On Catalan's Conjecture

Risto Huovinen

MSc thesis
April 2024

Reviewers:
Prof. Vesa Halava
PhD. Sebastian Zuniga Alterman

DEPARTMENT OF MATHEMATICS AND STATISTICS

TURUN YLIOPISTO
Matematiikan ja tilastotieteen laitos

Risto Huovinen: On Catalan's Conjecture
Pro gradu -tutkielma, 95 s.
Matematiikka
Huhtikuu 2024

Catalanin otaksuma on väittämä, jonka mukaan Catalanin yhtälöön $x^n - y^m = 1$, missä $x, y > 0$ ja $n, m > 1$ ovat luonnollisia lukuja, ei ole muita ratkaisuja kuin $3^2 - 2^3 = 1$.

Tässä työssä tarkastellaan Catalanin otaksumaan liittyviä osittaisia tuloksia. Catalanin otaksuma esitetään, mutta sitä ei todisteta.

Tutkielmassa todistetaan, että jos Catalanin yhtälön ratkaisussa (x, y, n, m) y on alkuluku, niin $y = 2$ ja $x = 3, n = 2, m = 3$.

Lisäksi todistetaan Casselsin lause, mikä antaa jaollisuusehtoja sellaisille Catalanin yhtälön ratkaisuille (x, y, n, m), missä n ja m ovat parittomia alkulukuja.

Casselsin lauseen avulla todistetaan lisää jaollisuusehtoja sellaisille Catalanin yhtälön ratkaisuille (x, y, n, m), missä n ja m ovat parittomia alkulukuja.

Tutkielman lopussa esitetään tuloksia ympyräkunnista ja niiden ihanteista ja todistetaan Inkerin lause, minkä avulla todistetaan, että suurelle määrälle alkulukuja $p, q > 2$ yhtälölle $x^p - y^q = 1$ ei ole ratkaisuja, missä $x, y > 0$.

Asiasanat: Catalanin otaksuma, ympyräkunta

Contents

1 Introduction

Eugène Catalan conjectured in 1844 that 2^3 and 3^2 are the only consecutive powers of natural numbers. The conjecture was proved by Preda Mihăilescu in 2002 by applying results from the theory of cyclotomic fields.

Catalan's Conjecture is among the famous problems in number theory that are simple to state, but difficult to prove, as attested to by the fact that the conjecture remained unsolved for some 150 years. We will present Catalan's Conjecture, make some immediate observations, and consider divisibility conditions for a solution to the Catalan's equation $x^p - y^q = 1$, including Cassels' theorem, and present techniques that were invented in an attempt to prove the conjecture in the late 20th century. In the end we prove partial results to the problem using results involving cyclotomic fields, including Inkeri's lemmas.

The actual proof of the conjecture, which is not presented in this work, examines the properties of the group of units of the ring of integers of the $p-$th cyclotomic field using properties of annihilators of ideals, eventually finding a property of that group which is impossible, as discussed by Metsänkylä in his 2003 article on Catalan's conjecture in [3].

In this work we assume basic facts about modular arithmetic. Theory of cyclotomic fields is covered as needed and no prior knowledge is assumed except arithmetic of complex numbers. The thesis is based on Paulo Ribenboim's book on Catalan's Conjecture [1], written at a time when the conjecture had not yet been proved.

2 Preliminaries

We will now gather facts which are used in the forthcoming chapters.

For a prime p and an integer $n \neq 0$, $v_p(n)$ denotes the *p-adic valuation of n*, that is $v_p(n) = k$ if $p^k \mid n$ and $p^{k+1} \nmid n$. Let n, m be integers, it is immediate that

$$v_p(mn) = v_p(m) + v_p(n).$$

If $v_p(n) < v_p(m)$ then

$$v_p(n+m) = v_p(n).$$

Define $v_p(0) = \infty$, and for $n \neq 0$, define $v_p\left(\frac{m}{n}\right) = v_p(m) - v_p(n)$. This is well defined, because for any integer $k \neq 0$ we have

$$\begin{aligned} v_p\left(\frac{km}{kn}\right) &= v_p(km) - v_p(kn) = [v_p(k) + v_p(m)] - [v_p(k) + v_p(n)] \\ &= v_p(m) - v_p(n) = v_p\left(\frac{m}{n}\right). \end{aligned}$$

For a prime q and an integer $n \geq 0$, the *q-adic expansion of n* is

$$n = a_0 + a_1 q + \cdots + a_n q^n$$

where the integers a_i satisfy $0 \leq a_i \leq q-1$ for $0 \leq i \leq n$.

