(|g_1(\zeta) \cdot g_2(\zeta)|), \ln(|g_1(\zeta^2) \cdot g_2(\zeta^2)|)) \\
&= (\ln(|g_1(\zeta)| \cdot |g_2(\zeta)|), \ln(|g_1(\zeta^2)| \cdot |g_2(\zeta^2)|)) \\
&= (\ln(|g_1(\zeta)|) + \ln(|g_2(\zeta)|), \ln(|g_1(\zeta^2)|) + \ln(|g_2(\zeta^2)|)) \\
&= (\ln(|g_1(\zeta)|), \ln(|g_1(\zeta^2)|)) + (\ln(|g_2(\zeta)|), \ln(|g_2(\zeta^2)|)) \\
&= \phi_3(\phi_2(\phi_1(g_1(\zeta)))) + \phi_3(\phi_2(\phi_1(g_2(\zeta)))) \\
&= \psi(g_1(\zeta)) + \psi(g_2(\zeta)) = \psi(a) + \psi(b)
\end{aligned}$$

This shows that $\psi(a \cdot b) = \psi(a) + \psi(b), \forall a, b \in \mathbb{Z}[\zeta]^\times$ proving that indeed $\psi : \mathbb{Z}[\zeta]^\times \to \mathbb{R} \times \mathbb{R}$ is a group homomorphism.

Q.E.D.

Before Lemma 7.3, it was shown that all the units of $\mathbb{Z}[\zeta]$ get mapped onto the line $x + y = 0$ in $\mathbb{R}^2$ under our map ψ. This line is a subgroup of $\mathbb{R}^2$ because of the group structure on $\mathbb{R}^2$. This is because the unit element $(0, 0)$ is on this line. Furthermore, adding two points on this line, $(a, -a)$ and $(b, -b)$, yields point $(a + b, -(a + b))$ which is also on the line $x + y = 0$. Finally each point $(a, -a)$ has an inverse given by $(-a, a)$ which also lies on $x + y = 0$.

The map ψ maps perfectly onto the line $x + y = 0$, because it is a homomorphism we have that the image $\psi(\mathbb{Z}[\zeta]^\times)$ forms a subgroup of the line $x + y = 0$. In order to then describe the group of all units, we are interested in finding out what type of group this image is as that allows us to nicely describe all the units.

Theorem 7.1 *the map ψ has a discrete image. In other words the intersection of $\psi(\mathbb{Z}[\zeta]^\times)$ and a ball of radius r centered at the origin contains finitely many points for all values of r.*

Proof: First let us describe a box B around the origin in the following way. The box is defined as $B := \{(x, y) \in \mathbb{R} || x| < k, |y| < k\}$. What we now aim to show that in box B there are only finitely many units $\forall k \in \mathbb{R}_{>0}$ as this shows the image of ψ is indeed discrete. The construction with the box is equivalent to the construction with a ball because the image of ψ is located on the line $x + y = 0$ in $\mathbb{R}^2$, therefore we use the box. Recall that $\psi(g(\zeta)) = (\ln(|g(\zeta)|), \ln(|g(\zeta^2)|))$. Therefore

$$\begin{aligned}\psi(\beta) \in B &\Rightarrow \psi(\beta) \in \{(x,y) \in \mathbb{R} || x| < k, |y| < k\} \\ &\Rightarrow (\ln(|g(\zeta)|), \ln(|g(\zeta^2)|)) \in \{(x,y) \in \mathbb{R} : |x| < k, |y| < k\} \\ &\Rightarrow |\ln(|g(\zeta)|)| < k \text{ and } |\ln(|g(\zeta^2)|)| < k \\ &\Rightarrow \ln(|g(\zeta)|) < k \text{ and } \ln(|g(\zeta^2)|) < k \\ &\Rightarrow |g(\zeta)| < e^k \text{ and } |g(\zeta^2)| < e^k.\end{aligned}$$

Define the disc $D_k := \{\alpha \in \mathbb{C} : |\alpha| < e^k\}$. From the above inequalities one finds that $g(\zeta)$ and $g(\zeta^2)$ are in D_k. Because complex conjugates have the same absolute value also $\overline{g(\zeta)} = g(\overline{\zeta}) = g(\zeta^4)$ and $\overline{g(\zeta^2)} = g(\overline{\zeta^2}) = g(\zeta^3)$ are in D_k. Therefore $|g(\zeta^l)| < e^k$ for all $l \in \{1,2,3,4\}$. Now because $g(\zeta) \in \mathbb{Q}[\zeta]$ and $[\mathbb{Q}[\zeta] : \mathbb{Q}] = 4$ we can conclude that the minimal polynomial of $g(\zeta)$ over $\mathbb{Q}$ has degree dividing $[\mathbb{Q}[\zeta] : \mathbb{Q}] = 4$. Therefore if $f(x)$ is the minimal polynomial of $g(\zeta)$, then we know that $\deg f(x) = 1, 2$ or 4. Now we define a polynomial $P(x)$ in the following way.

$$P(x) := \prod_{l=1}^{4} \left(x - g(\zeta^l)\right).$$

This polynomial has $g(\zeta^l)$ as roots for all $l \in \{1,2,3,4\}$. First we show a key results about this polynomial $P(x)$.

Lemma 7.4 *We have that* $P(x) \in \mathbb{Z}[x]$

Proof of Lemma 7.4: Since $P(x)$ has its roots located in $\mathbb{Q}[\zeta]$ we can already say that $P(x) \in \mathbb{Q}[\zeta][x]$ for sure. This itself is not a very strong argument however watch what happens if we apply an automorphism on it.

To recall, suppose $\sigma : \mathbb{Q}[\zeta] \to \mathbb{Q}[\zeta]$ is an automorphism. Then by definition the map σ is a bijective ring homomorphism from the field $\mathbb{Q}[\zeta]$ to itself that fixes the base field. This means that $\sigma(q) = q$ for all $q \in \mathbb{Q}$. We are interested in the possible values of $\sigma(\zeta)$. The minimal polynomial of ζ over $\mathbb{Q}$ is given by $f(x) = x^4 + x^3 + x^2 + x + 1$, this polynomial has the four roots ζ, ζ^2, ζ^3 and ζ^4. All of these roots are distinct, therefore $f(x)$ is a separable polynomial. Also note that all the powers of ζ are in $\mathbb{Q}[\zeta]$, therefore $\mathbb{Q}[\zeta]$ is a splitting field over $\mathbb{Q}$. This shows that the field extension $\mathbb{Q}[\zeta]$ is Galois over $\mathbb{Q}$. From this we conclude that the Galois group is well defined and it consists of all $\mathbb{Q}$-linear automorphisms. These are exactly the possible maps σ that we are looking for.

From Galois theory we know that all the possible $\mathbb{Q}$-linear automorphisms are exactly equal to the four maps σ_i as described earlier. Hence $\text{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q}) = \{\sigma_i : 1 \leq i \leq 4, \sigma_i(\zeta) = \zeta^i\}$. Now if a number γ is invariant under the action of the Galois group, we obtain that this number $\gamma \in \mathbb{Q}$. Note that γ being invariant under the action of the Galois group means that $\sigma(\gamma) = \gamma$ for all $\sigma \in \text{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q})$. Now applying any of these automorphisms on $P(x)$ yields that

$$\begin{aligned}
\sigma_i(P(x)) &= \sigma_i\left(\prod_{l=1}^{4}\left(x-g(\zeta^l)\right)\right)\\
&= \sigma_i(x^4+ax^3+bx^2+cx+d)\\
&= x^4+\sigma_i(a)x^3+\sigma_i(b)x^2+\sigma_i(c)x+\sigma_i(d)\\
&= \prod_{l=1}^{4}\left(x-\sigma_i(g(\zeta^l))\right)\\
&= \prod_{l=1}^{4}\left(x-g(\sigma_i(\zeta^l))\right)\\
&= \prod_{l=1}^{4}\left(x-g((\zeta^{il}))\right)\\
&= \prod_{j=1}^{4}\left(x-g((\zeta^{j}))\right) = P(x).
\end{aligned}$$

Here we used the linearity of σ_i and the fact that each σ_i permutes the set $\{\zeta,\zeta^2,\zeta^3,\zeta^4\}$. This allowed us to change the product in the last line by replacing each ζ^{il} with ζ^j because each power appears exactly once. This is also seen from $\{\zeta^i,\zeta^{2i},\zeta^{3i},\zeta^{4i}\} = \{\zeta,\zeta^2,\zeta^3,\zeta^4\}$. We have then shown that $\sigma_i(P(x)) = P(x)$ for all $\mathbb{Q}$-linear automorphisms $\sigma_i \in \text{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q})$. This shows that $P(x) \in \mathbb{Q}[x]$ which is already stronger than the previously observed $P(x) \in \mathbb{Q}[\zeta][x]$.

So we now know that $P(x) \in \mathbb{Q}[x]$, we now aim to show that in fact $P(x) \in \mathbb{Z}[x]$. We prove this by contradiction, so to start of suppose that $P(x) \notin \mathbb{Z}[x]$. Because $P(x)$ is a rational polynomial we need that at least one of the coefficients of $P(x) \notin \mathbb{Z}$. Let this coefficient be α, from which we know that $\alpha = \frac{a}{b}$ where a and b are relatively prime integers with $b \neq \pm 1$. From the definition $P(x) = \prod_{l=1}^{4}\left(x-g(\zeta^l)\right)$ we see that this α is in fact a sum of products of $g(\zeta^k)$ terms. Therefore we find that $\alpha \in \mathbb{Z}[\zeta]$, as α is just equal to some polynomial in terms of ζ. We then have that $\mathbb{Z}[\alpha] \subset \mathbb{Z}[\zeta]$ as rings. One can namely check that $\mathbb{Z}[\alpha]$ contains the unit element and that this ring is closed under addition and multiplication. Therefore it is indeed a subring.

Now on one end we have the ring $\mathbb{Z}[\zeta] = \{a+b\zeta+c\zeta^2+d\zeta^3 : a,b,c,d \in \mathbb{Z}\}$. Therefore as a group with respect to summation, $\mathbb{Z}[\zeta] \cong \mathbb{Z}^4$ via the isomorphism that maps $a+b\zeta+c\zeta^2+d\zeta^3$ to (a,b,c,d). On the other end we have the ring $\mathbb{Z}[\alpha]$, for which we had the inclusion $\mathbb{Z}[\alpha] \subset \mathbb{Z}[\zeta]$ as rings. If the inclusion is true as rings, this inclusion is also true as groups because it's about the same element set. Because the latter is isomorphic to $\mathbb{Z}^4$ we know that $\mathbb{Z}[\alpha]$ is isomorphic to a subgroup of $\mathbb{Z}^4$. There are only four different subgroups of $\mathbb{Z}^4$ up to isomorphism namely $\{\mathbb{Z}^0 = \{0\},\mathbb{Z}^1,\mathbb{Z}^2,\mathbb{Z}^3\}$. Since $\alpha = \frac{a}{b}$ we know that each power of α is linearly independent with respect to its previous powers over $\mathbb{Z}$. This means that it is impossible to find integers $a_0,a_1,...,a_{n-1}$ such that $\alpha^n = a_0+a_1\alpha+...+a_{n-1}\alpha^{n-1}$. Therefore $\mathbb{Z}[\alpha] = \{a_0+a_1\alpha+...+a_n\alpha^n+... : a_0,a_1,...,a_n,... \in \mathbb{Z}\}$. From this we can see that as groups, $\mathbb{Z}[\alpha]$ is not isomorphic to some $\mathbb{Z}^d$ where d is finite. This is then a contradiction, from which we see that each coefficient α of the polynomial $P(x)$ is in fact an integer. This then indeed shows us that the polynomial $P(x) = \prod_{l=1}^{4}\left(x-g(\zeta^l)\right) \in \mathbb{Z}[x]$.

Q.E.D.

Now that we have this result we can continue with proving Theorem 7.1, namely proving discreteness of the image. We have seen that $|g(\zeta^l)| < e^k$ for all $l \in \{1,2,3,4\}$, after expanding the polynomial we then find that

$$\begin{aligned} P(x) &= \prod_{l=1}^{4} \left(x - g(\zeta^l)\right) \\ &= (x - g(\zeta)) \cdot (x - g(\zeta^2)) \cdot (x - g(\zeta^3)) \cdot (x - g(\zeta^4)). \\ &= x^4 + ax^3 + bx^2 + cx + d \end{aligned}$$

where $a, b, c, d \in \mathbb{Z}$, as Lemma 7.4 shows we are dealing with a polynomial with integer coefficients. We have the following expressions for a, b, c and d:

- $a = -(g(\zeta) + g(\zeta^2) + g(\zeta^3) + g(\zeta^4))$.
- $b = g(\zeta) \cdot g(\zeta^2) + g(\zeta) \cdot g(\zeta^3) + g(\zeta) \cdot g(\zeta^4) + g(\zeta^2) \cdot g(\zeta^3) + g(\zeta^2) \cdot g(\zeta^4) + g(\zeta^3) \cdot g(\zeta^4)$.
- $c = -(g(\zeta) \cdot g(\zeta^2) \cdot g(\zeta^3) + g(\zeta) \cdot g(\zeta^2) \cdot g(\zeta^4) + g(\zeta) \cdot g(\zeta^3) \cdot g(\zeta^4) + g(\zeta^2) \cdot g(\zeta^3) \cdot g(\zeta^4))$.
- $d = g(\zeta) \cdot g(\zeta^2) \cdot g(\zeta^3) \cdot g(\zeta^4)$.

Now we use the bound that we found on each $|g(\zeta^l)|$ combined with the triangle inequality to obtain bounds on each of the coefficients.

- $\begin{aligned} |a| &= |(g(\zeta) + g(\zeta^2) + g(\zeta^3) + g(\zeta^4))| \\ &\leq |g(\zeta)| + |g(\zeta^2)| + |g(\zeta^3)| + |g(\zeta^4)| \\ &< e^k + e^k + e^k + e^k = 4e^k. \end{aligned}$
- $\begin{aligned} |b| &= |g(\zeta) \cdot g(\zeta^2) + g(\zeta) \cdot g(\zeta^3) + g(\zeta) \cdot g(\zeta^4) + g(\zeta^2) \cdot g(\zeta^3) + g(\zeta^2) \cdot g(\zeta^4) + g(\zeta^3) \cdot g(\zeta^4)| \\ &\leq |g(\zeta) \cdot g(\zeta^2)| + |g(\zeta) \cdot g(\zeta^3)| + |g(\zeta) \cdot g(\zeta^4)| + |g(\zeta^2) \cdot g(\zeta^3)| + |g(\zeta^2) \cdot g(\zeta^4)| + |g(\zeta^3) \cdot g(\zeta^4)| \\ &< e^k \cdot e^k + e^k \cdot e^k + e^k \cdot e^k + e^k \cdot e^k + e^k \cdot e^k + e^k \cdot e^k = 6e^{2k} \end{aligned}$
- $\begin{aligned} |c| &= |g(\zeta) \cdot g(\zeta^2) \cdot g(\zeta^3) + g(\zeta) \cdot g(\zeta^2) \cdot g(\zeta^4) + g(\zeta) \cdot g(\zeta^3) \cdot g(\zeta^4) + g(\zeta^2) \cdot g(\zeta^3) \cdot g(\zeta^4)| \\ &\leq |g(\zeta) \cdot g(\zeta^2) \cdot g(\zeta^3)| + |g(\zeta) \cdot g(\zeta^2) \cdot g(\zeta^4)| + |g(\zeta) \cdot g(\zeta^3) \cdot g(\zeta^4)| + |g(\zeta^2) \cdot g(\zeta^3) \cdot g(\zeta^4)| \\ &< e^k \cdot e^k \cdot e^k + e^k \cdot e^k \cdot e^k + e^k \cdot e^k \cdot e^k + e^k \cdot e^k \cdot e^k = 4e^{3k} \end{aligned}$
- $\begin{aligned} |d| &= |g(\zeta) \cdot g(\zeta^2) \cdot g(\zeta^3) \cdot g(\zeta^4)| \\ &< e^k \cdot e^k \cdot e^k \cdot e^k = e^{4k} \end{aligned}$

So this gives us our bounds on the coefficients of polynomial $P(x)$. Now since all of its coefficients are integers, which are shown bounded by a number k which is completely independent of everything else as this just determines the size of the box, we can make the following conclusion.

Since any finite range of integers contains only finitely many integers, there exist only finitely many polynomials $P(x)$ as how we defined them. Since each $g(\zeta)$ is a root of $P(x)$ there exists also only finitely many such $g(\zeta)$ values in $\mathbb{Z}[\zeta]$. Hence there exist finitely many $\beta \in \mathbb{Z}[\zeta]$ such that $\psi(\beta) \in B$. After restricting to the units of $\mathbb{Z}[\zeta]$ there are still only finitely many values that satisfy it. Therefore we can conclude that the intersection of $\psi(\mathbb{Z}[\zeta]^\times)$ and box B os size $2k \times 2k$ centered at the origin contains finitely many points and therefore the image of ψ is discrete which is precisely what we wanted to show.

Q.E.D.

Now that we have shown that the image is discrete, we aim to find a nicer way to describe it. First note that the line $x + y = 0$ in $\mathbb{R}^2$ can just be identified by $\mathbb{R}$ if we map all points $(x, -x)$ to x. This clearly is a bijection. Because ψ maps all the units onto this line we can also look at this new change of perspective such that the image of ψ lies completely in $\mathbb{R}$. This changes our question to finding all discrete subgroups of $\mathbb{R}$.

Lemma 7.5 *All discrete subgroups G of $\mathbb{R}$ are of the form $r\mathbb{Z}$ where r is some real number.*

Proof: Let G be a discrete subgroup of $\mathbb{R}$. If G is the trivial group, $G = \{0\}$, then we are done because $\{0\} = 0\mathbb{Z}$. Therefore now assume G is nontrivial. We define a real number r in the following way.

$$r := \min\{G \cap (0, \infty)\}$$

In words this means that r is the smallest real positive number that is also in G. This minimum exists because G is discrete. Therefore there exists some interval I around 0 such that the intersection of I and G is equals to $\{0\}$. Gradually making this interval larger will yield us another point in this intersection if I is large enough because G is nontrivial. This value of r lies in G and we claim that $G = r\mathbb{Z}$.

First observe that if $r \in G$ then any multiple of r is also in G due to the group structure. Hence $m \cdot r \in G$ holds $\forall m \in \mathbb{Z}$. Therefore $r\mathbb{Z} \subseteq G$. Suppose now that $G \neq r\mathbb{Z}$. Since the right set is a subset of the left one, we find that the set $G \backslash r\mathbb{Z}$ is nonempty. Hence pick $g \in G \backslash r\mathbb{Z}$. Therefore we can find some number $k \in \mathbb{Z}$ such that $kr < g < (k+1)r$. This is true as $g \in G$ but $g \notin r\mathbb{Z}$ and therefore g should lie between two multiples of r. Knowing this however we find $0 < kr - g < r$ and due to the group structure $kr - g \in G$. This is impossible due to the choice of r being $r = \min\{G \cap (0, \infty)\}$ and hence no numbers in the open interval $(0, r)$ are in G. Therefore supposing that $G \neq r\mathbb{Z}$ leads to a contradiction which shows that $G = r\mathbb{Z}$. Therefore we have shown that all discrete subgroups G of $\mathbb{R}$ are of the form $r\mathbb{Z}$ for some real number r.

Q.E.D.