Lemma 2.1. For coprime integers n and m, there exists an integer $a > 0$ such that $an \equiv 1 \pmod{m}$ and $gcd(a, m) = 1$.

Proof. Since n and m are coprime, by Bézout's identity, there exists integers a, b such that

$$an + bm = 1, \tag{1}$$

which means that $an \equiv 1 \pmod{m}$. We may assume that $a > 0$: if $a < 0$, then for an arbitrary integer k we get from the congruence $an \equiv 1 \pmod{m}$ that

$$an + kmn = (a + km)n \equiv 1 \pmod{m}$$

whereupon the integer k may be chosen such that $a + km > 0$. Denote $gcd(a, m) = d$. Then, from equation (1), $d \mid an + bm = 1$, hence $d = 1$. □

Let $m > 0$ and x be integers such that $gcd(x, m) = 1$. The *order of x modulo m*, denoted by $\mathrm{ord}_m(x)$, is the least integer $k > 0$ such that $x^k \equiv 1 \pmod{m}$.

For a real number r, *the floor function*, $\lfloor r \rfloor$, denotes the greatest integer k such that $k \leq r$.

3 Catalan's conjecture

Catalan's conjecture states that the equation

$$x^n - y^m = 1 \tag{2}$$

has no solution in natural numbers for $x, y > 0$ and $n, m > 1$ other than $3^2 - 2^3 = 1$. To prove this conjecture, it suffices to show that

$$x^p - y^q = 1 \tag{3}$$

has no solution for $x, y > 0$ and distinct prime exponents p and q other than $3^2 - 2^3 = 1$. This follows from the fact that if a solution exists to the equation (2) then also

$$(x^{\frac{n}{p}})^p - (y^{\frac{m}{q}})^q = 1$$

where primes p and q are arbitrary prime factors of n and m, respectively. If $p = q$ we have

$$1 = x^p - y^p = (x - y) \sum_{i=1}^{p} x^{p-i} y^{i-1},$$

which leads to a contradiction, because

$$\sum_{i=1}^{p} x^{p-i} y^{i-1} \geq \sum_{i=1}^{2} x^{2-i} y^{i-1} = x + y > 1.$$

So we may assume $p \neq q$ in what follows. Hence a solution to the equation (2) implies that there is a solution to the equation (3). The contraposition leads to that if the equation (3) has no solutions then neither does the equation (2).

The process of proving the non-existence of solutions to equation (3) other than $3^2 - 2^3 = 1$ may be divided into two cases according to the greatest common divisor (*gcd*) of the integers $x - 1$ and $\frac{x^p - 1}{x - 1}$, which appear in the equation

$$y^q = x^p - 1 = (x - 1) \frac{x^p - 1}{x - 1}.$$

Case I is when the *gcd* of $x - 1$ and $\frac{x^p - 1}{x - 1}$ equals 1, and *Case II* is when this *gcd* equals p. These are the only two possibilities which will be shown in the following lemma. The lemma considers also the *gcd* of the integers $x + 1$ and $\frac{x^p + 1}{x + 1}$, which will be useful in the forthcoming chapter.

Theorem 3.1. Given a prime p and an integer $x \neq \pm 1$, the *gcd* of the integers

$$x + 1 \text{ and } \frac{x^p + 1}{x + 1},$$

is either 1 or p, and the *gcd* of the integers

$$x - 1 \text{ and } \frac{x^p - 1}{x - 1},$$

is either 1 or p.

Proof. Let $x \neq \pm 1$ be an integer. If $p = 2$ then

$$\left| x \pm 1 - \frac{x^2 \pm 1}{x \pm 1} \right| = |x \pm 1 - (x \mp 1)| = 2,$$

so the *gcd* is either 1 or 2 as desired. Let us suppose p is an odd prime. Noting that

$$gcd\left(x - 1, \frac{x^p - 1}{x - 1}\right) = gcd\left(-x + 1, \frac{(-x)^p + 1}{-x + 1}\right)$$

it suffices to prove the claim for the integers

$$x - 1 \text{ and } \frac{x^p - 1}{x - 1}.$$

Let d be the *gcd* of the above integers. Then $x \equiv 1 \pmod{d}$ and

$$0 \equiv \frac{x^p - 1}{x - 1} \equiv 1 + x + \cdots + x^{p-1} \equiv p \pmod{d}.$$

Therefore d is a factor of p, which implies that $d = 1$ or $d = p$. □

The following lemma states some necessary properties of a solution to the equation (3) under certain restrictions, which will be useful in proving Cassels' Theorem in chapter 5. The ultimate goal of considerations like these is to find properties that a solution must possess, but which turn out to be impossible. We do not yet achieve this ultimate goal, but the lemma provides useful conditions nonetheless.

Lemma 3.2. Let p, q be distinct odd primes and $x, y > 0$ integers such that $x^p - y^q = \pm 1$. If $q \mid x$, then exists integers a, b such that

$$\begin{cases} y \pm 1 = q^{p-1}a^p \\ \dfrac{y^q \pm 1}{y \pm 1} = qb^p \end{cases}$$

where $q \nmid b$, $gcd\,(a, b) = 1$, $x = qab$.

Proof. Let $q \mid x$. Then we get that $0 \equiv x^p = y^q \pm 1 \equiv y \pm 1 \pmod{q}$, using Fermat's small theorem, and this implies $q \mid y \pm 1$. Since $y \equiv \mp 1 \pmod{q}$, we have that

$$\begin{aligned} \frac{y^q \pm 1}{y \pm 1} &= 1 + (\mp y) + \cdots + (\mp y)^{q-1} \\ &\equiv 1 + (\mp(\mp 1)) + \cdots + (\mp(\mp 1))^{q-1} \pmod{q} \\ &\equiv 1 + (1) + \cdots + (1)^{q-1} \equiv q \equiv 0 \pmod{q}, \end{aligned}$$

so $q \mid \frac{y^q \pm 1}{y \pm 1}$. By Theorem 3.1 $gcd\left(y \pm 1, \frac{y^q \pm 1}{y \pm 1}\right)$ is 1 or q, hence $gcd\left(y \pm 1, \frac{y^q \pm 1}{y \pm 1}\right) = q$. Then there exists integers a, b such that one of the following cases is true:

$$\begin{cases} y \pm 1 = qb^p \\ \dfrac{y^q \pm 1}{y \pm 1} = q^{p-1}a^p, \end{cases} \tag{4}$$

or

$$\begin{cases} y \pm 1 = q^{p-1}a^p \\ \dfrac{y^q \pm 1}{y \pm 1} = qb^p, \end{cases} \tag{5}$$

where $q \nmid b$, $gcd\,(a, b) = 1$, $x = qab$. If the equations (4) hold, then $y = qb^p \mp 1$, so that modulo q^3 we have the congruence

$$0 \equiv x^p = y^q \pm 1 = (qb^p \mp 1)^q \pm 1 = \sum_{k=0}^{q} \binom{q}{k} (qb^p)^k (\mp 1)^{q-k} \pm 1 \equiv q^2 b^p \pmod{q^3},$$

which is a contradiction, since $q \nmid b$. Therefore the equations (5) must hold. □

In Lemma 3.2 it was assumed that $q \mid x$, but it will be shown later that this fact already follows from the preceding assumptions of the lemma.

4 Special cases

Instead of trying to prove Catalan's conjecture outright, we will now prove that if $n, m > 1$ and $x > 0$ are integers and q is a prime number such that

$$x^n - q^m = 1,$$

then $x^n = 3^2$ and $q^m = 2^3$. This will require a few preliminary lemmas.

Lemma 4.1. If q is a prime number and $n, m > 0$ are integers such that

$$2^n - q^m = 1,$$

then $q \equiv 3 \pmod 4$ and m is odd.

Proof. It follows from the equation $2^n - q^m = 1$ that q is odd. If $n = 1$ then $2 - q^m = 1$, so $q^m = 1$, which is a contradiction since q is a prime number and $m > 0$. Therefore $n \geq 2$. Since q is an odd prime, we have that $q \equiv 1$ or $q \equiv 3 \pmod 4$. Since $n \geq 2$, we have that

$$q^m = 2^n - 1 \equiv 3 \pmod 4.$$

Therefore, $q \equiv 3 \pmod 4$ with odd m. □

Lemma 4.2. If q is prime number and $n, m > 0$ are integers such that

$$2^n - q^m = 1,$$

then $m = 1$ and n is a prime number.