Now that we have found the structure of each discrete subgroup of $\mathbb{R}$ we can describe the image of ψ completely and hence find a nice way to write the units by mapping back. The last problem we

face is finding the correct value of r as we have seen before. We make use of similar arguments used to show that $\psi(\mathbb{Z}[\zeta]^\times)$ is discrete in $\mathbb{R}^2$ to find this specific r. Our approach is the following. We find a potential value of r by plugging in a specific $\beta \in \mathbb{Z}[\zeta]$ into ψ and see what we end up with. After that we prove no smaller value of r would work giving us the final result.

Lemma 7.6 *The value of r such that $\psi(\mathbb{Z}[\zeta]^\times) = r\{(k,-k) : k \in \mathbb{Z}\}$ is given by $r = \ln(\frac{1+\sqrt{5}}{2})$.*

Proof: First note that the image of ψ is discrete by Theorem 7.1. Next up in Lemma 7.5 we saw what all the possible subgroups of $\mathbb{R}$ are. Using that the image of ψ lies on the line $x + y = 0$ and that this line is described by $(t, -t)$ for $t \in \mathbb{R}$ allows us to say that the image of ψ has the given structure as written in the statement of Lemma 7.6. Observe that $\zeta + \zeta^{-1} = \frac{-1+\sqrt{5}}{2} \in \mathbb{Z}[\zeta]$ and therefore also $1 + \zeta + \zeta^{-1} = \frac{1+\sqrt{5}}{2} \in \mathbb{Z}[\zeta]$. A quick computation shows that $\frac{-1+\sqrt{5}}{2} \cdot \frac{1+\sqrt{5}}{2} = 1$ which also shows us that $\frac{1+\sqrt{5}}{2} \in \mathbb{Z}[\zeta]^\times$. Under ϕ we find that $\phi(\frac{1+\sqrt{5}}{2}) = (\ln(\frac{1+\sqrt{5}}{2}), -\ln(\frac{1+\sqrt{5}}{2}))$ hence indeed showing us that $r \leq \ln(\frac{1+\sqrt{5}}{2})$. We show r is actually equal to the upper bound by way of contradiction. So suppose that $r < \ln(\frac{1+\sqrt{5}}{2})$. Because the image of ψ over the units is still a discrete subgroup of $\mathbb{R}$ which contains the value $\ln(\frac{1+\sqrt{5}}{2})$, we know that the actual value of r should then be $\leq \frac{1}{2} \cdot \ln(\frac{1+\sqrt{5}}{2})$ because each discrete subgroup of $\mathbb{Z}$ equals some real number times the integers. Hence there exists some integer $k \geq 2$ such that $r \cdot k = \ln(\frac{1+\sqrt{5}}{2})$ which shows the new bound on r. To prove is then that there do no exist units that get mapped to the box $B = \{(x,y) \in \mathbb{R}^2 : |x|, |y| \leq \frac{1}{2} \cdot \ln(\frac{1+\sqrt{5}}{2})\}$ except for units that are mapped to $(0,0)$, as they do not contribute towards the value of r.

Suppose $\beta \in \mathbb{Z}$ is such that $\psi(\beta) \in B$. It then holds that

$$\begin{aligned}
\psi(\beta) \in B &\Rightarrow \psi(\beta) \in \{(x,y) \in \mathbb{R}^2 : |x|, |y| < \frac{1}{2} \cdot \ln(\frac{1+\sqrt{5}}{2})\} \\
&\Rightarrow (\ln(|g(\zeta)|), \ln(|g(\zeta^2)|)) \in \{(x,y) \in \mathbb{R}^2 : |x|, |y| < \frac{1}{2} \cdot \ln(\frac{1+\sqrt{5}}{2})\} \\
&\Rightarrow |g(\zeta)| < e^{\frac{1}{2} \cdot \ln(\frac{1+\sqrt{5}}{2})} = \sqrt{\frac{1+\sqrt{5}}{2}} \text{ and } \Rightarrow |g(\zeta^2)| < e^{\frac{1}{2} \cdot \ln(\frac{1+\sqrt{5}}{2})} = \sqrt{\frac{1+\sqrt{5}}{2}}
\end{aligned}$$

Now following the proof of Theorem 7.1, we construct the polynomial

$$P(x) = \prod_{l=1}^{4} \left(x - g(\zeta^l)\right)$$

which was shown to be in $\mathbb{Z}[x]$ by Lemma 7.4. For this polynomial we bound all it's coefficients so that we are able to find potential units as roots of all these different polynomial $P(x)$. This method allows us to find the $\beta \in \mathbb{Z}[\zeta]$ that get mapped into box B. It then remains to check which values

of β are units, if any are. So we obtain that $P(x) = x^4 + ax^3 + bx^2 + cx + d$ where bounds on $a, b, c, d \in \mathbb{Z}$ are given by

$$|a| < 4 \cdot \sqrt{\frac{1+\sqrt{5}}{2}} < 6, |b| < 6 \cdot \left(\sqrt{\frac{1+\sqrt{5}}{2}}\right)^2 < 10$$
$$|c| < 4 \cdot \left(\sqrt{\frac{1+\sqrt{5}}{2}}\right)^3 < 9, |d| < \left(\sqrt{\frac{1+\sqrt{5}}{2}}\right)^4 < 3.$$

Now this leaves us with a total of $11 \cdot 19 \cdot 17 \cdot 5 = 17765$ different polynomials in $\mathbb{Z}[x]$. Each polynomial has 4 distinct roots giving us 71060 potential units. To then check whether or not a root is a unit we need to see if ψ maps a root to the line $x + y = 0$. This means that $\ln(|g(\zeta^2)|) = -\ln(|g(\zeta)|)$ is needed. This becomes the condition $|g(\zeta) \cdot g(\zeta^2)| = 1$. Using that $|\overline{g(\zeta)}| = |g(\overline{\zeta})| = |g(\zeta^4)|$ and $|\overline{g(\zeta^2)}| = |g(\overline{\zeta^2})| = |g(\zeta^3)|$ we actually find the following four relations.

$$|g(\zeta) \cdot g(\zeta^2)| = |g(\zeta) \cdot g(\zeta^3)| = |g(\zeta^4) \cdot g(\zeta^2)| = |g(\zeta^4) \cdot g(\zeta^3)| = 1.$$

This allows us to slightly lower the bounds on a, b, c, d to become

$$|a| < 6, |b| < 8, |c| < 6, |d| = 1.$$

This then means that there are 3630 different polynomials in $\mathbb{Z}[x]$ from which we need to check 14520 different roots for if they lie in $\mathbb{Z}[\zeta]$. This can be done by checking factorization inside $\mathbb{Z}[\zeta][x]$. Furthermore we also want that these roots satisfy that ψ maps into B with these roots. The amount of polynomials that need to be checked can be reduced by a factor of approximately 4 by using the following two symmetrical arguments:

1. After checking $P(x) = x^4 + ax^3 + bx^2 + cx + d$, we don't need to check $-P(x) = -x^4 - ax^3 - bx^2 - cx - d$.
2. After checking $P(x) = x^4 + ax^3 + bx^2 + cx + d$, we don't need to check $P(-x) = x^4 - ax^3 + bx^2 - cx + d$.

One can go through all these different polynomials to find that there is only one polynomial which has roots in $\mathbb{Z}[\zeta]$ that are units, under the condition that ψ maps into B. This polynomial is $f(x) = x^4 + x^3 + x^2 + x + 1$ as

$$f(x) = x^4 + x^3 + x^2 + x + 1 = (x - \zeta)(x - \zeta^2)(x - \zeta^3)(x - \zeta^4).$$

Note however that $\psi(\zeta^i) = (\ln(|\zeta^i|), \ln(|\zeta^{2i}|)) = (0,0)$. This means that these units do not contribute to that value of r. Hence no other units exist in $\mathbb{Z}[\zeta]$ that get mapped into this box. This contradicts our assumption that $r < \ln(\frac{1+\sqrt{5}}{2})$ as no units lie on the line $x+y=0$ in between the points $(0,0)$ and $(\ln(\frac{1+\sqrt{5}}{2}), -\ln(\frac{1+\sqrt{5}}{2}))$. This then shows us that also $r \geq \ln(\frac{1+\sqrt{5}}{2})$.

Since $r \leq \ln(\frac{1+\sqrt{5}}{2})$ was shown already we can conclude that in fact $r = \ln(\frac{1+\sqrt{5}}{2})$. Therefore the value of r such that $\psi(\mathbb{Z}[\zeta]^\times) = r\{(k,-k) : k \in \mathbb{Z}\}$ is equal to $\ln(\frac{1+\sqrt{5}}{2})$, proving Lemma 7.6.

Q.E.D.

7.1.2 The structure of the units

Now it is time to classify the units of $\mathbb{Z}[\zeta]$ using all our knowledge from above.

Theorem 7.2 *If $u \in \mathbb{Z}$ is a unit then there exist integers r and k such that $u = \pm(\zeta)^r \cdot \left(\frac{1+\sqrt{5}}{2}\right)^k$*

Proof: We aim for the result that $\mathbb{Z}[\zeta]^\times = \{\pm(\zeta)^r \cdot \left(\frac{1+\sqrt{5}}{2}\right)^k : r,k \in \mathbb{Z}\}$, we will do this using double inclusion.

Suppose that $\alpha \in \{\pm(\zeta)^r \cdot \left(\frac{1+\sqrt{5}}{2}\right)^k : r,k \in \mathbb{Z}\}$. We aim to show that then $\alpha \in \mathbb{Z}[\zeta]^\times$. Since $\alpha \in \{\pm(\zeta)^r \cdot \left(\frac{1+\sqrt{5}}{2}\right)^k : r,k \in \mathbb{Z}\}$ we can find integers a and b such that $\alpha = \pm(\zeta)^a \cdot \left(\frac{1+\sqrt{5}}{2}\right)^b$. Let $\beta := \pm(\zeta)^{4a} \cdot \left(\frac{1+\sqrt{5}}{2} - 1\right)^b \in \mathbb{Z}[\zeta]$, then we can check that

$$\begin{aligned}
\alpha \cdot \beta &= \left(\pm(\zeta)^a \cdot \left(\frac{1+\sqrt{5}}{2}\right)^b\right) \cdot \left(\pm(\zeta)^{4a} \cdot \left(\frac{1+\sqrt{5}}{2} - 1\right)^b\right) \\
&= (\zeta)^{a+4a} \cdot \left(\left(\frac{1+\sqrt{5}}{2}\right) \cdot \left(\frac{1+\sqrt{5}}{2} - 1\right)\right)^b \\
&= (\zeta)^{5a} \cdot \left(\frac{(1+\sqrt{5})^2}{4} - \frac{1+\sqrt{5}}{2}\right)^b \\
&= 1 \cdot \left(\frac{6+2\sqrt{5}}{4} - \frac{1+\sqrt{5}}{2}\right)^b = \left(\frac{3}{2} - \frac{1}{2} + \frac{\sqrt{5}}{2} - \frac{\sqrt{5}}{2}\right)^b = 1^b = 1.
\end{aligned}$$

This shows that for all $\alpha \in \{\pm(\zeta)^r \cdot \left(\frac{1+\sqrt{5}}{2}\right)^k : r,k \in \mathbb{Z}\}$ it is possible to find a $\beta \in \mathbb{Z}[\zeta]$ such that $\alpha \cdot \beta = 1$. Therefore α is a unit so $\alpha \in \mathbb{Z}[\zeta]^\times$. Hence we obtain the relation that $\{\pm(\zeta)^r \cdot \left(\frac{1+\sqrt{5}}{2}\right)^k : r,k \in \mathbb{Z}\} \subseteq \mathbb{Z}[\zeta]^\times$.

Suppose that $\alpha \in \mathbb{Z}[\zeta]^\times$. We then know that

$$\psi(\alpha) \in \psi(\mathbb{Z}[\zeta]^\times) = \ln\left(\frac{1+\sqrt{5}}{2}\right) \cdot \{(k,-k) : k \in \mathbb{Z}\}$$

following Lemma 7.6. Therefore we know that there exists an integer l such that

$$\psi(\alpha) = \left(l \cdot \ln\left(\frac{1+\sqrt{5}}{2}\right), -l \cdot \ln\left(\frac{1+\sqrt{5}}{2}\right)\right).$$

Recall that α can be written as some $g(\zeta)$ and that $\psi(g(\zeta)) = (\ln(|g(\zeta)|), -\ln(|g(\zeta)|))$ for units, therefore we find that

$$\begin{aligned}
\psi(\alpha) = \left(l \cdot \ln\left(\frac{1+\sqrt{5}}{2}\right), -l \cdot \ln\left(\frac{1+\sqrt{5}}{2}\right)\right) &= (\ln(|g(\zeta)|), -\ln(|g(\zeta)|)) \\
\Rightarrow l \cdot \ln\left(\frac{1+\sqrt{5}}{2}\right) = \ln(|g(\zeta)|) \text{ and } -l \cdot \ln\left(\frac{1+\sqrt{5}}{2}\right) &= -\ln(|g(\zeta)|) \\
\Rightarrow |g(\zeta)| = \left(\frac{1+\sqrt{5}}{2}\right)^l \Rightarrow |\alpha| &= \left(\frac{1+\sqrt{5}}{2}\right)^l.
\end{aligned}$$

It remains to then find all elements of $\mathbb{Z}[\zeta]^\times$ that have absolute value equal to $\left(\frac{1+\sqrt{5}}{2}\right)^l$. We know that the element $\left(\frac{1+\sqrt{5}}{2}\right)^l$ satisfies this but we are eager to find all such units. Notice that $\left(\frac{1+\sqrt{5}}{2}\right)^l$ is indeed a unit as shown in the first inclusion above. I claim that $|\alpha| = |\beta| \Leftrightarrow \psi(\alpha) = \psi(\beta)$ for all units α and β. This if and only if statement follows from the fact that the natural logarithm is a bijective function from $\mathbb{R}_{>0} \to \mathbb{R}$. Now notice however that

$$\begin{aligned}
\psi(\alpha) = \psi(\beta) \Rightarrow \psi(\alpha \cdot \beta^{-1}) &= \psi(\alpha) + \psi(\beta^{-1}) \\
&= \psi(\alpha) + (\psi(\beta))^{-1} \\
&= \psi(\alpha) + (\psi(\alpha))^{-1} \\
&= \psi(a) - \psi(\alpha) = 0
\end{aligned}$$

where we used that ψ is a group homomorphism and that $(\psi(x))^{-1} = -\psi(x)$, a result that follows from the group law imposed on $\mathbb{R} \times \mathbb{R}$. Since $\psi(\alpha \cdot \beta^{-1}) = 0$, it follows that $\alpha \cdot \beta^{-1} \in \ker(\psi)$. We would now like to determine what the set $\ker(\psi)$ is as this tells us something about the relation between α and β.

I make the claim that $x \in \ker(\psi) \Leftrightarrow |x| = 1$. If $|x| = 1$ then we see that $\psi(x) = (\ln(|x|), -\ln(|x|)) = (\ln(1), -\ln(1)) = (0,0)$ and so $x \in \ker(\psi)$. If $x \in \ker(\psi)$ then $\psi(x) = 0 \Rightarrow (\ln(|x|), -\ln(|x|)) = (0,0) \Rightarrow |x| = 1$ which proves this claim. Notice however that we can add a second claim to that by

the same strategy. Recall that the Galois group satisfied $\text{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q}) = \{\sigma_i : 1 \leq i \leq 4, \sigma_i(\zeta) = \zeta^i\}$. Notice then that $g(\zeta^i) = \sigma_i(\alpha)$ however for the following part we will use the notation using σ_i for our convenience.

The second claim that I make is that not only $|x| = |\sigma_1(x)| = 1 \Leftrightarrow x \in \ker(\psi)$ but that actually $|\sigma_1(x)| = |\sigma_2(x)| = 1 \Leftrightarrow x \in \ker(\psi)$. Notice that this follows from the fact that $\ln(|\sigma_2(x)|) = -\ln(|\sigma_1(x)|)$ for units and that from there the claim follows. Now recall that $|g(\zeta)| = |g(\zeta^4)|$ and $|g(\zeta^2)| = |g(\zeta^3)|$ as they are each others complex conjugates. From this we can see that

$$x \in \ker(\psi) \Leftrightarrow |\sigma_i(x)| = 1, \forall 1 \leq i \leq 4.$$

Now we will compute all such α by hand in the following way. Writing numbers in $\mathbb{Z}[\zeta]$ with respect to the basis $\{\zeta, \zeta^2, \zeta^3, \zeta^4\}$ makes things much easier for us as we can see the following relations.

$$\begin{aligned}
\alpha = \sigma(\alpha) &= a\zeta + b\zeta^2 + c\zeta^3 + d\zeta^4 \\
\sigma^2(\alpha) &= c\zeta + a\zeta^2 + d\zeta^3 + b\zeta^4 \\
\sigma^3(\alpha) &= b\zeta + d\zeta^2 + a\zeta^3 + c\zeta^4 \\
\sigma^4(\alpha) &= d\zeta + c\zeta^2 + b\zeta^3 + a\zeta^4.
\end{aligned}$$

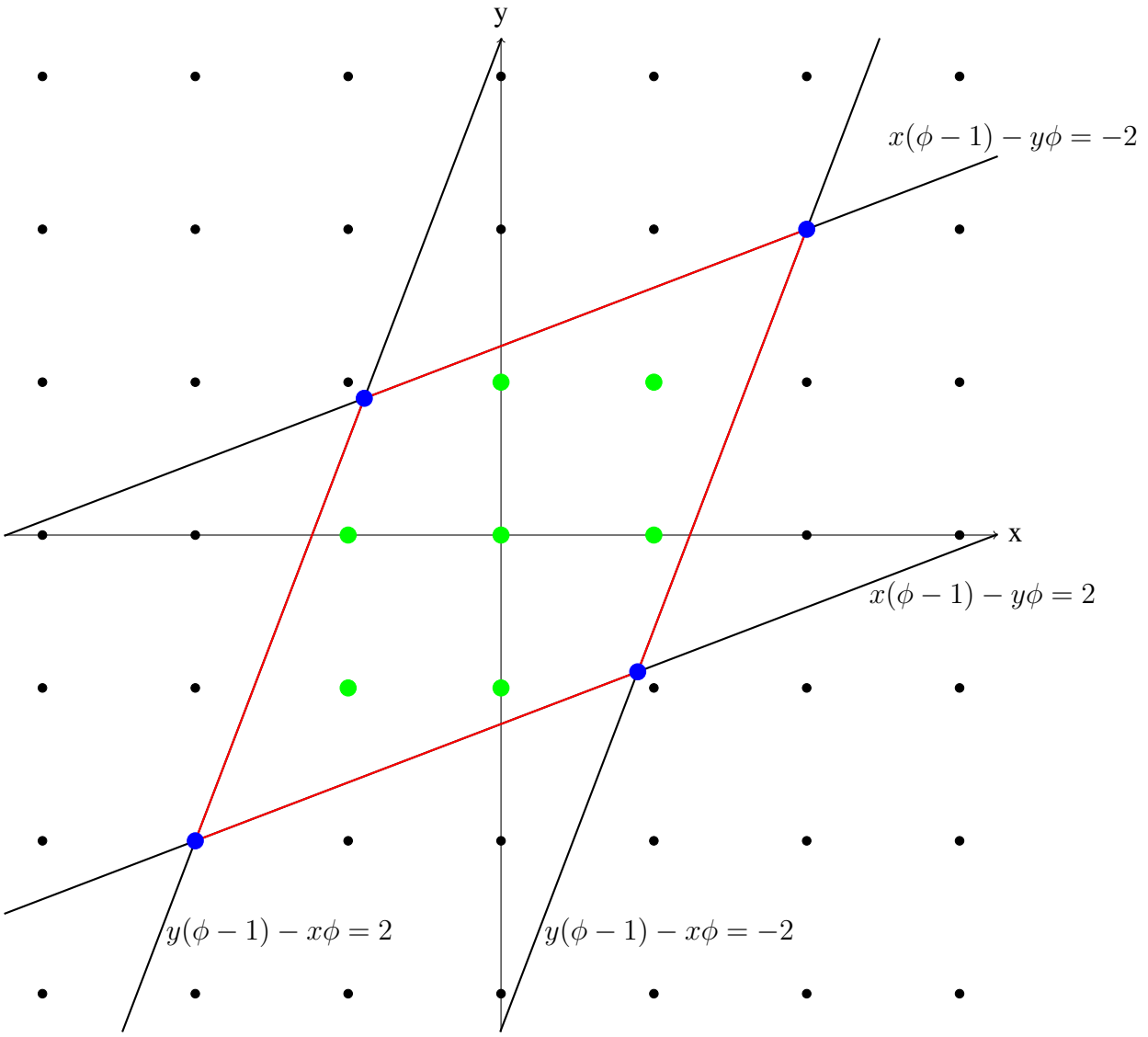
All of these numbers have absolute value equal to 1 as we saw above. Now we will add complex conjugates to each other to get completely real numbers where we then also use that $\zeta + \zeta^4 = \phi - 1$ and $\zeta^2 + \zeta^3 = -\phi$. Now from the triangle inequalities we obtain the two relations