Proof. Suppose $m = pk$ where p is prime. It follows from the equation $2^n - q^m = 1$ that q is odd. By Lemma 4.1, pk is odd, so in particular p is odd. Now

$$\begin{aligned} 2^n &= -((-q)^k - 1)\frac{(-q)^{pk} - 1}{(-q)^k - 1} \\ &= -((-q)^k - 1)(1 + (-q)^k + ((-q)^k)^2 + \cdots + ((-q)^k)^{p-1}) \end{aligned}$$

where the integer

$$s = 1 + (-q)^k + ((-q)^k)^2 + \cdots + ((-q)^k)^{p-1}$$

is odd since p is odd. Then $s \mid 2^n$ where s is odd, so necessarily $s = 1$ which implies $p = 1$, which is a contradiction. Hence $m = 1$.

If $n = 1$ then from $2^n - q^m = 1$ and $m = 1$ we get that $q = 1$, which is a contradiction since q is prime. Therefore $n \geq 2$, so we may write $n = pk$ where p is prime and $k > 0$. Now we have that

$$q = (2^p - 1)\frac{2^{pk} - 1}{2^p - 1}$$

implying $k = 1$, since q is prime, and therefore $n = p$.

□

Theorem 4.3. If q is a prime number, x is an integer, and $n, m \geq 2$ are integers such that

$$x^n - q^m = 1,$$

then $x^n = 3^2$ and $q^m = 2^3$.

Proof. Let us first show that it suffices to prove the claim for instances where n is prime. Suppose the claim is true for all primes n. Suppose $a \geq 2$ is an integer such that $x^a - q^m = 1$. Let p be a prime factor of a. Now

$$(x^{\frac{a}{p}})^p - q^m = 1$$

so by assumption $(x^{\frac{a}{p}})^p = x^a = 3^2$ and $q^m = 2^3$ as desired.

Let us suppose that $x^p - q^m = 1$ where q is prime and $p, m \geq 2$. Then

$$q^m = (x-1)\frac{x^p - 1}{x - 1} \tag{6}$$

where by Theorem 3.1 $gcd\left(x-1, \frac{x^p-1}{x-1}\right)$ is 1 or p. If the gcd is 1, then from the fact that both factors are powers of q, it follows that exactly one of them is equal to 1. Since

$$\frac{x^p - 1}{x - 1} \geq \frac{x^2 - 1}{x - 1} = x + 1 > x - 1,$$

it must be that $x - 1 = 1$, hence $x = 2$. If the gcd is p, then from the equation (6) it follows that $p \mid q^m$, which implies $p = q$. Since the integers $x - 1$ and $\frac{x^p-1}{x-1}$ are both powers of q and $gcd\left(x-1, \frac{x^p-1}{x-1}\right) = q$ and $\frac{x^p-1}{x-1} > x - 1$, it follows that $x - 1 = q$. Now we have that

$$(q+1)^q - 1 = q^m.$$

Then using the binomial theorem we get that

$$q^m = \sum_{k=1}^{q} \binom{q}{k} q^k = q^2 \left(1 + \sum_{k=2}^{q} \binom{q}{k} q^{k-2}\right). \tag{7}$$

If $q \geq 3$ then q divides $\binom{q}{2}$, whereby q divides the sum $\sum_{k=2}^{q} \binom{q}{k} q^{k-2}$. But then the factor $1 + \sum_{k=2}^{q} \binom{q}{k} q^{k-2}$ on the right-hand side of the equation (7) is not a power of q, which is a contradiction. Thus $q = 2$. Hence $x^n = 3^2$ and $q^m = 2^3$.

In the case of $x = 2$, it follows from lemma 4.2 that $m = 1$, which contradicts the assumption $m \geq 2$. □

The following theorem shows that if $x^p - y^q = 1$ for odd primes p, q and integers $x, y > 0$, then x and y cannot be successive integers except when $x^p = 3^2$ and $y^q = 2^3$.