- $|\sigma(\alpha) + \sigma^4(\alpha)| \leq |\sigma(\alpha)| + |\sigma^4(\alpha)| = 1 + 1 = 2$ and
- $|\sigma^2(\alpha) + \sigma^3(\alpha)| \leq |\sigma^2(\alpha)| + |\sigma^3(\alpha)| = 1 + 1 = 2.$

Using these we obtain the following inequalities:

$$\begin{aligned}
\bullet |\sigma(\alpha) + \sigma^4(\alpha)| \leq 2 &\Rightarrow |(a+d)\zeta + (b+c)\zeta^2 + (b+c)\zeta^3 + (a+d)\zeta^4| \leq 2 \\
&\Rightarrow |(a+d)(\zeta + \zeta^4) + (b+c)(\zeta^2 + \zeta^3)| \leq 2 \\
&\Rightarrow |(a+d)(\phi - 1) - (b+c)\phi| \leq 2 \\
\bullet |\sigma^2(\alpha) + \sigma^3(\alpha)| \leq 2 &\Rightarrow |(b+c)\zeta + (a+d)\zeta^2 + (a+d)\zeta^3 + (b+c)\zeta^4| \leq 2 \\
&\Rightarrow |(b+c)(\zeta + \zeta^4) + (a+d)(\zeta^2 + \zeta^3)| \leq 2 \\
&\Rightarrow |(b+c)(\phi - 1) - (a+d)\phi| \leq 2.
\end{aligned}$$

Now note that the region $|x(\phi-1)-y\phi| \leq 2$ describe a tilted rectangle in $\mathbb{R}^2$ and that the region $|y(\phi-1)-x\phi| \leq 2$ also describes a tilted rectangle in $\mathbb{R}^2$. Looking at the intersection of these two regions we see that it is a parallelogram, call it P, in $\mathbb{R}^2$ with it's vertices being $(-2,-2), (\frac{2}{\sqrt{5}}, \frac{-2}{\sqrt{5}}), (2,2), (\frac{-2}{\sqrt{5}}, \frac{2}{\sqrt{5}})$. In the following picture we plot these lines. The parallelogram P is closed in by the red lines and the blue points are it's vertices.



As we saw that the numbers $a+d$ and $b+c$ satisfy these bounds, the coordinate $(a+d, b+c)$ must lay inside this parallelogram as well. Because all the variables are integers, $(a+d, b+c)$ is an integer coordinate in this parallelogram P. All integer coordinates are given by the following list:

$$L = \{(-2,-2), (-1,-1), (-1,0), (0,-1), (0,0), (0,1), (1,0), (1,1), (2,2)\}.$$

These points represent the green points inside P as seen in the above picture. Furthermore two of it's vertices are also accounted for, those being $(-2,-2)$ and $(2,2)$. From this we can conclude that $(a+d, b+c) \in L$. Now recall that we showed the relation

$$x \in \ker(\psi) \Leftrightarrow |x| = 1.$$

Now note that if $\alpha \in \ker(\psi)$, then it follows that $\zeta \cdot \alpha \in \ker(\psi)$ because $|\zeta \cdot \alpha| = |\zeta| \cdot |\alpha| = 1$. It follows then that $|\sigma_i(\zeta \cdot \alpha)| = 1$ for all $1 \leq i \leq 4$ as well. Note that

$$\begin{aligned} \zeta \cdot \alpha &= \zeta(a\zeta + b\zeta^2 + c\zeta^3 + d\zeta^4) \\ &= -d\zeta + (a-d)\zeta^2 + (b-d)\zeta^3 + (c-d)\zeta^4. \end{aligned}$$

Using the same argument that we used on α to get conditions on it's coefficients, we also obtain conditions on the coefficients of $\zeta \cdot \alpha$ as following. Namely since $\alpha = a\zeta + b\zeta^2 + c\zeta^3 + d\zeta^4$ yielded $(a+d, b+c) \in L$, it follows that $\zeta \cdot \alpha = -d\zeta + (a-d)\zeta^2 + (b-d)\zeta^3 + (c-d)\zeta^4$ yields $(c-2d, a+b-2d) \in L$. Because these two points lie in L, each individual coordinate is equal to some value that we denote by v_i. The linear system we now obtain is given by

$$\begin{cases} a+d = v_1 \\ b+c = v_2 \\ c-2d = v_3 \\ a+b-2d = v_4 \end{cases}$$

Putting this in matrix notation yields

$$\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & -2 \\ 1 & 1 & 0 & -2 \end{pmatrix} \cdot \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} v_1 \\ v_2 \\ v_3 \\ v_4 \end{pmatrix}$$

Solving this system for a, b, c, d gives us that

$$\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & -2 \\ 1 & 1 & 0 & -2 \end{pmatrix}^{-1} \cdot \begin{pmatrix} v_1 \\ v_2 \\ v_3 \\ v_4 \end{pmatrix} = \frac{1}{5} \cdot \begin{pmatrix} 4v_1 - v_2 + v_3 + v_4 \\ -2v_1 + 3v_2 - 3v_3 + 2v_4 \\ 2v_1 + 2v_2 + 3v_3 - 2v_4 \\ v_1 + v_2 - v_3 - v_4 \end{pmatrix}$$

Now recall that the v_i were chosen such that $(v_1, v_2) \in L$ and $(v_3, v_4) \in L$. Therefore we have a total of 81 possible outcomes for (v_1, v_2, v_3, v_4). Since our a, b, c and d are all integers we can

reduce our list a bit so we don't have to check what each value set (v_1, v_2, v_3, v_4) yields. The easiest value to investigate on is d since

$$|d| = \frac{1}{5} \cdot |v_1 + v_2 - v_3 - v_4| \leq \frac{1}{5}(|v_1| + |v_2| + |v_3| + |v_4|) = \frac{8}{5} < 2.$$

Checking the possible quadruples of v_i for which $d = -1$, $d = 0$ or $d = 1$ yields only 21 possible quadruples of v_i. One can check that indeed all of them give an $\alpha \in \mathbb{Z}[\zeta]$ because all of a, b, c and d are integers for these 21. Now we just do a manual check of which of these 21 alpha indeed satisfy $|a| = 1$:

$$1.\ (v_1, v_2, v_3, v_4) = (-2, -2, 0, 1) \Rightarrow \alpha = -\zeta - 2\zeta^3 - \zeta^4 \Rightarrow |\alpha| = 1,54..$$
$$2.\ (v_1, v_2, v_3, v_4) = (-2, -2, 1, 0) \Rightarrow \alpha = -\zeta - \zeta^2 - \zeta^3 - \zeta^4 = 1 \Rightarrow |\alpha| = 1$$
$$3.\ (v_1, v_2, v_3, v_4) = (-1, 0, 2, 2) \Rightarrow \alpha = -\zeta^4 \Rightarrow |\alpha| = 1$$
$$4.\ (v_1, v_2, v_3, v_4) = (0, -1, 2, 2) \Rightarrow \alpha = \zeta - \zeta^2 - \zeta^4 \Rightarrow |\alpha| = 1,54..$$
$$5.\ (v_1, v_2, v_3, v_4) = (2, 2, 0, -1) \Rightarrow \alpha = \zeta + 2\zeta^3 + \zeta^4 \Rightarrow |\alpha| = 1,54..$$
$$6.\ (v_1, v_2, v_3, v_4) = (2, 2, -1, 0) \Rightarrow \alpha = \zeta + \zeta^2 + \zeta^3 + \zeta^4 = -1 \Rightarrow |\alpha| = 1$$
$$7.\ (v_1, v_2, v_3, v_4) = (1, 0, -2, -2) \Rightarrow \alpha = \zeta^4 \Rightarrow |\alpha| = 1,$$
$$8.\ (v_1, v_2, v_3, v_4) = (0, 1, -2, -2) \Rightarrow \alpha = -\zeta + \zeta^2 + \zeta^4 \Rightarrow |\alpha| = 1,54..$$
$$9.\ (v_1, v_2, v_3, v_4) = (-2, -2, -2, -2) \Rightarrow \alpha = -2\zeta - 2\zeta^3 \Rightarrow |\alpha| = 1,23..$$
$$10.\ (v_1, v_2, v_3, v_4) = (-1, -1, -1, -1) \Rightarrow \alpha = -\zeta - \zeta^3 \Rightarrow |\alpha| = 0,61..$$
$$11.\ (v_1, v_2, v_3, v_4) = (-1, 0, -1, 0) \Rightarrow \alpha = -\zeta + \zeta^2 - \zeta^3 - \Rightarrow |\alpha| = 0,38..$$
$$12.\ (v_1, v_2, v_3, v_4) = (-1, 0, 0, -1) \Rightarrow \alpha = -\zeta \Rightarrow |\alpha| = 1$$
$$13.\ (v_1, v_2, v_3, v_4) = (0, -1, -1, 0) \Rightarrow \alpha = -\zeta^3 \Rightarrow |\alpha| = 1$$
$$14.\ (v_1, v_2, v_3, v_4) = (0, -1, 0, -1) \Rightarrow \alpha = -\zeta^2 \Rightarrow |\alpha| = 1$$
$$15.\ (v_1, v_2, v_3, v_4) = (0, 0, 0, 0) \Rightarrow \alpha = 0 \Rightarrow |\alpha| = 0$$
$$16.\ (v_1, v_2, v_3, v_4) = (1, 0, 1, 0) \Rightarrow \alpha = \zeta + \zeta^2 - \zeta^3 \Rightarrow |\alpha| = 0,38..$$
$$17.\ (v_1, v_2, v_3, v_4) = (1, 0, 0, 1) \Rightarrow \alpha = \zeta \Rightarrow |\alpha| = 1$$
$$18.\ (v_1, v_2, v_3, v_4) = (0, 1, 1, 0) \Rightarrow \alpha = \zeta^3 \Rightarrow |\alpha| = 1$$
$$19.\ (v_1, v_2, v_3, v_4) = (0, 1, 0, 1) \Rightarrow \alpha = \zeta^2 - \Rightarrow |\alpha| = 1$$
$$20.\ (v_1, v_2, v_3, v_4) = (1, 1, 1, 1) \Rightarrow \alpha = \zeta + \zeta^3 \Rightarrow |\alpha| = 0,61...$$
$$21.\ (v_1, v_2, v_3, v_4) = (2, 2, 2, 2) \Rightarrow \alpha = 2\zeta + 2\zeta^3 \Rightarrow |\alpha| = 1,23...$$

From this entire list we see that the only $\alpha \in \mathbb{Z}[\zeta]^\times$ with $|\alpha| = 1$ are $\{\pm 1, \pm\zeta, \pm\zeta^2, \pm\zeta^3, \pm\zeta^4\}$ from which we conclude that $\ker(\psi) = \{\pm 1, \pm\zeta, \pm\zeta^2, \pm\zeta^3, \pm\zeta^4\}$.

We had shown that $|\alpha| = |\beta| \Leftrightarrow \psi(\alpha) = \psi(\beta) \Rightarrow \alpha \cdot \beta^{-1} \in \ker(\psi)$ and therefore $\alpha = \pm(\zeta)^i \cdot \beta$. Hence if some α is a unit we can determine its absolute value. The other units with same

absolute value are given by $\pm(\zeta^i)\cdot\alpha$. Because for units all possible absolute values are given by $\left(\frac{1+\sqrt{5}}{2}\right)^l$ where $l\in\mathbb{Z}$ and the element $\alpha^*=\left(\frac{1+\sqrt{5}}{2}\right)^l\in\mathbb{Z}[\zeta]$ satisfies $|\alpha^*|=\left(\frac{1+\sqrt{5}}{2}\right)^l$. We can therefore describe every possible unit as a "$\pm(\zeta)^i$" term multiplied by a "$\left(\frac{1+\sqrt{5}}{2}\right)^l$" term.

Therefore $\alpha=\pm(\zeta)^i\cdot\left(\frac{1+\sqrt{5}}{2}\right)^l$ for some integers i and l which implies that $\alpha\in\{\pm(\zeta)^r\cdot\left(\frac{1+\sqrt{5}}{2}\right)^k : r,k\in\mathbb{Z}\}$. Hence we obtain the relation that $\mathbb{Z}[\zeta]^\times\subseteq\{\pm(\zeta)^r\cdot\left(\frac{1+\sqrt{5}}{2}\right)^k : r,k\in\mathbb{Z}\}$.

From this we find that $\{\pm(\zeta)^r\cdot\left(\frac{1+\sqrt{5}}{2}\right)^k : r,k\in\mathbb{Z}\}=\mathbb{Z}[\zeta]^\times$ as we intended to show.

Q.E.D.

So we managed to describe all units in the ring $\mathbb{Z}[\zeta]$. We did this by defining a map $\psi:\mathbb{Z}[\zeta]^\times\to\mathbb{R}^2$ and showing various properties of this map. These properties allowed us to get a nice description of all elements inside $\mathbb{Z}[\zeta]^\times$. Although this approach was different from the one done in Lemma 3.1 and Lemma 5.1, where we determined the units of respectively $\mathbb{Z}[\zeta_3]$ and $\mathbb{Z}[i]$, the key idea remains. Namely we aim to find a function $N(.)$ from $\mathbb{Z}[\zeta]^\times\to\mathbb{Z}$ such that α is a unit if and only if $N(\alpha)=\pm1$. The difference here is that we used a different method to determine which α satisfy $N(\alpha)=\pm1$.

7.2 Unique factorization in $\mathbb{Z}[\zeta_5]$.

Next up we would like to determine whether or not we have unique factorization up to units in the ring $\mathbb{Z}[\zeta]$. Again by following Theorem 2.1, it is enough to show that $\mathbb{Z}[\zeta]$ is a Euclidean domain.

Theorem 7.3 *The ring $\mathbb{Z}[\zeta]$ is a Euclidean domain, hence a factorization domain*

Proof: We are going to follow along the notes from Italian mathematician Gemma Branchini [1]

According to Definition 2.5, it is enough to show that there exists a map $\Phi:\mathbb{Z}[\zeta]\backslash\{0\}\to\mathbb{N}$ such that given any $m,n\in\mathbb{Z}[\zeta]$ where n is nonzero, there exists q and r such that $m=nq+r$ where either $r=0$ or $\Phi(r)<\Phi(n)$. We will take the norm as defined previously and show this one satisfies. Quickly recall Equation 7.1 as

$$N(\alpha)=N(g(\zeta))=g(\zeta)\cdot g(\zeta^2)\cdot g(\zeta^3)\cdot g(\zeta^4).$$

First we extend the norm function into $\mathbb{Q}[\zeta]$ by the natural extension $N(\frac{a}{b}):=\frac{N(a)}{N(b)}$. We inspect the number $\frac{m}{n}$ to find a nice representation for us. Because $\frac{m}{n}\in\mathbb{Q}[\zeta]$, there exist $q_i\in\mathbb{Q}$ such that $\frac{m}{n}=q_0+q_1\zeta+q_2\zeta^2+q_3\zeta^3+q_4\zeta^4$. Because each $q_i\in\mathbb{Q}$ we can find $r_i\in\mathbb{Z}$ and $\epsilon_i\in\mathbb{Q}$ such that $q_i=r_i+\epsilon_i$ where $0\le\epsilon_i<1$. Therefore we can split $\frac{m}{n}$ up as

$$\begin{aligned}\frac{m}{n} &= q_0 + q_1\zeta + q_2\zeta^2 + q_3\zeta^3 + q_4\zeta^4 \\ &= (r_0 + r_1\zeta + r_2\zeta^2 + r_3\zeta^3 + r_4\zeta^4) + (\epsilon_0 + \epsilon_1\zeta + \epsilon_2\zeta^2 + \epsilon_3\zeta^3 + \epsilon_4\zeta^4)\end{aligned}$$

where the $r_i\zeta^i$ part is in $\mathbb{Z}[\zeta]$ and the $\epsilon_i\zeta^i$ part is in $\mathbb{Q}[\zeta]$. Now we will use the expression

$$1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 = 0$$

to express ϵ_0 in terms of powers of ζ and add those to the other non integer part to obtain the relation

$$\begin{aligned}&\epsilon_0 + \epsilon_1\zeta + \epsilon_2\zeta^2 + \epsilon_3\zeta^3 + \epsilon_4\zeta^4 \\ &= \epsilon_0(-\zeta - \zeta^2 - \zeta^3 - \zeta^4) + \epsilon_1\zeta + \epsilon_2\zeta^2 + \epsilon_3\zeta^3 + \epsilon_4\zeta^4 \\ &= (\epsilon_1 - \epsilon_0)\zeta + (\epsilon_2 - \epsilon_0)\zeta^2 + (\epsilon_3 - \epsilon_0)\zeta^3 + (\epsilon_4 - \epsilon_0)\zeta^4.\end{aligned}$$

Now we can say without loss of generality that $|\epsilon_i - \epsilon_0| \leq \frac{1}{2}$. Suppose otherwise, then we can do a $\pm\zeta^i$ to make $|\epsilon_i - \epsilon_0|$ smaller by at most 1 and this operation can be canceled out in the $\mathbb{Z}[\zeta]$ part by doing the inverse operation. For example the number $\beta = 2 + \frac{4}{5}\zeta$ has $|\frac{4}{5}| \not\leq \frac{1}{2}$ however by applying a "$-\zeta$" on the $\mathbb{Q}[\zeta]$ part and a "$+\zeta$" on the $\mathbb{Z}[\zeta]$ part we can also write $\beta = 2 + \zeta - \frac{1}{5}\zeta$ where now for the rational part indeed $|\frac{-1}{5}| \leq \frac{1}{2}$. Therefore we are indeed allowed to assume that $|\epsilon_i - \epsilon_0| \leq \frac{1}{2}$. Letting the $\mathbb{Z}[\zeta]$ part be A and the $\mathbb{Q}[\zeta]$ part be α shows that we can write

$$\frac{m}{n} = A + \alpha \text{ where } A \in \mathbb{Z}[\zeta] \text{ and } \alpha = a\zeta + b\zeta^4 + c\zeta^2 + d\zeta^3 \in \mathbb{Q}[\zeta] : |a|, |b|, |c|, |d| \leq \frac{1}{2}.$$

These a, b, c, d we reference to as the coefficients of α. We now aim for the result that $N(\alpha) < 1$ as then we find that

$$\begin{aligned}\frac{m}{n} = A + \alpha \Rightarrow m &= An + \alpha n \\ &\Rightarrow N(\alpha \cdot n) = N(\alpha) \cdot N(n) < N(n)\end{aligned}$$

which shows that $\mathbb{Z}[\zeta]$ is euclidean. Letting $\alpha = g(\zeta)$ to compute the norm we make the following computations.

$$N(\alpha) = (g(\zeta) \cdot g(\zeta^4)) \cdot (g(\zeta^2) \cdot g(\zeta^3))$$

Setting $P := g(\zeta) \cdot g(\zeta^4) = |g(\zeta)|^2$ and $Q := g(\zeta^2) \cdot g(\zeta^3) = |g(\zeta^2)|^2$ yields that $N(\alpha) = P \cdot Q$. Now one can compute and verify that

$$\begin{aligned}
P = g(\zeta) \cdot g(\zeta^4) &= (a\zeta + b\zeta^4 + c\zeta^2 + d\zeta^3) \cdot (a\zeta^4 + b\zeta^{16} + c\zeta^8 + d\zeta^{12}) \\
&= (a\zeta + b\zeta^4 + c\zeta^2 + d\zeta^3) \cdot (b\zeta^4 + a\zeta^1 + d\zeta^2 + c\zeta^3) \\
&= (a^2 + b^2 + c^2 + d^2) + (\zeta^2 + \zeta^3)(ab + ad + bc) \\
&\quad + (\zeta + \zeta^4)(ac + bd + cd) \\
Q = g(\zeta^2) \cdot g(\zeta^3) &= (a\zeta + b\zeta^4 + c\zeta^2 + d\zeta^3) \cdot (a\zeta^3 + b\zeta^{12} + c\zeta^6 + d\zeta^9) \\
&= (a\zeta + b\zeta^4 + c\zeta^2 + d\zeta^3) \cdot (c\zeta + d\zeta^4 + b\zeta^2 + a\zeta^3) \\
&= (a^2 + b^2 + c^2 + d^2) + (\zeta + \zeta^4)(ab + ad + bc) \\
&\quad + (\zeta^2 + \zeta^3)(ac + bd + cd)
\end{aligned}$$

By adding these two equation we obtain

$$\begin{aligned}
P + Q &= [(a^2 + b^2 + c^2 + d^2) + (\zeta^2 + \zeta^3)(ab + ad + bc) + (\zeta + \zeta^4)(ac + bd + cd)] \\
&\quad + [(a^2 + b^2 + c^2 + d^2) + (\zeta + \zeta^4)(ab + ad + bc) + (\zeta^2 + \zeta^3)(ac + bd + cd)] \\
&= 2(a^2 + b^2 + c^2 + d^2) + (\zeta + \zeta^2 + \zeta^3 + \zeta^4)(ab + ac + ad + bc + bd + bc) \\
&= 2(a^2 + b^2 + c^2 + d^2) - (ab + ac + ad + bc + bd + cd) \\
\Rightarrow 2(P + Q) &= 4(a^2 + b^2 + c^2 + d^2) - 2(ab + ac + ad + bc + bd + cd) \\
&= 5(a^2 + b^2 + c^2 + d^2) - (a + b + c + d)^2.
\end{aligned}$$

Now note that we have the following expressions with regards to α.

- $\zeta \cdot \alpha = \zeta \cdot (a\zeta + b\zeta^4 + c\zeta^2 + d\zeta^3) = a\zeta^2 + b + c\zeta^3 + d\zeta^4 = -b\zeta + (d - b)\zeta^4 + (a - b)\zeta^2 + (c - b)\zeta^3$
- $\zeta^2 \cdot \alpha = \zeta^2 \cdot (a\zeta + b\zeta^4 + c\zeta^2 + d\zeta^3) = a\zeta^3 + b\zeta + c\zeta^4 + d = (b - d)\zeta + (c - d)\zeta^4 - d\zeta^2 + (a - d)\zeta^3$
- $\zeta^3 \cdot \alpha = \zeta^3 \cdot (a\zeta + b\zeta^4 + c\zeta^2 + d\zeta^3) = a\zeta^4 + b\zeta^2 + c + d\zeta = (d - c)\zeta + (a - c)\zeta^4 + (b - c)\zeta^2 - c\zeta^3$
- $\zeta^4 \cdot \alpha = \zeta^4 \cdot (a\zeta + b\zeta^4 + c\zeta^2 + d\zeta^3) = a + b\zeta^3 + c\zeta + d\zeta^2 = (c - a)\zeta - a\zeta^4 + (d - a)\zeta^2 + (b - a)\zeta^3$

One may observe that if we have $\frac{m}{n} = A + \alpha$, then $\frac{\zeta^i m}{n} = \zeta^i A + \zeta^i \alpha$. Now the norm of all these numbers does not changed as $N(u \cdot \beta) = N(\beta)$ when u is a unit, because of this we can actually find some better bounds on $|a|, |b|, |c|, |d|$ because multiplying the equation by a unit leaves all the norms exactly the same.

Now we claim that there are in fact two possible cases that we need to consider for our α due to the fact that we can replace it by $\zeta^i \alpha$ terms to keep the norm the same yet change coefficients. The cases are the following:

- Case A is that at least two out of the a, b, c, d satisfy that $|...| \leq \frac{1}{4}$.
- Case B is that one out of a, b, c, d satisfies $|...| \leq \frac{1}{4}$ while two of the remaining coefficients satisfy $|...| + |...| \leq \frac{3}{4}$.

We will show that any α can be put in one of these two cases using clever transformations. First we can see that one of the coefficients of α can always be taken to have $|...| < \frac{1}{4}$. This is because if all the coefficients of α exceed $\frac{1}{4}$ in absolute value, we can take two of them with the same sign (which is possible by the pigeonhole principle) and replace α by $\zeta^i\alpha$ for an appropriate i. For example if a and c have the same sign we can replace α by $\zeta^4\alpha$ to get a new coefficient somewhere that equals $c - a$. Since a and c have the same sign and because $\frac{1}{4} < |a|, |c| \leq \frac{1}{2}$ we find that $|c - a| \leq \frac{1}{4}$. All other coefficients can then be made such that $|...| \leq \frac{1}{2}$ again by adding or subtracting corresponding ζ^i if necessary. Hence we can always take one of the coefficients of α to have $|...| \leq \frac{1}{4}$.

Now if α is such that there are more coefficients with $|...| \leq \frac{1}{4}$ then we are in case A, therefore assume this to not be true now. So one of a, b, c, d has $|...| \leq \frac{1}{4}$ while the other three have $\frac{1}{4} < |...| \leq \frac{1}{2}$. For the demonstration we assume d to be such that $|d| \leq \frac{1}{4}$ but one can replace d by a different coefficient by also choosing a different yet consistent value of i for the $\zeta^i\alpha$ replacement. If we assume that the three remaining coefficients have the same sign, so that being a, b and c, then one can replace α by $\zeta^4\alpha$ to obtain the coefficients $c - a$ and $b - a$ which will then satisfy $|c - a|, |b - a| \leq \frac{1}{4}$ while $-a$ and $d - a$ can be forced into the interval $\left(\frac{-1}{2}, \frac{1}{2}\right)$ again by adding or subtracting a ζ^2 or ζ^4 term if needed. Since now at least two out of the four coefficients satisfy $|...| \leq \frac{1}{4}$ we land in case A.

Therefore now assume that $|d| \leq \frac{1}{4}$ and that only two out of a, b, c have the same sign. Again for the demonstration we take one case, here a and b to have the same sign while assuming c has opposite sign, but one can verify the other cases give similar outcomes by choosing different values of i for the $\zeta^i\alpha$ transformations. Now because a and c have different sign we can consider two situations.

1. If it holds that $|a| + |c| \leq \frac{3}{4}$ we land in case B as $|d| \leq \frac{1}{4}$ was also assumed.
2. If it holds that $|a| + |c| > \frac{3}{4}$ we replace α by $\zeta^4\alpha$ to obtain coefficient $b - a$ which has $|b - a| \leq \frac{1}{4}$ as a and b were assumed to have the same sign. Furthermore the coefficient $c - a$ satisfies $1 \geq |c - a| \geq \frac{3}{4}$ because a and c were assumed to be different sign, however adding or subtracting a power of ζ^4 will make this new coefficient satisfy $|...| \leq \frac{1}{4}$. As two out of the four coefficients now satisfy $|...| \leq \frac{1}{4}$ we land in case A.

Therefore we can always assume α to be as in one of the two cases described above. Now we will show that $N(\alpha) < 1$ in both these cases. In case A we have that two out of the a, b, c, d satisfy that $|...| \leq \frac{1}{4}$. Now we combine that with the fact that $(a + b + c + d)^2 \geq 0$ to obtain

$$\begin{aligned}
2(P+Q) &= 5(a^2+b^2+c^2+d^2) - (a+b+c+d)^2 \\
&\leq 5(a^2+b^2+c^2+d^2) \\
&\leq 5\left(\frac{1}{4}+\frac{1}{4}+\frac{1}{16}+\frac{1}{16}\right) = 5\cdot\left(\frac{5}{8}\right) = \frac{25}{8} \\
\Rightarrow P+Q &\leq \frac{25}{16}.
\end{aligned}$$

Now because both P and Q are positive numbers, $P = |g(\zeta)|^2, Q = |g(\zeta^2)|^2$, the numbers $\sqrt{P}$ and $\sqrt{Q}$ are well defined in $\mathbb{R}$. Therefore we can obtain the simple relation

$$\begin{aligned}
(\sqrt{P}-\sqrt{Q})^2 \geq 0 &\Rightarrow P - 2\sqrt{PQ} + Q \geq 0 \\
&\Rightarrow P+Q \geq 2\sqrt{PQ} \\
&\Rightarrow \frac{P+Q}{2} \geq \sqrt{PQ} \\
&\Rightarrow \frac{1}{4}\cdot(P+Q)^2 \geq PQ
\end{aligned}$$

Therefore we obtain

$$N(\alpha) = P\cdot Q \leq \frac{1}{4}\cdot(P+Q)^2 \leq \frac{1}{4}\cdot\left(\frac{25}{16}\right)^2 = \left(\frac{25}{32}\right)^2 < 1$$

which proves that $N(\alpha) < 1$ in case A. In case B we have that one out of the a, b, c, d satisfies $|...| \leq \frac{1}{4}$ while two of the remaining coefficients satisfy $|...| + |...| \leq \frac{3}{4}$. Now the trick is that from this condition we can also bound the sum of squares right now. Namely observe that if $|x|+|y| \leq \frac{3}{4}$ and $\frac{1}{4} < |x|, |y| \leq \frac{1}{2}$ we find that

$$\begin{aligned}
x^2+y^2 = |x|^2+|y|^2 &\leq |x|^2 + \left(\frac{3}{4}-|x|\right)^2 \\
&= 2|x|^2 - \frac{3}{2}\cdot|x| + \frac{9}{16} \\
&\leq \frac{5}{16}.
\end{aligned}$$

Note that $|x| + |y| \leq \frac{3}{4}$ implies $|y| \leq \frac{3}{4} - |x|$ and that the function $f(u) = 2u^2 - \frac{3}{2}u + \frac{9}{16}$ for $\frac{1}{4} < u \leq \frac{1}{2}$ satisfies $f(u) \leq \frac{5}{16}$, here u has the same bounds as $|x|$. So for the two coefficients that satisfy $|...| + |...| \leq \frac{3}{4}$ we know that $(...)^2 + (...)^2 \leq \frac{5}{16}$. Since from the two remaining coefficients one has $|...| \leq \frac{1}{4}$ and the other has $|...| \leq \frac{1}{2}$ we find that

$$\begin{aligned}
2(P+Q) &= 5(a^2+b^2+c^2+d^2) - (a+b+c+d)^2 \\
&\leq 5(a^2+b^2+c^2+d^2) \\
&\leq 5\left(\frac{1}{4}+\frac{1}{16}+\frac{5}{16}\right) = 5\cdot\left(\frac{5}{8}\right) = \frac{25}{8} \\
\Rightarrow P+Q &\leq \frac{25}{16}.
\end{aligned}$$

Using the earlier obtained bound that $PQ \leq \frac{1}{4}\cdot(P+Q)^2$ we conclude that

$$N(\alpha) = P\cdot Q \leq \frac{1}{4}\cdot(P+Q)^2 \leq \frac{1}{4}\cdot\left(\frac{25}{16}\right)^2 = \left(\frac{25}{32}\right)^2 < 1$$

which proves that $N(\alpha) < 1$ in case B, hence $N(\alpha) < 1$ for both possible cases, hence we can finish up the proof.

The result we obtain is then that for any $m, n \in \mathbb{Z}[\zeta]$ where n is nonzero there exists some $q \in \mathbb{Z}[\zeta]$ such that $N\left(\frac{m}{n} - q\right) = N(\frac{m}{n} - A) = N(\alpha) < 1$ which leads us to there existing an $r \in \mathbb{Z}[\zeta]$ such that $m = nq + r$ where $r = 0$ or $N(r) < N(n)$ which shows that $\mathbb{Z}[\zeta]$ is indeed a Euclidean domain and hence a unique factorization domain by Theorem 2.1.

Q.E.D.

The strategies that we used in Theorem 3.1, Theorem 5.1 and Theorem 7.3 to prove that respectively $\mathbb{Z}[\zeta_3], \mathbb{Z}[i]$ and $\mathbb{Z}[\zeta_5]$ are a UFD are very similar. Namely in all three proofs we used the previously defined norm function $N(.)$ and used that to determine that the rings are Euclidean domains as according to Definition 2.5. The only difference is that for $\mathbb{Z}[\zeta_3]$ and $\mathbb{Z}[i]$ this was easier due to the more regular structure of these rings. In $\mathbb{Z}[\zeta_5]$ we had to obtain more results which allowed us to conclude the proof. It's very interesting to see that the rings $\mathbb{Z}[\zeta_n]$ are all a Euclidean domain for the first couple of values for n, it begs the question then whether this is a property that is always valid. This is something that we return to in Chapter 9.

8 Proving Fermat's last theorem for $n = 5$

Using our obtained results about the ring $\mathbb{Z}[\zeta_5]$ we are now able to prove that the equation $x^5+y^5 = z^5$ has no nontrivial solutions in $\mathbb{Z}$. The whole structure of the proof follows the $n = 3$ case done earlier very closely. The main ideas are the same yet a couple parts need to be changed accordingly. We split the proof up into two parts, one where we consider xyz to not be divisible by 5 and in the other part we consider the case where xyz is divisible by 5. Again this split has to do with the fact that in the ring $\mathbb{Z}[\zeta]$ it is true that $1-\zeta$ divides 5. One can verify that $5 = (1-\zeta)^4 \cdot (\zeta^3 - \zeta - 1)$ where $\zeta^3 - \zeta - 1 = \zeta^3 \cdot \left(\frac{1+\sqrt{5}}{2}\right)^2$ which is a unit according to the form we found in Theorem 7.2. We first prove the first case.

Lemma 8.1 *The equation $x^5 + y^5 = z^5$ has no solution over the integers whenever xyz is not divisible by 5.*

Proof: The proof is very similar to what we did in the $n = 3$ case, namely we are going to use some simple modular arithmetic. Since xyz is not divisible by 5 we know that x, y and z are also not divisible by 5 because 5 is a prime number in $\mathbb{Z}$. Hence $x, y, z \equiv 1, 2, 3$ or $4 \pmod 5$. We now look at the equation $x^5 + y^5 = z^5 \pmod{25}$, first we check each fifth power $\pmod{25}$ to obtain the following values.

$$x \equiv 1 \pmod 5 \Rightarrow x^5 \equiv 1 \pmod{25}, x \equiv 2 \pmod 5 \Rightarrow x^5 \equiv 7 \pmod{25}$$
$$x \equiv 3 \pmod 5 \Rightarrow x^5 \equiv 18 \pmod{25}, x \equiv 4 \pmod 5 \Rightarrow x^5 \equiv 24 \pmod{25}.$$

These are also all the possible values of $y^5 \pmod{25}$ and $z^5 \pmod{25}$. Therefore if we reduce $\pmod{25}$ in $x^5 + y^5 = z^5$, the left side satisfies $x^5 + y^5 \equiv 0, 2, 6, 8, 11, 14, 17, 19$ or $23 \pmod{25}$ whereas the right side satisfies $z^5 \equiv 1, 7, 18$ or $24 \pmod{25}$. Since the two sides are never equal $\pmod{25}$ they are also never equal in general, hence the equation $x^5 + y^5 = z^5$ has no solutions when xyz is not divisible by 5.

Q.E.D.

The following lemma tells us something about the reducibility of the number $1 - \zeta$.

Lemma 8.2 *The number $1 - \zeta$ is irreducible in $\mathbb{Z}[\zeta]$. That is the only divisors of $1 - \zeta$ are itself, units and products of those two numbers.*

Proof: Note that we compute the norm of $1 - \zeta$ to be

$$\begin{aligned} N(1-\zeta) = N(g(\zeta)) &= g(\zeta) \cdot g(\zeta^2) \cdot g(\zeta^3) \cdot g(\zeta^4) \\ &= (1-\zeta) \cdot (1-\zeta^2) \cdot (1-\zeta^3) \cdot (1-\zeta^4) \\ &= (1-\zeta-\zeta^2+\zeta^3) \cdot (1-\zeta^3-\zeta^4+\zeta^2) \\ &= (1-\zeta-\zeta^2+\zeta^3)(2+\zeta+2\zeta^2) \\ &= 2+\zeta+2\zeta^2-2\zeta-\zeta^2-2\zeta^3 \\ &- 2\zeta^2-\zeta^3-2\zeta^4+2\zeta^3+\zeta^4+2\zeta^5 \\ &= 2-\zeta-\zeta^2-\zeta^3-\zeta^4+2\zeta^5 \\ &= 2+2-(\zeta+\zeta^2+\zeta^3+\zeta^4) = 2+2-(-1) = 5. \end{aligned}$$

Therefore if $1 - \zeta = A \cdot B$ for some $A, B \in \mathbb{Z}[\zeta]$, it holds that $5 = N(1-\zeta) = N(A \cdot B) = N(A) \cdot N(B)$ showing that either $N(A) = 1$ or $N(B) = 1$. Therefore either A or B is a unit from which we can conclude that $1 - \zeta$ is indeed irreducible in $\mathbb{Z}[\zeta]$.

Q.E.D.

So, just like in the $n = 3$ and $n = 4$ case the number $1 - \zeta$ is irreducible in the ring $\mathbb{Z}[\zeta]$. To continue with the second case of Fermat's last theorem for $n = 5$ we are again going to show that a more complicated equation has no solution from which the desired result follows. First we can assume without loss of generality that the z term is divisible by 5 and therefore x and y are not. The argument for this is the same as with the $n = 3$ case. We are going to show that the equation

$$x^5 + y^5 = u((1-\zeta)^k z)^5 \tag{8.1}$$

has no solution in $\mathbb{Z}[\zeta]$ where u is a unit, $k \geq 1$ is an integer, x, y and z are pairwise co-prime and xyz is not divisible by $1 - \zeta$. If this equation has no solution in $\mathbb{Z}[\zeta]$, then the equation $x^5 + y^5 = z^5$ has no solution in $\mathbb{Z}$ where x, y, z are pairwise co-prime and z is divisible by 5. This can be deduced by observing that solutions to $x^5 + y^5 = z^5$ in $\mathbb{Z}$ also solve Equation **??** in a similar way as we described in the $n = 3$ case. It remains for us to then show the following.

Theorem 8.1 *The equation $x^5 + y^5 = u((1-\zeta)^k z)^5$ for u a unit, $k \geq 1$ an integer, x, y and z relatively co-prime and xyz not divisible by $1 - \zeta$ has no solution for $x, y, z \in \mathbb{Z}[\zeta]$.*

Proof: We start of by giving the structure of the proof, as we are going to do a proof by infinite descent. We aim to show the following two statements from which we can conclude no solution exists.

1. If a solution exists, then $k \geq 2$.
2. If there is a solution for $k \geq 2$, then there is also a solution for k being replaced by $k - 1$.

If these statements hold, then we can indeed conclude that there are no solutions to

$$x^5 + y^5 = u((1-\zeta)^k z)^5$$

over $\mathbb{Z}[\zeta]$. We first proof the first statement, hence suppose a solutions exists for some $k \geq 1$. To help us with the proof, instead of writing elements of $\mathbb{Z}[\zeta]$ as $a + b\zeta + c\zeta^2 + d\zeta^3$ we opt for a slightly different style of writing, namely

- $x = a_0 + a_1(1-\zeta) + a_2(1-\zeta)^2 + a_3(1-\zeta)^3$
- $y = b_0 + b_1(1-\zeta) + b_2(1-\zeta)^2 + b_3(1-\zeta)^3$

where the a_i and b_i are integers. Both x and y are not divisible by $1-\zeta$, from this it follows that a_0 and b_0 are not divisible by 5. This is because we showed 5 is a multiple of $1-\zeta$. If a_0 were to be divisible by 5, it then follows that x is divisible by $1-\zeta$ from the form $x = a_0 + a_1(1-\zeta) + a_2(1-\zeta)^2 + a_3(1-\zeta)^3$ however we assumed it not to be.

Now if we have a solution to Equation 8.1, replacing y by $\zeta^j y$ still yields a valid solution as $y^5 = (\zeta^j y)^5$. This motivates us to look into $\zeta^j y$. For any $j \geq 0$ we have the following relation.

$$\begin{aligned}
\zeta^j y &= (1-(1-\zeta))^j (b_0 + b_1(1-\zeta) + b_2(1-\zeta)^2 + b_3(1-\zeta)^3) \\
&\equiv (1-(1-\zeta))^j (b_0 + b_1(1-\zeta)) \pmod{(1-\zeta)^2} \\
&\equiv (1-j(1-\zeta))(b_0 + b_1(1-\zeta)) \pmod{(1-\zeta)^2} \\
&\equiv b_0 + (b_1 - jb_0)(1-\zeta) \pmod{(1-\zeta)^2}.
\end{aligned}$$

Next up we pick j such that $a_1 + b_1 - jb_0 \equiv 0 \pmod 5$. This j always exists because b_0 is not a multiple of 5, therefore $(b_0)^{-1} \pmod 5$ exists. For this specific j we see that

$$\begin{aligned}
x + \zeta^j y &= a_0 + a_1(1-\zeta) + a_2(1-\zeta)^2 + a_3(1-\zeta)^3 \\
&\quad + \zeta^j (b_0 + b_1(1-\zeta) + b_2(1-\zeta)^2 + b_3(1-\zeta)^3) \\
&\equiv a_0 + a_1(1-\zeta) + b_0 + (b_1 - jb_0)(1-\zeta) \pmod{(1-\zeta)^2} \\
&\equiv a_0 + b_0 + (a_1 + b_1 - jb_0)(1-\zeta) \pmod{(1-\zeta)^2} \\
&\equiv a_0 + b_0 \pmod{(1-\zeta)^2}
\end{aligned}$$

where we used that $a_1 + b_1 - jb_0$ is a multiple of 5, hence a multiple of $1-\zeta$. Now there exist integers c_i, d_i, e_i and f_i such that

- $\zeta y = c_0 + c_1(1-\zeta) + c_2(1-\zeta)^2 + c_3(1-\zeta)^3$
- $\zeta^2 y = d_0 + d_1(1-\zeta) + d_2(1-\zeta)^2 + d_3(1-\zeta)^3$
- $\zeta^3 y = e_0 + e_1(1-\zeta) + e_2(1-\zeta)^2 + e_3(1-\zeta)^3$
- $\zeta^4 y = f_0 + f_1(1-\zeta) + f_2(1-\zeta)^2 + f_3(1-\zeta)^3$.

We aim for the result that $b_0 \equiv c_0 \equiv d_0 \equiv e_0 \equiv f_0 \pmod{(1-\zeta)^2}$. From the expression $\zeta^j y = b_0 + (b_1 - jb_0)(1-\zeta) + K(1-\zeta)^2$, where $K \in \mathbb{Z}[\zeta]$, we can see that the c_0, d_0, e_0 and f_0 terms are now only influenced by the b_0 term and the $K(1-\zeta)^2$ term. The latter one is irrelevant after reducing $\pmod{(1-\zeta)^2}$ leaving just b_0. Hence we have the result that $b_0 \equiv c_0 \equiv d_0 \equiv e_0 \equiv f_0 \pmod{(1-\zeta)^2}$ This then implies that

$$\begin{aligned} x + \zeta^j y &\equiv a_0 + b_0 \pmod{(1-\zeta)^2} \equiv a_0 + c_0 \pmod{(1-\zeta)^2} \\ &\equiv a_0 + d_0 \pmod{(1-\zeta)^2} \equiv a_0 + e_0 \pmod{(1-\zeta)^2} \\ &\equiv a_0 + f_0 \pmod{(1-\zeta)^2} \end{aligned}$$

which means that after replacing y by $\zeta^j y$, we can find a representation of $x + \zeta^j y \pmod{(1-\zeta)^2}$ that uses a_0 from how x was written and one of b_0, c_0, d_0, e_0, f_0 depending on what our value of j is. We can pick the corresponding correct terms and because of this replacement property we can say that, without loss of generality, $x + y \equiv a_0 + b_0 \pmod{(1-\zeta)^2}$.

Now we also find that $x + \zeta^i y \equiv x + y \pmod{1-\zeta} \equiv a_0 + b_0 \pmod{1-\zeta}, \forall i \geq 0$ using that $\zeta \equiv 1 \pmod{1-\zeta}$. Returning to our original equation $x^5 + y^5 = u((1-\zeta)^k z)^5$, we see that the left sides factors into

$$x^5 + y^5 = (x+y)(x+\zeta y)(x+\zeta^2 y)(x+\zeta^3 y)(x+\zeta^4 y)$$

inside $\mathbb{Z}[\zeta]$. Because the right-hand side of $x^5 + y^5 = u((1-\zeta)^k z)^5$ is divisible by $1-\zeta$, so is the left-hand side. Therefore we find that

$$\begin{aligned} 0 &\equiv x^5 + y^5 \pmod{1-\zeta} \\ &\equiv (x+y)(x+\zeta y)(x+\zeta^2 y)(x+\zeta^3 y)(x+\zeta^4 y) \pmod{1-\zeta} \\ &\equiv (a_0+b_0)(a_0+b_0)(a_0+b_0)(a_0+b_0)(a_0+b_0) \pmod{1-\zeta} \\ &\equiv (a_0+b_0)^5 \pmod{1-\zeta}. \end{aligned}$$

Because $1-\zeta$ is irreducible and divides $(a_0+b_0)^5$, it is actually true that it divides a_0+b_0. Now I make the following claim:

$$\mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}[\zeta]/(1-\zeta)\mathbb{Z}[\zeta] \tag{8.2}$$

This can be done by defining the following map, $\Phi : \mathbb{Z}[\zeta]/(1-\zeta)\mathbb{Z}[\zeta] \to \mathbb{Z}/5\mathbb{Z}$ by $\Phi(a + b\zeta + c\zeta^2 + d\zeta^3) = \overline{a+b+c+d}$. This works as $a + b\zeta + c\zeta^2 + d\zeta^3 \equiv a + b + c + d \pmod{1-\zeta}$ so the map Φ is in fact the natural map between the two objects. Because both 5 and $1-\zeta$ are irreducible in respectively $\mathbb{Z}$ and $\mathbb{Z}[\zeta]$, both the domain and co-domain of Φ are fields. Combined with the observation that Φ is a surjective map it follows that both of the fields are actually isomorphic. The important thing is then that zeroes in $\mathbb{Z}[\zeta]/(1-\zeta)\mathbb{Z}[\zeta]$ correspond to zeroes in $\mathbb{Z}/5\mathbb{Z}$.

Since $a_0 + b_0$ is divisible by $1-\zeta$, it corresponds to $\overline{0}$ in $\mathbb{Z}[\zeta]/(1-\zeta)\mathbb{Z}[\zeta]$. Because $a_0 + b_0 \in \mathbb{Z}$ and $\Phi|_{\mathbb{Z}} = id|_{\mathbb{Z}}$ we can conclude that $a_0 + b_0$ is a multiple of 5, hence $a_0 + b_0 \equiv 0 \pmod{5}$. In particular $a_0 + b_0 \equiv 0 \pmod{(1-\zeta)^2}$.

Because we had the equivalence $x+y \equiv a_0+b_0 \pmod{(1-\zeta)^2}$ it also shows that $x+y$ is divisible by $(1-\zeta)^2$. We can therefore say the following thing about $x^5+y^5 = (x+y)(x+\zeta y)(x+\zeta^2 y)(x+\zeta^3 y)(x+\zeta^4 y)$.

- We have $x + y \equiv 0 \pmod{(1-\zeta)^2}$.
- We have $x + \zeta y \equiv a_0 + b_0 \pmod{1-\zeta} \equiv 0 \pmod{1-\zeta}$ because 5 is divisible by $1-\zeta$.
- We have $x + \zeta^2 y \equiv a_0 + b_0 \pmod{1-\zeta} \equiv 0 \pmod{1-\zeta}$ because 5 is divisible by $1-\zeta$.
- We have $x + \zeta^3 y \equiv a_0 + b_0 \pmod{1-\zeta} \equiv 0 \pmod{1-\zeta}$ because 5 is divisible by $1-\zeta$.
- We have $x + \zeta^4 y \equiv a_0 + b_0 \pmod{1-\zeta} \equiv 0 \pmod{1-\zeta}$ because 5 is divisible by $1-\zeta$.

So after multiplying everything we find that $x^5 + y^5$ is divisible by $(1-\zeta)^6$. Going back to $x^5 + y^5 = u((1-\zeta)^k z)^5$ we now see that the left side is divisible by $(1-\zeta)^6$, therefore also the right side should be divisible by $(1-\zeta)^6$. Since u is a unit and z was assumed to not be divisible by $1-\zeta$ we must have that $k \geq 2$ as since if k were to equal 1, the right side is only divisible by $(1-\zeta)^5$ but not by the sixth power. This proves the first statement which said that if a solution exists, then $k \geq 2$.

To now prove the second statement, we take a solution for a certain $k \geq 2$ and try to construct a solution where k is now replaced by $k-1$. Because x and y were said to be co-prime, it also follows that the numbers $\frac{x+\zeta^a y}{1-\zeta}$ and $\frac{x+\zeta^b y}{1-\zeta}$ are co-prime where without loss of generality $0 \leq a < b < 5$. The proof of this small observation is exactly the same as in the $n = 3$ case so we omit it here. Returning to the equation $x^5 + y^5 = u((1-\zeta)^k z)^5$, one factors the left side as before to obtain

$$(x+y)(x+\zeta y)(x+\zeta^2 y)(x+\zeta^3 y)(x+\zeta^4 y) = u((1-\zeta)^k z)^5.$$

Because the product of five numbers with only one common divisor equals a fifth power we can make the following factorization, which is unique because in Theorem 7.3 we showed that $\mathbb{Z}[\zeta]$ is a Euclidean domain and therefore a unique factorization domain.

- $x + y = u_0(1-\zeta) \cdot (1-\zeta)^{5(k-1)} \cdot (t_0)^5$
- $x + \zeta y = u_1(1-\zeta) \cdot (t_1)^5$
- $x + \zeta^2 y = u_2(1-\zeta) \cdot (t_2)^5$
- $x + \zeta^3 y = u_3(1-\zeta) \cdot (t_3)^5$
- $x + \zeta^4 y = u_4(1-\zeta) \cdot (t_4)^5$

Here each u_i is a unit, each t_i is not divisible by $1-\zeta$ and all t_i's are relatively co-prime as well. The reasoning that this is the correct factorization is the same as in the $n = 3$ case from before.

The fact that $x + y$ contains all other powers of $1 - \zeta$ will come in handy in constructing the new solution. Observe namely the following expression:

$$\begin{aligned}(x + \zeta y) + \zeta(x + \zeta^4 y) &= x + \zeta y + \zeta x + \zeta^5 y \\ &= x + \zeta x + y + \zeta y \\ &= (1 + \zeta)x + (1 + \zeta)y \\ &= (1 + \zeta)(x + y).\end{aligned}$$

Before we continue one can check that $1 + \zeta = -\zeta^3 \cdot \left(\frac{1+\sqrt{5}}{2}\right)^1$ and that therefore $1 + \zeta$ is a unit by Theorem 7.2. Using the factorization we found for $x + y, x + \zeta y$ and $x + \zeta^4 y$ we obtain the equation

$$u_1(1 - \zeta) \cdot (t_1)^5 + \zeta \cdot u_4(1 - \zeta) \cdot (t_4)^5 = (1 + \zeta) \cdot u_0(1 - \zeta) \cdot (1 - \zeta)^{5(k-1)} \cdot (t_0)^5.$$

After dividing both sides by $1 - \zeta$ we obtain

$$u_1 \cdot (t_1)^5 + \zeta \cdot u_4 \cdot (t_4)^5 = (1 + \zeta) \cdot u_0 \cdot (1 - \zeta)^{5(k-1)} \cdot (t_0)^5.$$

Next we can divide by the unit u_1 and replace $k - 1$ by l for convenience to get the equation

$$(t_1)^5 + \zeta \cdot \frac{u_4}{u_1} \cdot (t_4)^5 = (1 + \zeta) \cdot \frac{u_0}{u_1} \cdot (1 - \zeta)^{5l} \cdot (t_0)^5.$$

Finally to make the reading better we replace $\zeta \cdot \frac{u_4}{u_1}$ by A and $(1 + \zeta) \cdot \frac{u_0}{u_1}$ by B where now A and B are both units because they are a product and quotient of units.

$$(t_1)^5 + A \cdot (t_4)^5 = B \cdot (1 - \zeta)^{5l} \cdot (t_0)^5. \tag{8.3}$$

Now because k was said to be ≥ 2 and $l = k - 1$ we have $l \geq 1$. Therefore $(1 - \zeta)^{5l} = (1 - \zeta)^{5l-4} \cdot (1 - \zeta)^4 \equiv 0 \pmod 5$. This shows that the right side of Equation 8.3 is equivalent to $0 \pmod 5$ which also means that $(t_1)^5 + A \cdot (t_4)^5 \equiv 0 \pmod 5$. Now any $\alpha = a + b\zeta + c\zeta^2 + d\zeta^3$ satisfies $\alpha^5 \equiv a^5 + b^5 + c^5 + d^5 \pmod 5$ and is therefore congruent to a rational integer $\pmod 5$. Because t_i is not a multiple of $1 - \zeta$, we have that $(t_i)^5 \not\equiv 0 \pmod 5$. This shows us that

$$(t_4)^5 \equiv 1, 2, 3, \text{ or } 4 \pmod 5.$$

Hence there exists some integer n such that $n \cdot (t_4)^5 \equiv 1 \pmod 5$. After multiplying Equation 8.3 by n we see that the unit A is a rational integer $\pmod 5$ because $n \cdot (t_1)^5 + An \cdot (t_2)^5 \equiv n \cdot (t_1)^5 + A \pmod 5 \equiv 0 \pmod 5$. Now A is a unit, then by Theorem 7.2 there are integers p and q such that

$$A = \pm(\zeta)^p \cdot \left(\frac{1+\sqrt{5}}{2}\right)^q.$$

First observe that it is enough to check all these numbers where $0 \leq p, q \leq 4$ as the $(\zeta)^p$ can only take on five different values. Furthermore, if we have $q \geq 5$ we can take out some $\left(\frac{1+\sqrt{5}}{2}\right)^5$ terms and factor them into the $(t_4)^5$ in Equation 8.3. Therefore we get these bounds on p and q. Notice that the only values of p and q that produce a rational integer $\pmod 5$ are $p = q = 0$ yielding $A = \pm 1$. Because t_4 can be replaced by $-t_4$ for a solution to Equation 8.3 we only have to look at $A = 1$ which yields

$$\begin{aligned}(t_1)^5 + (t_4)^5 &= B \cdot (1-\zeta)^{5l} \cdot (t_0)^5 \\ &= B((1-\zeta)^l t_0)^5\end{aligned}$$

where we have that B is a unit, $l \geq 1$ is an integer, t_0, t_1 and t_4 are relatively co-prime and all not divisible by $1 - \zeta$. This is exactly our Equation 8.1 from before again, however we have now constructed a solution from a given one where k was replaced by $k - 1 = l$. This proves the second statement which said that if there is a solution for $k \geq 2$, then there is also a solution for k being replaced with $k - 1$.

Therefore we have proven that the equation $x^5 + y^5 = u((1-\zeta)^k z)^5$ for u a unit, $k \geq 1$ an integer, x, y and z relatively co-prime and xyz not divisible by $1 - \zeta$ has no solution for $x, y, z \in \mathbb{Z}[\zeta]$.

Q.E.D.

We have now proven Fermat's last theorem for the case $n = 5$. This is probably the coolest result of this thesis as we had to extend the simple ideas seen in Chapters $3, 4, 5$ and 6 to a ring with the same requirements which were more involved to show. The proof of Fermat for $n = 5$ very closely resembles the proof of Fermat for $n = 3$ as seen in Lemma 4.2 for case 1 and Theorem 4.1 for case 2. The fact that this proof extends so nicely begs the question on which further extensions can be made. Therefore in the next chapter we discuss some results about $\mathbb{Z}[\zeta_n]$, for n prime > 2, and see what we can say about Fermat's last theorem.

9 The ring $\mathbb{Z}[\zeta_n]$ and Fermat for general primes n

We are interested in finding out some more general results about the ring $\mathbb{Z}[\zeta_n]$ where n is prime and use those to say something about Fermat's last theorem. We start of by finding a very general way of describing the units in any such rings $\mathbb{Z}[\zeta_n]$. We rely on results from [8] for the results in this chapter.

9.1 The units of $\mathbb{Z}[\zeta_n]$

We begin with some new notions .

Definition 9.1 *A number $\alpha \in \mathbb{C}$ is called an algebraic integer if it is the root of some monic polynomial with integer coefficients.*

Examples of algebraic integers are $\sqrt{2}$ and $5 - i\sqrt[3]{7}$, as they are roots of $x^2 - 2$ and $(x-5)^6 + 49$ respectively. Examples of non-algebraic integers are π, $\ln(2)$ and $\frac{3}{5} + \frac{4}{5}i$, as the first two numbers are not even algebraic and the minimal polynomial of $\frac{3}{5} + \frac{4}{5}i$ is $f(x) = 5x^2 - 6x + 5$ which means it can never be the root of a monic polynomial with integer coefficients. The nice thing about these algebraic integers is that if we take it's minimal polynomial and expand it in linear factors, the minimal polynomial looks like

$$(x - r_1)(x - r_2)...(x - r_n)$$

where there is no additional factor in front.

Definition 9.2 *The algebraic conjugates of an algebraic element α over a field extension L/K are all the roots of the minimal polynomial of α over K.*

Algebraic conjugates of $\sqrt{2}$ over $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ are $\sqrt{2}$ and $-\sqrt{2}$. Over $\mathbb{R}$ however there is no algebraic conjugate as the minimal polynomial of $\sqrt{2}$ over $\mathbb{R}$ is $f(x) = x - \sqrt{2}$.

Lemma 9.1 *If α is an algebraic integer, all of whose algebraic conjugates have absolute value 1, then α is a root of unity.*

Proof: Let $f(x)$ be the minimal polynomial of α. For notational convenience we write α_j to denote all the conjugates of α where we pick $\alpha_1 := \alpha$. By Definition 9.1 and 9.2, one can write $f(x) = \prod_{j=1}^{d}(x - \alpha_j)$ where d is the degree of $f(x)$. This is just factoring the polynomial in linear terms. Now one is able to also write $f(x)$ as $f(x) = x^d - \sigma_1 x^{d-1} + \sigma_2 x^{d-2} - ... + (-1)^{d-1}\sigma_{d-1}x + (-1)^d\sigma_d$ where

$$\begin{aligned}
\sigma_1 &= \alpha_1 + \alpha_2 + ... + \alpha_d \\
\sigma_2 &= \alpha_1\alpha_2 + \alpha_1\alpha_3 + ... + \alpha_1\alpha_n + \alpha_2\alpha_3 + ... + \alpha_2\alpha_n + ... + \alpha_{d-1}\alpha_d \\
\sigma_3 &= \alpha_1\alpha_2\alpha_3 + ... = \sum_{1\leq i<j<k\leq d} \alpha_i\alpha_j\alpha_k \\
&\vdots \\
\sigma_t &= \sum_{1\leq i_1<i_2<...<i_t\leq d} \alpha_{i_1}\alpha_{i_2}\cdots\alpha_{i_t} \\
&\vdots \\
\sigma_d &= \alpha_1\alpha_2\cdots\alpha_d.
\end{aligned}$$

This is found by expanding the brackets. All these σ_i terms are called the elementary symmetric polynomials in $\{\alpha_1, \alpha_2, ..., \alpha_d\}$. Notice that because $f(x)$ is a polynomial with integer coefficients (as it is the minimal polynomial of α which is an algebraic integer), every σ_i has to be an integer. Therefore $\sigma_i \in \mathbb{Z}, \forall i \in \{1, 2, ..., d\}$. Now for notational convenience we define

$$f_n(x) = \prod_{j=1}^{d}(x - \alpha_j^n). \tag{9.1}$$

Notice that $f_1(x) = f(x)$. If we expand $f_n(x)$ we obtain a polynomial of the form $f_n(x) = x^d + b_{1,n}x^{d-1} + b_{2,n}x^{d-2} + ... + b_{d-1,n}x + b_{d,n}$. Now each $b_{i,n}$ will be symmetric with respect to the α_j terms. This means that if one where to swap the values of any α_{j_1} and α_{j_2}, every b_i is still the same. For example $x^2 + y^2$ and x^3y^3 are symmetric in x and y but $x^2 + xy$ is not. Now we apply a result which we are not going to prove, however this result allows us to say something really important about each $f_n(x)$.

Theorem 9.1 *Any symmetric polynomial $f \in R[x_1, x_2, ..., x_d]$ can be written uniquely as a polynomial in $\sigma_1, \sigma_2, ..., \sigma_d$ with coefficients in R.*

Proof: Theorem 4.1.4 in [2].

This result is called the main theorem of symmetric polynomials. As a consequence of this theorem, each $b_{i,n}$ term is an integer. This is because $b_{i,n}$ was shown to be symmetric with respect to the α_j terms, hence each $b_{i,n}$ is a symmetric polynomial in terms of $\alpha_1, \alpha_2, ..., \alpha_d$ with integer coefficients. Hence by Theorem 9.1 we can write every $b_{i,n}$ term as a unique polynomial in $\sigma_1, \sigma_2, ..., \sigma_d$ with coefficients in $\mathbb{Z}$. Because it was shown that each $\sigma_i \in \mathbb{Z}$, it follows that each $b_{i,n} \in \mathbb{Z}$ as well. Therefore also $f_n(x) = x^d + b_{1,n}x^{d-1} + b_{2,n}x^{d-2} + ... + b_{d-1,n}x + b_{d,n}$ is a polynomial with integer coefficients. This shows that $f_n(x)$ as in Equation 9.1 lies in $\mathbb{Z}[x]$ for all $n \geq 1$.

Now the property that α and all its conjugates have absolute value 1 gives that each

$$|\alpha_j^n| = 1, \forall j \in \{1, 2, ..., d\}, \forall n \in \mathbb{N}_{\geq 1}.$$

Therefore each $b_{i,n}$ is bounded in absolute value by $\binom{r}{i}$. One sees this as each $b_{i,n}$ is a sum of $\binom{r}{i}$ terms, each of which is a product of numbers with absolute value equal to 1. Hence all $f_n(x)$ form polynomials in $\mathbb{Z}[x]$ where the coefficients are bounded by something that is independent of n and of the degree d. It follows that there are only finitely many distinct polynomials $f_n(x)$. Pick k and l such that $k < l$ and $f_k(x) = f_l(x), \forall x \in \mathbb{Z}$. Because the two polynomials are exactly the same, they must have the same roots as well. Therefore $\alpha_j^k = \alpha_j^l, \forall j \in \{1, 2, ..., d\}$. In particular $\alpha^k = \alpha_1^k = \alpha_1^l = \alpha^l$. Since $\alpha \neq 0$, as $|\alpha| = 1$, it shows us that $\alpha^{l-k} = 1$. This shows us that α is indeed a root of unity which finishes the proof of Lemma 9.1.

Q.E.D.

Notice how this result gives an alternative proof to a subpart of Theorem 7.2 describing the units of $\mathbb{Z}[\zeta_5]$. The part in question is about finding the Kernel of ψ which consists of the values α whose algebraic conjugates all have absolute value equal to 1.

Now that we have shown the result from Lemma 9.1, we are able to give a better classification of the units in any ring $\mathbb{Z}[\zeta_n]$ for n being a prime number. First however we require some information about the number $1 - \zeta_n$.

Lemma 9.2 *The number $1 - \zeta_n$ is irreducible in $\mathbb{Z}[\zeta_n]$ when n is prime*

Proof: Suppose that n is a prime number. Following the structure of how we found a norm function for $n = 5$ we define the following functions.

- The map $\sigma_i : \mathbb{Z}[\zeta_n] \to \mathbb{Z}[\zeta_n]$ is defined as the linear map $\sigma_i(\zeta_n) = (\zeta_n)^i$, which is equal to the identity map on $\mathbb{Z}$.
- The map $N : \mathbb{Z}[\zeta_n] \to \mathbb{R}$ is defined by $N(\alpha) = \prod_{i=1}^{n-1}(\sigma_i(\alpha))$.

One can check that the map $N(\alpha)$ is indeed a valid norm function following Definition 2.3. Furthermore it is in fact true that N maps perfectly into $\mathbb{Z}$. Therefore $N(u) = \pm 1$ whenever u is a unit. We are now interested in the norm of the number $\alpha = 1 - \zeta_n$. Following the definition above, one finds that

$$N(1 - \zeta_n) = \prod_{i=1}^{n-1}(\sigma_i(1 - \zeta_n)) = \prod_{i=1}^{n-1}(1 - (\zeta_n)^i).$$

Now the minimal polynomial of ζ_n is given by $f(x) = x^{n-1} + ... + x + 1$. This is the result of Lemma 2.3. In addition to that, all of it's roots are $\{\zeta_n, (\zeta_n)^2, ..., (\zeta_n)^{n-1}\}$ which allows the

following factorization:

$$f(x) = x^{n-1} + ... + x + 1 = \prod_{i=1}^{n-1}(x - (\zeta_n)^i).$$

Plugging in $x = 1$ yields $f(1) = 1^{n-1} + ... + 1 + 1 = n$ however it also yields

$$f(x) = \prod_{i=1}^{n-1}(x - (\zeta_n)^i)$$
$$\Rightarrow f(1) = \prod_{i=1}^{n-1}(1 - (\zeta_n)^i) = N(1 - \zeta_n).$$

Therefore we find that $N(1 - \zeta_n) = n$. Now if we have two elements $A, B \in \mathbb{Z}[\zeta_n]$ such that $1 - \zeta_n = A \cdot B$, then also

$$N(1 - \zeta_n) = N(A \cdot B) = N(A) \cdot N(B) \Rightarrow n = N(A) \cdot N(B).$$

Because n is a prime number, this yields that either $N(A) = \pm 1$ or $N(B) = \pm 1$ and therefore either A is a unit or B is a unit. We conclude that $1 - \zeta_n$ is indeed irreducible in $\mathbb{Z}[\zeta_n]$ if n is a prime number.

Q.E.D.

The following Lemma will be important to us in a bit where we give a general description of units in $\mathbb{Z}[\zeta_n]$.

Lemma 9.3 *Let n be a prime number. The largest totally real subfield of $\mathbb{Q}[\zeta_n]$ is the field $\mathbb{Q}[\zeta_n + (\zeta_n)^{-1}]$.*

Proof: Since $\mathbb{Q}[\zeta_n]$ is a finite extension of $\mathbb{Q}$, the minimal polynomial of ζ_n is $f(x) = x^{n-1} + ... + x + 1$ hence $[\mathbb{Q}[\zeta_n] : \mathbb{Q}] = n - 1$, we would like to find the number $[\mathbb{Q}[\zeta_n] : \mathbb{Q}[\zeta_n + (\zeta_n)^{-1}]]$ as this tells us something about the fields that are in between $\mathbb{Q}[\zeta_n]$ and $\mathbb{Q}[\zeta_n + (\zeta_n)^{-1}]$. Now note that the polynomial $f(x) = x^2 - (\zeta_n + (\zeta_n)^{-1})x + 1$ is a polynomial in $\mathbb{Q}[\zeta_n + (\zeta_n)^{-1}][x]$ and has ζ_n as a root. Indeed,

$$f(\zeta_n) = (\zeta_n)^2 - (\zeta_n + (\zeta_n)^{-1})(\zeta_n) + 1 = (\zeta_n)^2 - (\zeta_n)^2 - 1 + 1 = 0.$$

Therefore $[\mathbb{Q}[\zeta_n] : \mathbb{Q}[\zeta_n + (\zeta_n)^{-1}]] \leq 2$ as we can find a polynomial of degree 2 in $\mathbb{Q}[\zeta_n + (\zeta_n)^{-1}][x]$ that has ζ_n as a root.

Now notice that ζ_n is a complex number and that $\mathbb{Q}[\zeta_n + (\zeta_n)^{-1}]$ contains only real numbers. This is because

$$\begin{aligned}\zeta_n + (\zeta_n)^{-1} &= e^{\frac{2\pi i}{n}} + e^{\frac{-2\pi i}{n}} \\ &= \cos\left(\frac{2\pi}{n}\right) + i \cdot \sin\left(\frac{2\pi}{n}\right) + \cos\left(\frac{-2\pi}{n}\right) + i \cdot \sin\left(\frac{-2\pi}{n}\right) \\ &= \cos\left(\frac{2\pi}{n}\right) + i \cdot \sin\left(\frac{2\pi}{n}\right) + \cos\left(\frac{2\pi}{n}\right) - i \cdot \sin\left(\frac{2\pi}{n}\right) \\ &= 2\cos\left(\frac{2\pi}{n}\right) \in \mathbb{R}.\end{aligned}$$

Hence $\mathbb{Q}[\zeta_n] \neq \mathbb{Q}[\zeta_n + (\zeta_n)^{-1}] \Rightarrow [\mathbb{Q}[\zeta_n] : \mathbb{Q}[\zeta_n + (\zeta_n)^{-1}]] > 1$. This then shows us that $[\mathbb{Q}[\zeta_n] : \mathbb{Q}[\zeta_n + (\zeta_n)^{-1}]] = 2$ and hence $\mathbb{Q}[\zeta_n + (\zeta_n)^{-1}]$ is the largest real subfield of $\mathbb{Q}[\zeta_n]$ as we now easily deduce that $\mathbb{R} \cap \mathbb{Q}[\zeta_n] = \mathbb{Q}[\zeta_n + (\zeta_n)^{-1}]$.

Q.E.D.

First recall Theorem 2.2 which states that for all $n \in \mathbb{N}$, the minimal polynomial of the n-th root of unity is given by

$$f_n(x) = \prod_{1 \leq j < n : \gcd(j,n)=1} (x - (\zeta_n)^j).$$

This Lemma is useful for the following important observation.

Lemma 9.4 *If* $\gcd(m, n) = 1$, *then* $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$.

Proof: Note that Theorem 2.2 gives us that $[\mathbb{Q}(\zeta_k) : \mathbb{Q}] = \phi(k)$ for all natural numbers k as $|\{1 \leq j < k : \gcd(j, k) = 1\}| = \phi(k)$. This is useful as this helps us determine the degree of certain extensions. Observe first that $\mathbb{Q}(\zeta_m, \zeta_n) = \mathbb{Q}(\zeta_{mn})$. We are going to show this by double inclusion. For one direction note that

$$\bullet (\zeta_{mn})^n = \left(e^{\frac{2\pi i}{mn}}\right)^n = e^{\frac{2\pi i}{m}} = \zeta_m \Rightarrow \zeta_m \in \mathbb{Q}(\zeta_{mn}).$$
$$\bullet (\zeta_{mn})^m = \left(e^{\frac{2\pi i}{mn}}\right)^m = e^{\frac{2\pi i}{n}} = \zeta_n \Rightarrow \zeta_n \in \mathbb{Q}(\zeta_{mn}).$$

Therefore $\zeta_m, \zeta_n \in \mathbb{Q}(\zeta_{mn})$ which implies that $\mathbb{Q}(\zeta_m, \zeta_n) \subseteq \mathbb{Q}(\zeta_{mn})$ showing the first inclusion. For the second inclusion we first make the claim that $\gcd(m, n) = 1 \Rightarrow \gcd(mn, m + n) = 1$. Suppose by contradiction that $\gcd(mn, m + n) = d > 1$ and let p be a prime divisor of d. It then holds that $p|mn$ and $p|(m + n)$. Observe that $p|mn$ implies either $p|m$ or $p|n$.

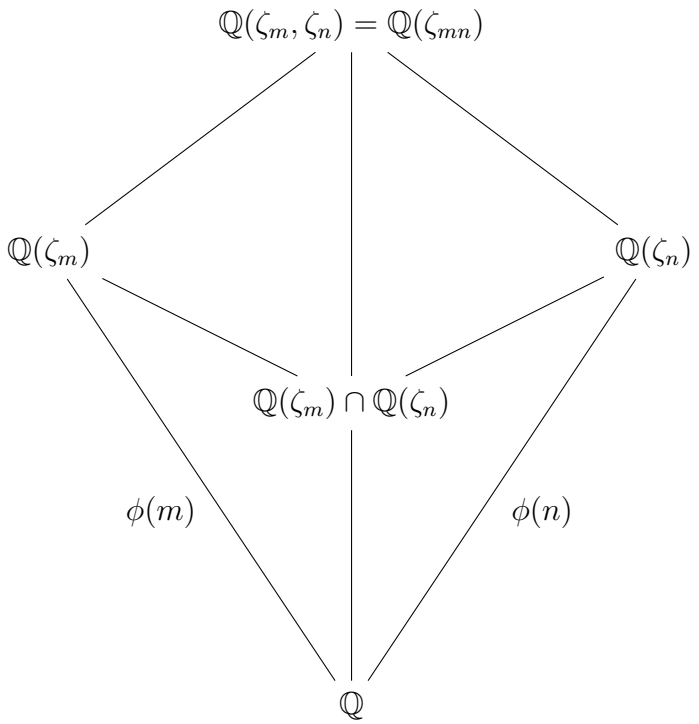
If $p|m$, then combining with $p|(m+n)$ yields that $p|(m+n-m) \Rightarrow p|n$.
Hence $p|\gcd(m,n) \Rightarrow p|1$ which is a contradiction.

If $p|n$, then combining with $p|(m+n)$ yields that $p|(m+n-n) \Rightarrow p|m$.
Hence $p|\gcd(m,n) \Rightarrow p|1$ which is a contradiction.

So the assumption that $\gcd(mn, m+n) = d > 1$ is false, therefore indeed $\gcd(mn, m+n) = 1$. From this we see that there exists some integer k such that $k(m+n) \equiv 1 \pmod{mn}$. For this integer k we see that

$$\begin{aligned}(\zeta_m \cdot \zeta_n)^k &= \left(e^{\frac{2\pi i}{m}} \cdot e^{\frac{2\pi i}{n}}\right)^k \\ &= \left(e^{\frac{2\pi i(m+n)}{mn}}\right)^k \\ &= e^{\frac{2\pi ik(m+n)}{mn}} = e^{\frac{2\pi i}{mn}} = \zeta_{mn}.\end{aligned}$$

Therefore $\zeta_{mn} \in \mathbb{Q}(\zeta_m, \zeta_n)$ which implies that $\mathbb{Q}(\zeta_{mn}) \subseteq \mathbb{Q}(\zeta_m, \zeta_n)$ showing the second inclusion. Combining these two inclusions indeed shows $\mathbb{Q}(\zeta_m, \zeta_m) = \mathbb{Q}(\zeta_{mn})$. We aim to show that $[\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) : \mathbb{Q}] = 1$ as this implies equality of the two fields. We have the following diagram of field extensions:



Now, from Theorem 2.2 we see that the minimal polynomials of ζ_m and ζ_n are given respectively by

$$f_m(x) = \prod_{1\leq j<m:\gcd(j,m)=1} (x-(\zeta_m)^j) \text{ and } f_n(x) = \prod_{1\leq j<n:\gcd(j,n)=1} (x-(\zeta_n)^j).$$

We see that all the roots of $f_m(x)$ and $f_n(x)$ are given by respectively powers of ζ_m and powers of ζ_n, all of them are contained in the respective fields $\mathbb{Q}(\zeta_m)$ and $\mathbb{Q}(\zeta_n)$. Because both of these polynomials have no repeated roots and are therefore separable polynomials and both of the fields $\mathbb{Q}(\zeta_m)$ and $\mathbb{Q}(\zeta_n)$ are respectively the splitting fields of the polynomials, both of the field extensions are actually a Galois extension. Now I make the following claims.

1. Since $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ is Galois, so are $\mathbb{Q}(\zeta_{mn})/\mathbb{Q}(\zeta_n)$ and $\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_m)\cap\mathbb{Q}(\zeta_n)$.
2. Since $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ is Galois, as groups it holds that $\text{Gal}(\mathbb{Q}(\zeta_{mn})/\mathbb{Q}(\zeta_n)) \cong \text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_m)\cap \mathbb{Q}(\zeta_n))$.
3. Since $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ is Galois, we have the following relation between degrees of extension:

$$[\mathbb{Q}(\zeta_{mn}):\mathbb{Q}] = \frac{[\mathbb{Q}(\zeta_m):\mathbb{Q}]\cdot[\mathbb{Q}(\zeta_n):\mathbb{Q}]}{[\mathbb{Q}(\zeta_m)\cap\mathbb{Q}(\zeta_n):\mathbb{Q}]}.$$

Notice that claim 3 proves Lemma 9.4. We saw that, as a consequence of Theorem 2.2, $[\mathbb{Q}(\zeta_k):\mathbb{Q}] = \phi(k)$ and furthermore since m and n are relatively co-prime the Euler phi function is multiplicative meaning that $\phi(mn) = \phi(m)\phi(n)$. Therefore from the third claim it follows that

$$[\mathbb{Q}(\zeta_m)\cap\mathbb{Q}(\zeta_n):\mathbb{Q}] = \frac{[\mathbb{Q}(\zeta_m):\mathbb{Q}]\cdot[\mathbb{Q}(\zeta_n):\mathbb{Q}]}{[\mathbb{Q}(\zeta_{mn}):\mathbb{Q}]} = \frac{\phi(m)\cdot\phi(n)}{\phi(mn)} = 1.$$

which indeed proves that $\mathbb{Q}(\zeta_m)\cap\mathbb{Q}(\zeta_n) = \mathbb{Q}$ whenever $\gcd(m,n) = 1$. These three claims are then all that remain to be proven. The proof of these statements is based on a handout given during the course Advanced Algebraic Structures. Unfortunately these notes are not freely available however we follow the proofs very closely.

1. Since $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ is Galois, we know that $\mathbb{Q}(\zeta_m)$ is the splitting field of a separable polynomial $P(x)$ over $\mathbb{Q}[x]$. In fact we know that this polynomial $P(x)$ equals the polynomial $f_m(x) = \prod_{1\leq j<m:\gcd(j,m)=1}(x-(\zeta_m)^j)$. From this we find that $\mathbb{Q}(\zeta_{mn}) = \mathbb{Q}(\zeta_m,\zeta_n)$ is the splitting field of $f_m(x)$ over $\mathbb{Q}(\zeta_n)$. Namely $f_m(x)$ still has no repeated roots and all of its roots lie in $\mathbb{Q}(\zeta_m,\zeta_n)$. This shows that $\mathbb{Q}(\zeta_{mn})/\mathbb{Q}(\zeta_n)$ is a Galois extension. Similarly we obtain that $\mathbb{Q}(\zeta_m)$ is the splitting field of $f_m(x)$ over $\mathbb{Q}(\zeta_m)\cap\mathbb{Q}(\zeta_n)$ which also shows that $\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_m)\cap\mathbb{Q}(\zeta_n)$ is also a Galois extension. This proves the first claim.

2. Since $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ is Galois, the first claim yields that $\mathbb{Q}(\zeta_{mn})/\mathbb{Q}(\zeta_n)$ and $\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_m)\cap\mathbb{Q}(\zeta_n)$ are also Galois meaning that the respective Galois groups are well defined. Define the map ψ by

$$\psi: \ \text{Gal}(\mathbb{Q}(\zeta_{mn})/\mathbb{Q}(\zeta_n)) \to \text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_m)\cap\mathbb{Q}(\zeta_n)) \ \text{ as } \ \psi(\sigma) := \sigma|_{\mathbb{Q}(\zeta_m)}.$$

We aim to show that ψ is an isomorphism as this proves the claim. First one may notice that ψ is in fact well defined by how automorphisms in both Galois groups work. Because ψ maps around automorphisms, ψ itself is a homomorphism with respect to function composition. To show that ψ is injective we need $\ker(\psi) = id \in \text{Gal}(\mathbb{Q}(\zeta_{mn})/\mathbb{Q}(\zeta_n))$. Suppose $\sigma \in \ker(\psi)$, then by definition $\psi(\sigma) = \sigma|_{\mathbb{Q}(\zeta_m)} = id$. Therefore $\sigma(x) = x$ for all $x \in \mathbb{Q}(\zeta_m)$. Now since $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_{mn})/\mathbb{Q}(\zeta_n))$ it is also true that $\sigma(y) = y$ for all $y \in \mathbb{Q}(\zeta_n)$. Since σ is the identity on the fields $\mathbb{Q}(\zeta_m)$ and $\mathbb{Q}(\zeta_n)$, by linearity it is also identity on the compositum of the fields which is $\mathbb{Q}(\zeta_m, \zeta_n) = \mathbb{Q}(\zeta_{mn})$. Hence $\sigma \in \ker(\psi)$ implies that $\sigma = id \in \text{Gal}(\mathbb{Q}(\zeta_{mn})/\mathbb{Q}(\zeta_n))$ which shows that ψ is an injective group homomorphism.

For surjectivity, note that any element $\tau \in \text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_m)\cap\mathbb{Q}(\zeta_n))$ is determined by where it send the roots of $f_m(x)$ because $\mathbb{Q}(\zeta_m)$ is the splitting field of $f_m(x)$ over $\mathbb{Q}(\zeta_m)\cap\mathbb{Q}(\zeta_n)$. Taking then $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_{mn})/\mathbb{Q}(\zeta_n))$ that is defined by mapping the roots of $f_m(x)$ to the same values as τ does yields that $\sigma|_{\mathbb{Q}(\zeta_m)} = \tau$ and therefore $\psi(\sigma) = \tau$. Hence ψ is also a surjective group homomorphism.

Because ψ is injective and surjective, it is indeed bijective and so ψ is an isomorphism which shows that $\text{Gal}(\mathbb{Q}(\zeta_{mn})/\mathbb{Q}(\zeta_n)) \cong \text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_m)\cap\mathbb{Q}(\zeta_n))$. This proves the second claim.

3. Since $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ is Galois, the first and second claim hold. Now because $\mathbb{Q}(\zeta_{mn})/\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is a tower of field extensions we have the relation that

$$[\mathbb{Q}(\zeta_{mn}) : \mathbb{Q}] = [\mathbb{Q}(\zeta_{mn}) : \mathbb{Q}(\zeta_n)] \cdot [\mathbb{Q}(\zeta_n) : \mathbb{Q}].$$

From the second claim we know that $\text{Gal}(\mathbb{Q}(\zeta_{mn})/\mathbb{Q}(\zeta_n)) \cong \text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_m)\cap\mathbb{Q}(\zeta_n))$, since we work with finite extensions these group are also finite and therefore have the same cardinality. Therefore we obtain that

$$\begin{aligned}[\mathbb{Q}(\zeta_{mn}) : \mathbb{Q}(\zeta_n)] &= |\text{Gal}(\mathbb{Q}(\zeta_{mn})/\mathbb{Q}(\zeta_n))| \\ &= |\text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_m)\cap\mathbb{Q}(\zeta_n))| \\ &= [\mathbb{Q}(\zeta_m) : \mathbb{Q}(\zeta_m)\cap\mathbb{Q}(\zeta_n)].\end{aligned}$$

Furthermore $\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_m)\cap\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is also a tower of field extensions giving us the relation that

$$\begin{aligned}&[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = [\mathbb{Q}(\zeta_m) : \mathbb{Q}(\zeta_m)\cap\mathbb{Q}(\zeta_n)] \cdot [\mathbb{Q}(\zeta_m)\cap\mathbb{Q}(\zeta_n) : \mathbb{Q}] \\ &\Rightarrow [\mathbb{Q}(\zeta_m) : \mathbb{Q}(\zeta_m)\cap\mathbb{Q}(\zeta_n)] = \frac{[\mathbb{Q}(\zeta_m) : \mathbb{Q}]}{[\mathbb{Q}(\zeta_m)\cap\mathbb{Q}(\zeta_n) : \mathbb{Q}]}.\end{aligned}$$

Finally combining all these results yield

$$\begin{aligned}[\mathbb{Q}(\zeta_{mn}):\mathbb{Q}] &= [\mathbb{Q}(\zeta_{mn}):\mathbb{Q}(\zeta_n)]\cdot[\mathbb{Q}(\zeta_n):\mathbb{Q}] \\ &= [\mathbb{Q}(\zeta_m):\mathbb{Q}(\zeta_m)\cap\mathbb{Q}(\zeta_n)]\cdot[\mathbb{Q}(\zeta_n):\mathbb{Q}] \\ &= \frac{[\mathbb{Q}(\zeta_m):\mathbb{Q}]}{[\mathbb{Q}(\zeta_m)\cap\mathbb{Q}(\zeta_n):\mathbb{Q}]}\cdot[\mathbb{Q}(\zeta_n):\mathbb{Q}] \\ &= \frac{[\mathbb{Q}(\zeta_m):\mathbb{Q}]\cdot[\mathbb{Q}(\zeta_n):\mathbb{Q}]}{[\mathbb{Q}(\zeta_m)\cap\mathbb{Q}(\zeta_n):\mathbb{Q}]}.\end{aligned}$$

This shows that $[\mathbb{Q}(\zeta_{mn}):\mathbb{Q}] = \frac{[\mathbb{Q}(\zeta_m):\mathbb{Q}]\cdot[\mathbb{Q}(\zeta_n):\mathbb{Q}]}{[\mathbb{Q}(\zeta_m)\cap\mathbb{Q}(\zeta_n):\mathbb{Q}]}$ which proves the third claim.

Now that the third claim is proven, so is the lemma. Hence we conclude that if m and n are such that $\gcd(m,n)=1$, then $\mathbb{Q}(\zeta_m)\cap\mathbb{Q}(\zeta_n)=\mathbb{Q}$.

Q.E.D.

As a corollary of Lemma 9.4, if n is prime then any root of unity in the field $\mathbb{Q}(\zeta_n)$ is of the form $\pm(\zeta_n)^k$ for some integer $0 \leq k < n$. Note that indeed no (ζ_m) lies in $\mathbb{Q}(\zeta_n)$ whenever m is not a multiple of n. If m is a multiple of n however, independence of the two fields can be shown because $[\mathbb{Q}(\zeta_{kn}):\mathbb{Q}] = [\mathbb{Q}(\zeta_n):\mathbb{Q}]$ if and only if $k=1$ or $k=2$. However since $\mathbb{Q}(\zeta_{2n})=\mathbb{Q}(\zeta_n)$ this is not a significant result. This follows because $\phi(2n)=\phi(n)$ for primes $n>2$.

This principle extends to the ring of integers, meaning that the only roots of unity in $\mathbb{Z}[\zeta_n]$ for n prime are of the form $\pm(\zeta_n)^k$ for some integer $0 \leq k < n$. Now that we have this result we are able to give a more general classification of units in the ring $\mathbb{Z}[\zeta_n]$ for any prime number n

Theorem 9.2 *Let u be a unit of $\mathbb{Z}[\zeta_n]$ for n a prime number. Then there exists $\epsilon \in \mathbb{Q}[\zeta_n+\zeta_n^{-1}]$ and $r\in\mathbb{Z}$ such that $u=(\zeta_n)^r\cdot\epsilon$.*

Proof: Let $\alpha = \frac{u}{\overline{u}}$. Then α is an algebraic integer as u and $\overline{u}$ are both units. Furthermore all algebraic conjugates of α have absolute value equal to 1 because complex conjugation commutes with algebraic conjugation. Then by Lemma 9.1 it follows that there exists some integer a such that $\alpha = \frac{u}{\overline{u}} = \pm(\zeta_n)^a$ as the only roots of unity in $\mathbb{Z}[\zeta_n]$ are of this form which is a consequence of Lemma 9.4 which is discussed right before Theorem 9.2.

Suppose first that $\frac{u}{\overline{u}} = -(\zeta_n)^a$. Because u is a unit of $\mathbb{Z}[\zeta_n]$ one can find integers c_i such that

$$u = c_0 + c_1\zeta_n + \ldots + c_{p-2}(\zeta_n)^{p-2} \equiv c_0 + c_1 + \ldots + c_{p-2} \pmod{1-\zeta_n}$$

because $1 \equiv \zeta_n \pmod{\zeta_n}$. Now because $\overline{\zeta_n} = (\zeta_n)^{-1}$, one finds that

$$\begin{aligned}\overline{u} &= c_0 + c_1(\zeta_n)^{-1} + ... + c_{p-2}(\zeta_n)^{-(p-2)} \\ &\equiv c_0 + c_1 + ... + c_{p-2} \pmod{1-\zeta_n} \\ &\equiv u \pmod{1-\zeta_n} \\ &\equiv -\overline{u}\cdot(\zeta_n)^a \pmod{1-\zeta_n} \\ &\equiv -\overline{u} \pmod{1-\zeta_n}.\end{aligned}$$

Therefore $2\overline{u} \equiv 0 \pmod{1-\zeta_n}$ which shows that either 2 is divisible by $1-\zeta_n$ or $\overline{u}$ is divisible by $1-\zeta_n$. Now because $\overline{u}$ is a unit, it is not divisible by $1-\zeta_n$. This is because

$$N(1-\zeta_n) = n \text{ does not divide } N(\overline{u}) = 1.$$

Furthermore because $N(2) = \prod_{i=1}^{n-1}(\sigma_i(2)) = \prod_{i=1}^{n-1}(2) = 2^{n-1}$ is not divisible by $N(1-\zeta_n) = n$, since n is a prime greater than 2, we can also conclude that 2 is not divisible by $1-\zeta_n$. Therefore $2\overline{u} \equiv 0 \pmod{1-\zeta_n}$ leads to a contradiction. Hence the assumption that $\frac{u}{\overline{u}} = -(\zeta_n)^a$ is wrong.

Therefore we find that in fact $\frac{u}{\overline{u}} = +(\zeta_n)^a$. Let r be such that $2r \equiv a \pmod{n}$, which exists as $\gcd(2,n) = 1$, and let $\epsilon = (\zeta_n)^{-r}\cdot u$. Then $u = (\zeta_n)^r \cdot \epsilon$ and

$$\overline{\epsilon} = \overline{(\zeta_n)^{-r}\cdot u} = (\zeta_n)^r \cdot \overline{u} = (\zeta_n)^a \cdot \overline{u} \cdot (\zeta_n)^{-r} = (\zeta_n)^{-r}\cdot u = \epsilon.$$

which shows that ϵ is completely real.

Now from Lemma 9.3 we know that the largest possible real subfield of $\mathbb{Q}[\zeta_n]$ is the field $\mathbb{Q}[\zeta_n + (\zeta_n)^{-1}]$. Because ϵ is a number in $\mathbb{Q}[\zeta_n]$ that satisfies $\epsilon = \overline{\epsilon}$, we know that it is a real number. Therefore ϵ is an element of the largest possible real subfield of $\mathbb{Q}[\zeta_n]$ which shows that $\epsilon \in \mathbb{Q}[\zeta_n + (\zeta_n)^{-1}]$.

Therefore we conclude that for any unit $u \in \mathbb{Z}[\zeta_n]$, there exists $\epsilon \in \mathbb{Q}[\zeta_n + (\zeta_n)^{-1}]$ and $r \in \mathbb{Z}$ such that $u = (\zeta_n)^r \cdot \epsilon$.

Q.E.D.

So now we found a general structure for the units of $\mathbb{Z}[\zeta_n]$ for any prime number n. It is less precise as the unit groups found in Lemma 3.1, Lemma 5.1 and Theorem 7.2, as here we determined the unit groups explicitly. We still have determined enough to be able to prove the first case of Fermat's last theorem under certain conditions.

9.2 The first case of Fermat's last theorem

Now we would like to investigate the equation $x^n + y^n = z^n$ in the ring $\mathbb{Z}[\zeta_n]$ to show that there are no nontrivial solutions for this. Because we assume n to be a prime number greater than 5, since the other cases were done previously, we can apply a factorization on the left side to obtain

$$x^n + y^n = \prod_{i=0}^{n-1}(x + (\zeta_n)^i y) = z^n.$$

If all these factors on the left side are relatively prime up to some extend, we would like that each one would be equal to a unit multiplied by common divisors, followed up by an n-th power. This however is only the case when $\mathbb{Z}[\zeta_n]$ is a unique factorization domain. For the remainder of this chapter we therefore assume that n is such that $\mathbb{Z}[\zeta_n]$ is a Euclidean domain.

Next up we are going to proof only the first case of Fermat's last theorem for the value's of n such that $\mathbb{Z}[\zeta_n]$ is a Euclidean domain. Our goal is then to show that the equation

$$x^n + y^n = z^n \text{ where } \gcd(xyz, n) = 1$$

has no solutions in integers. Now before we start the proof of this statement there are some observations that we need to make. For notational convenience, we set $\zeta := \zeta_n$ and can also assume that x, y and z are relatively prime as any common factors can be divided out.

Lemma 9.5 *The number $\frac{1-\zeta^k}{1-\zeta}$ is a unit whenever k is not multiple of n.*

Proof: First we find that

$$\frac{1-\zeta^k}{1-\zeta} = 1 + \zeta + \zeta^2 + ... + \zeta^{k-1} \in \mathbb{Z}[\zeta].$$

Next up, we aim to show that $\frac{1-\zeta}{1-\zeta^k}$ is also an element of $\mathbb{Z}[\zeta]$. Because n is prime and k is not a multiple of n, we have $\gcd(k, n) = 1$. Therefore there exists an integer l such that $kl \equiv 1 \pmod{n}$. This implies that $\zeta = \zeta^{kl}$. We then find that

$$\frac{1-\zeta}{1-\zeta^k} = \frac{1-\zeta^{kl}}{1-\zeta^k} = 1 + \zeta^l + \zeta^{2l} + ... + \zeta^{l(k-1)} \in \mathbb{Z}[\zeta].$$

This shows that $\left(\frac{1-\zeta^k}{1-\zeta}\right)^{-1}$ exists, and therefore $\frac{1-\zeta^k}{1-\zeta}$ is a unit.

Q.E.D.

The following Lemma tells us something about the relative coprimality of all the $x + \zeta^i y$ terms that we obtain after the factorization

$$x^n + y^n = (x + y)(x + \zeta y) \cdots (x + \zeta^{n-1} y).$$

Lemma 9.6 *The terms $x + \zeta^i y$ for $i = 0, 1, ..., n-1$ are all pairwise relatively prime.*

Proof: By way of contradiction, suppose p is irreducible, not a unit and that p divides both $x + \zeta^i y$ and $x + \zeta^j y$ where $i \neq j$. Therefore we assume that $i < j$, we then obtain that

$$\begin{aligned} p \text{ divides } \quad (x + \zeta^i y) - (x + \zeta^j y) &= (\zeta^i - \zeta^j) y \\ &= \zeta^i (1 - \zeta^{j-i}) y \\ &= \zeta^i (1 - \zeta) \frac{1 - \zeta^{j-i}}{1 - \zeta} y. \end{aligned}$$

Notice that ζ^i is a unit and that $\frac{1-\zeta^{j-i}}{1-\zeta}$ is a unit as well following Lemma 9.5. Therefore we see that p divides $(unit)(1-\zeta)y$. Because p is irreducible it follows that p divides $1-\zeta$ or p divides y.

Similarly we see that

$$\begin{aligned} p \text{ divides } \quad \zeta^j(x+\zeta^i y) - \zeta^i(x+\zeta^j y) &= (\zeta^j - \zeta^i)x \\ &= \zeta^i(\zeta^{j-i}-1)x \\ &= -\zeta^i(1-\zeta)\frac{1-\zeta^{j-i}}{1-\zeta}x. \end{aligned}$$

Again since ζ^i and $\frac{1-\zeta^{j-i}}{1-\zeta}$ are units we see that p divides $(unit)(1-\zeta)x$. Since p is irreducible it follows that p divides $1-\zeta$ or p divides x.

If p does not divide $1-\zeta$, then it follows that p divides x and p divides y. However it was assumed that x and y are relatively prime, hence this is is not possible. Therefore we see that p divides $1-\zeta$. Since in Lemma 9.2 it was shown that $1-\zeta$ is irreducible, it follows that $p = u(1-\zeta)$ where u is a unit. Now observe that this implies the following lines:

$$\begin{aligned} 1-\zeta^i \text{ is divisible by } \ p &\Rightarrow 1-\zeta^i \equiv 0 \pmod{p} \\ &\Rightarrow 1 \equiv \zeta^i \pmod{p} \\ &\Rightarrow y \equiv \zeta^i y \pmod{p} \\ &\Rightarrow x+y \equiv x+\zeta^i y \pmod{p} \equiv 0 \pmod{p} \end{aligned}$$

where the last line holds because p was chosen to divide $1-\zeta^i y$. Now observe that $x+y$ is an integer and $x+y \equiv 0 \pmod{p}$. This means that $x+y$ is divisible by $1-\zeta$. Now I make the following claim:

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}[\zeta]/(1-\zeta)\mathbb{Z}[\zeta] \tag{9.2}$$

This can be done by defining the following map, $\Phi : \mathbb{Z}[\zeta]/(1-\zeta)\mathbb{Z}[\zeta] \to \mathbb{Z}/n\mathbb{Z}$ by $\Phi(a_0 + a_1\zeta + ...+a_{n-1}\zeta^{n-1}) = \overline{a_0 + a_1 + ... + a_{n-1}}$. This works as $a_0+a_1\zeta+...+a_{n-1}\zeta^{n-1} \equiv a_0+a_1+...+a_{n-1} \pmod{1-\zeta}$, so the map Φ is in fact the natural map between the two objects. Because both n and $1-\zeta$ are irreducible in respectively $\mathbb{Z}$ and $\mathbb{Z}[\zeta]$, both the domain and co-domain of Φ are fields. Combined with the observation that Φ is a surjective map it follows that both of the fields are actually isomorphic. The important thing is then that zeroes in $\mathbb{Z}[\zeta]/(1-\zeta)\mathbb{Z}[\zeta]$ correspond to zeroes in $\mathbb{Z}/5\mathbb{Z}$.

Since $x+y$ is divisible by $1-\zeta$, it corresponds to $\overline{0}$ in $\mathbb{Z}[\zeta]/(1-\zeta)\mathbb{Z}[\zeta]$. Because $x+y \in \mathbb{Z}$ and $\Phi|_{\mathbb{Z}} = id|_{\mathbb{Z}}$ we can conclude that $x+y$ is a multiple of n. Hence $x+y \equiv 0 \pmod{n}$. Finally, by using Fermat's little theorem to obtain $x^n \equiv x \pmod{n}$ and $y^n \equiv y \pmod{n}$ we get the result that

$$z^n = x^n + y^n \equiv x+y \pmod{n} \equiv 0 \pmod{n}.$$

Therefore n divides z, however it was assumes that $\gcd(xyz, n) = 1$. This leads to a contradiction, therefore the p as described in the start does not exist. Hence we conclude that no non-unit p exists which divides $1 - \zeta^i$ and $1 - \zeta^j$ whenever $i \neq j$. This proves that all the terms $1 - \zeta^i y$ for $i = 0, 1, ..., n - 1$ are pairwise relatively prime.

Q.E.D.

Lemma 9.7 *Let $\alpha \in \mathbb{Z}[\zeta]$. Then α^n is congruent to a rational integer* $\pmod n$

Proof: We can write $\alpha = a_0 + a_1\zeta + ... + a_{n-1}\zeta^{n-1}$. It then follows that

$$\begin{aligned}\alpha^n &= (a_0 + a_1\zeta + ... + a_{n-1}\zeta^{n-1})^n \\ &\equiv (a_0)^n + (a_1\zeta)^n + ... + (a_{n-1}\zeta^{n-1})^n \pmod n \\ &\equiv (a_0)^n + (a_1)^n + ... + (a_{n-1})^n \pmod n\end{aligned}$$

using that all the binomial coefficients of cross terms in $(a_0 + a_1\zeta + ... + a_{n-1}\zeta^{n-1})^n$ are divisible by n because n is prime. Furthermore, as each $a_i \in \mathbb{Z}$, the number $a_0)^n + (a_1)^n + ... + (a_{n-1})^n$ is equal to an integer. Therefore α^n is indeed congruent to a rational integer $\pmod n$.

Q.E.D.

We need one more result before we can start with proving the first case of Fermat's last theorem.

Lemma 9.8 *Let $\alpha = a_0 + a_1\zeta + ... + a_{n-1}\zeta^{n-1}$ with each $a_i \in \mathbb{Z}$ where at least one $a_i = 0$. If n divides α, then n divides each a_j for $0 \leq j \leq n - 1$.*

Proof: Because $1 + \zeta + ... + \zeta^{n-1} = 0$, we may use any subset of $\{1, \zeta, ..., \zeta^{n-1}\}$ with $n - 1$ elements as a basis of $\mathbb{Z}[\zeta]$. Since α is divisible by n we can write $\alpha = nK$ for some $K \in \mathbb{Z}[\zeta]$. Let $\alpha = a_0 + a_1\zeta + ... + a_{n-1}\zeta^{n-1}$ and let i be such that $a_i = 0$. If

$$K = b_0 + b_1\zeta + ... + b_{n-1}\zeta^{n-1}, K \in \mathbb{Z}[\zeta]$$

we can replace $b_i\zeta^i$ by $b_i(-1 - \zeta - ... - \zeta^{i-1} - \zeta^{i+1} - ... - \zeta^{n-1})$ to make sure the coefficient of ζ^i of K is also equal to 0. Hence without loss of generality we assume that $b_i = 0$. We then see the following result:

$$\begin{aligned}\alpha = nK &\Rightarrow \alpha - nK = 0 \\ &\Rightarrow (a_0 + a_1\zeta + ... + a_{n-1}\zeta^{n-1}) - n(b_0 + b_1\zeta + ... + b_{n-1}\zeta^{n-1}) = 0 \\ &\Rightarrow (a_0 - nb_0) + (a_1 - nb_1)\zeta + ... + (a_{n-1} - nb_{n-1})\zeta^{n-1} = 0.\end{aligned}$$

It's important to note that the ζ^i coefficient of above number is 0. What we can do now is cancel away all the coefficients of ζ^{n-1} over the other coordinates to obtain that the ζ^{n-1} coefficient is equal to 0. In other words, if

$$L = c_0 + c_1\zeta + ... + c_{n-1}\zeta^{n-1} = 0, L \in \mathbb{Z}[\zeta]$$

with $c_i = 0$, we plug in $\zeta^{n-1} = -1 - \zeta - ... - \zeta^{n-2}$ to obtain

$$(c_0 - c_{n-1}) + (c_1 - c_{n-1})\zeta - ... - c_{n-1}\zeta^i - ... - (c_{n-2} - c_{n-1})\zeta^{n-2} = 0.$$

Defining the polynomial $g(x) := (c_0 - c_{n-1}) + (c_1 - c_{n-1})x - ... - c_{n-1}x^i - ... - (c_{n-2} - c_{n-1})x^{n-2}$ leads to the following three observations:

1. The degree of $g(x)$ is at most $n - 2$.
2. The polynomial $g(x) \in \mathbb{Z}[x]$.
3. The polynomial $g(x)$ satisfies $g(\zeta) = 0$.

Recall however that Lemma 2.3 states that the minimal polynomial of ζ over $\mathbb{Z}$ has degree equal to $n - 1$. Hence $g(\zeta)$ is possible if and only if $g(x) = 0$ for all x. This means that all the coefficients of $g(x)$ are equal to 0. Hence

$$\begin{aligned} c_j - c_{n-1} = 0 \text{ for all } 0 \leq j \leq n-2 \text{ and } \quad c_{n-1} = 0 &\Rightarrow c_j = 0 \text{ for all } 0 \leq j \leq n-2 \\ &\Rightarrow L = 0. \end{aligned}$$

So, $L = c_0 + c_1\zeta + ... + c_{n-1}\zeta^{n-1} = 0$ with $c_i = 0$ for some i implies that each $c_j = 0$. Going back to

$$(a_0 - nb_0) + (a_1 - nb_1)\zeta + ... + (a_{n-1} - nb_{n-1})\zeta^{n-1}$$

where it was assumed that $a_i = b_i = 0$ we conclude by above observation that each $a_j - nb_j = 0$. Hence we conclude that each $a_j = nb_j$ for some integer b_j showing that in fact, each a_j is divisible by n for $0 \leq j \leq n - 1$.

Q.E.D.

Now we are ready to prove the first case of Fermat's last theorem, under the condition that $\mathbb{Z}[\zeta_n]$ is a Euclidean domain as said at the start of Section 9.2.

Theorem 9.3 *The equation* $x^n + y^n = z^n$ *where* $\gcd(xyz, n) = 1$ *has no solutions in* $\mathbb{Z}$.

Proof: We start of by rewriting the equation as

$$z^n = x^n + y^n = (x + y)(x + \zeta y)...(x + \zeta^{n-1}y).$$

By Lemma 9.6 we know that all the $x + \zeta^i y$ terms are relatively prime with each other. As we assumed $\mathbb{Z}[\zeta]$ to be a Euclidean domain and therefore a unique factorization domain, we obtain the following. Since the product of n numbers forms an n-th power and all those numbers are relatively prime with respect to each other, it follows that each of those individual numbers is itself an n-th power multiplied by a unit. That means that

$$x + \zeta^i y = u_i \cdot (\alpha_i)^n \text{ where each } u_i \text{ is a unit.}$$

Setting $i = 1$ and omitting the subscripts we have $x + \zeta y = u\alpha^n$ for some unit u. According to Theorem 9.2, there exists some $\epsilon \in \mathbb{Q}[\zeta + \zeta^{-1}]$ and integer r such that $u = \zeta^r \cdot \epsilon$. More importantly, this ϵ satisfies that $\overline{\epsilon} = \epsilon$. From Lemma 9.7 it follows that $\alpha^n \equiv a \pmod{n}$ for some rational integer a. Hence,

$$x + \zeta y = u\alpha^n = \zeta^r \cdot \epsilon \cdot \alpha^n \equiv \zeta^r \cdot \epsilon \cdot a \pmod{n}.$$

Taking complex conjugates will result in the expression

$$\overline{x + \zeta y} = x + \overline{\zeta} y = x + \zeta^{-1} y = \overline{\zeta^r \cdot \epsilon \cdot \alpha^n} \equiv \zeta^{-r} \cdot \epsilon \cdot \overline{a} \pmod{n} \equiv \zeta^{-r} \cdot \epsilon \cdot a \pmod{n}$$

where we used that $\overline{a} = a, \overline{\zeta} = \zeta^{-1}$ and $\overline{\epsilon} = \epsilon$. We then end up with the following two expressions:

$$\begin{cases} x + \zeta y \equiv \zeta^r \cdot \epsilon \cdot a \pmod{n} \\ x + \zeta^{-1} y \equiv \zeta^{-r} \cdot \epsilon \cdot a \pmod{n} \end{cases}$$

Observe that multiplying the first equation by ζ^{-r} and the second equation by ζ^r will result in equality and therefore

$$\zeta^{-r}(x + \zeta y) \equiv \zeta^r (x + \zeta^{-1} y) \pmod{n}.$$

After some simplification this becomes the equation

$$x + \zeta y - \zeta^{2r} x - \zeta^{2r-1} y \equiv 0 \pmod{n}. \tag{9.3}$$

If $1, \zeta, \zeta^{2r}$ and ζ^{2r-1}, then Lemma 9.8 tells us that n divides the coefficients of all these ζ-powers. This would imply that n divides x and y which contradicts that $\gcd(xyz, n) = 1$. Therefore we now assume that these four ζ-powers are not distinct. Because $1 \neq \zeta$ and $\zeta^{2r-1} \neq \zeta^{2r}$, we are left with three cases to consider.

- Case 1 is that $1 = \zeta^{2r}$. If this is true then Equation 9.3 becomes

$$\begin{aligned} x + \zeta y - \zeta^{2r} x - \zeta^{2r-1} y &\equiv x + \zeta y - x - \zeta^{-1} y \pmod{n} \\ &\equiv \zeta y - \zeta^{-1} y \pmod{n} \\ &\equiv \zeta y - \zeta^{n-1} y \pmod{n} \equiv 0 \pmod{n}. \end{aligned}$$

  Then from Lemma 9.8 it follows that the coefficients of ζ and ζ^{n-1} are divisible by n. Therefore it follows that y is divisible by n which contradicts the assumption that $\gcd(xyz, n) = 1$.

- Case 2 is that $\zeta = \zeta^{2r-1}$. If this is true then Equation 9.3 becomes

$$\begin{aligned} x + \zeta y - \zeta^{2r} x - \zeta^{2r-1} y &\equiv x + \zeta y - \zeta^2 x - \zeta y \pmod{n} \\ &\equiv x - \zeta^2 x \pmod{n} \equiv 0 \pmod{n}. \end{aligned}$$

  Then from Lemma 9.8 it follows that the coefficients of 1 and ζ^2 are divisible by n. Therefore it follows that x is divisible by n which contradicts the assumption that $\gcd(xyz, n) = 1$.

- Case 3 is that $1 = \zeta^{2r-1}$, this is equivalent to the case $\zeta = \zeta^{2r}$. If this is true then Equation 9.3 becomes

$$\begin{aligned} x + \zeta y - \zeta^{2r} x - \zeta^{2r-1} y &\equiv x + \zeta y - \zeta x - y \pmod{n} \\ &\equiv (x - y) - (x - y)\zeta \pmod{n} \\ &\equiv 0 \pmod{n}. \end{aligned}$$

  Then from Lemma 9.8 it follows that the coefficients of 1 and ζ are divisible by n. Therefore it follows that $x - y$ is divisible by n which is equivalent to $x \equiv y \pmod{n}$.

  Starting from equation $x^n + y^n = z^n$ we obtained the relation $x \equiv y \pmod{n}$. Similarly, by rewriting the original equation into $x^n + (-z)^n = (-y)^n$ and going through all the steps described above we determine that $x \equiv -z \pmod{n}$. Using these equivalences we find

$$\begin{aligned} x^n + y^n = z^n \Rightarrow & x^n + y^n \equiv z^n \pmod{n} \\ \Rightarrow & x^n + x^n \equiv (-x)^n \pmod{n} \\ \Rightarrow & 3x^n \equiv 0 \pmod{n}. \end{aligned}$$

  Notice however that we assumed n to be a prime greater than 5, therefore $3x^n \equiv 0 \pmod{n}$ implies that x is divisible by n which contradicts the assumption that $\gcd(xyz, n) = 1$.

Therefore we can conclude that the equation

$$x^n + y^n = z^n$$

where $\gcd(xyz, n) = 1$ has no solutions in $\mathbb{Z}$, which is what we wanted to show.

Q.E.D.

Observe that the proof for the first case is different from that of the first case where $n = 3$ or $n = 5$. The reason is that the equation $x^n + y^n = z^n$ can have solutions $\pmod{n^2}$ when n is larger than 5. For example we have the relation $1^7 + 30^7 \equiv 31^7 \pmod{49}$. Because of this, the method used in Lemma 4.2 and Lemma 8.1 does not work. We therefore chose for a different strategy here. That being said, we still made use of a description of units from $\mathbb{Z}[\zeta_n]$ and the assumption that it is a Euclidean domain. During previous results those facts were mainly used during the proof of the second case of Fermat's last theorem. Proving the second case of Fermat's last theorem however for these values of n such that $\mathbb{Z}[\zeta_n]$ is Euclidean is beyond the scope of this project, however more details can be found in Chapter 9 of [8].

9.3 Notable results

We proved the first case of Fermat's last theorem under the assumption that n is a prime for which $\mathbb{Z}[\zeta_n]$ is a Euclidean domain. In chapter 11 from [8] it is shown that the list of all such primes is given by

$$\mathbb{Z}[\zeta_n] \text{ is Euclidean with } n \text{ prime } \Leftrightarrow n \in \{3, 5, 7, 11, 13, 17, 19\}.$$

These are not a lot of primes, however there is a catch. In order to factorize

$$x^n + y^n = (x + y)(x + \zeta y) \cdots (x + \zeta^{n-1} y) = z^n$$

and say that each of the individual terms on the left is equal to a unit multiplied by an n-th power we don't need to have unique factorization into irreducible elements. Instead unique factorization up to prime ideals will be enough for this. The rest of the proof remains the same however we are then able to extend it to more primes. Call these prime numbers regular primes.

The most well known such result was discovered by Kummer and it is Theorem 5.34 from [8]. The results states that a prime p is regular if and only if p divides the numerator of some Bernoulli number B_k for $k = 2, 4, 6, ..., p - 3$, where the Bernoulli numbers are defined as following:

$$\frac{x}{e^x - 1} = \sum_{n=0}^{\infty} B_n \cdot \frac{x^n}{n!}$$

This extends the proof of the first case for Fermat's last theorem to more exponents, namely to all of those such that the exponent is a multiple of a regular prime. The first exponents underneath 200 that will sadly not work are then given by

$$\{37, 59, 67, 74, 101, 103, 118, 131, 134, 149, 157\}$$

which is already a great improvement if we compare it to when $\mathbb{Z}[\zeta_n]$ was Euclidean.

10 Conclusion

In this paper we have investigated the ring $\mathbb{Z}[\zeta_n]$ for certain small values of n namely $n = 3, 4$ and 5. We determined the unit groups of these three rings and also saw that we had unique factorization. These key results were applied to proof Fermat's last theorem for $n = 3, 4$ and 5 respectively. Furthermore we obtained some general results about how units look in the ring $\mathbb{Z}[\zeta_n]$ and were able to prove the first case of Fermat's last theorem under the condition that $\mathbb{Z}[\zeta_n]$ is a Euclidean domain. Even though this is only true for a handful of values of n, our method has great extension under a less strong assumption. The methods we discussed are classical and rely on results from ring theory that are quite quickly taught. These methods helped people develop proofs of Fermat's last theorem for many exponents however to prove the theorem in its entirely one can not use the methods described in this paper.

11 Afterword

Throughout this paper, definitions, theorems and examples were used from the courses Group theory [7] and Algebraic structures [3]. To cite these papers at the required places would clutter the text and risk bringing confusing. Therefore we only refer to them when suitable. I would like to thank my supervisor prof. dr. J. Top for the great assistance and help I got during this project.

References

[1] Gemma Branchini. "Algoritmo del massimo comun divisore nel corpo delle radici quinte dell'unita". In: *Atti della Reale Accademia dei Lincei, Roma*. 5th ser. 32 (1923), pp. 68–72. URL: http://operedigitali.lincei.it/rendicontiFMN/rol/pdf/S5V32T1A1923P68_72.pdf.

[2] H.W. Lenstra L.N.M. van Geemen, F. Oort, and J. Top. *Advanced Algebraic Structures*. Univesity of Groningen, 2017. URL: https://www.rug.nl/staff/steffen.muller/lecture_notes_advanced_algebraic_structures.pdf.

[3] H.W. Lenstra L.N.M. van Geemen, F. Oort, and J. Top. *Algebraic Structures*. Univesity of Groningen, 2017. URL: https://www.rug.nl/staff/steffen.muller/lecture_notes_algebraic_structures.pdf.

[4] Joseph Lipman. "$x^3 + y^3 + z^3 \neq 0$". In: (). course notes. URL: https://www.math.purdue.edu/~jlipman/MA598/x%5E3+y%5E3+z%5E3.pdf.

[5] David C. Marshall, Edward Odell, and Michal Starbird. *Number Theory Through Inquiry*. MAA textbooks, 2007.

[6] Paolo Ribenboim. *Fermat's Last Theorem For Amateurs*. Springer New York, NY, 1999.

[7] J. Top and J.S. Müller. *Group theory*. Univesity of Groningen, 2018. URL: https://www.rug.nl/staff/steffen.muller/lecture-notes-group.pdf.

[8] Lawrence C. Washington. *Introduction to Cyclotomic Fields second edition*. Springer New York, NY, 1997.