Theorem 4.4. If $x^p - y^q = 1$ where $x \geq 2$ and $y \geq 3$ and p, q are distinct odd primes, then $x \not\equiv 1 \pmod{y}$ and $x \not\equiv -1 \pmod{y}$.

Proof. Assume first that $x \equiv -1 \pmod{y}$. Then $1 = x^p - y^q \equiv -1 \pmod{y}$, which is a contradiction since $y \geq 3$. Next, assume that $x \equiv 1 \pmod{y}$. Now

$$y^q = (x-1)\frac{x^p - 1}{x - 1} \tag{8}$$

where by Theorem 3.1 the *gcd* of the factors on the right-hand side is either 1 or p. Since $x-1$ is a non-zero multiple of y, it must be that the *gcd* is p and

$$gcd\left(y, \frac{x^p-1}{x-1}\right) = p.$$

From this, and the fact that $\frac{x^p-1}{x-1} \mid y^q$ in equation (8), we have that

$$\frac{x^p-1}{x-1} = p^{n-1}$$

for some integer $n \geq 2$. Since $gcd\left(x-1, \frac{x^p-1}{x-1}\right) = p$, we may write

$$x-1 = mp$$

where $m > 0$. Since $p^3 \mid y^q$, we have that $p^2 \nmid x-1 = mp$, and, therefore, $p \nmid m$. Now $y^q = p^n m$. Since p is prime, it satisfies $p \mid \binom{p}{k}$ for $0 < k < p$. Now we have

$$0 \equiv x^p - 1 = (mp+1)^p - 1 = \sum_{k=1}^{p} \binom{p}{k} (pm)^k \equiv p^2 m \pmod{p^3},$$

which is a contradiction. □

5 Theorem of Cassels

Cassels' theorem provides further necessary conditions for a possible solution for Catalan's equation. In order to prove Cassels' theorem, several lemmas are required. The lemmas and their proofs are from [1] unless otherwise indicated.

Lemma 5.1. If $n > 1$ and x, y are non-zero relatively prime integers, then

$$\frac{x^n - y^n}{x - y} = k(x - y) + ny^{n-1}$$

where

$$k = \sum_{i=0}^{n-2} \binom{n}{i} (x - y)^{n-2-i} y^i.$$

Proof. Using Newton's binomial formula, we get that

$$\begin{aligned}
\frac{x^n - y^n}{x - y} &= \frac{((x - y) + y)^n - y^n}{x - y} = \frac{\sum_{i=0}^{n} \binom{n}{i} (x - y)^{n-i} y^i - y^n}{x - y} \\
&= \frac{\sum_{i=0}^{n-1} \binom{n}{i} (x - y)^{n-i} y^i}{x - y} = \sum_{i=0}^{n-1} \binom{n}{i} (x - y)^{n-1-i} y^i \\
&= \sum_{i=0}^{n-2} \binom{n}{i} (x - y)^{n-1-i} y^i + ny^{n-1} = k(x - y) + ny^{n-1}
\end{aligned}$$

where k is as claimed. □

Lemma 5.2. Let a, b, t be real numbers such that $b > 0$, $t > 1$, and $a + b^t > 0$ and let $f_{a,b}(t) = (a + b^t)^{1/t}$. Then

$$f'_{a,b}(t) > 0 \text{ if and only if } b^t \log b^t > (a + b^t) \log (a + b^t).$$

In particular, for real numbers $m > n > 1$ and $z > 1$ we have the inequalities

$$\begin{aligned}
(z^n - 1)^m &< (z^m - 1)^n \\
(z^m + 1)^n &< (z^n + 1)^m.
\end{aligned}$$

Proof. Let us denote $f(t) = f_{a,b}(t)$. Now

$$f'(t) = \frac{(a + b^t)^{\frac{1}{t}}}{t} \left(\frac{b^t \log b}{a + b^t} - \frac{1}{t} \log (a + b^t) \right)$$

where $\frac{(a+b^t)^{\frac{1}{t}}}{t} > 0$, and, therefore, $f'(t) > 0$ if and only if

$$\frac{b^t \log b}{a + b^t} - \frac{1}{t} \log (a + b^t) > 0,$$

which is equivalent to $b^t \log b^t > (a + b^t) \log (a + b^t)$.

Let $a = -1$, $b = z > 1$, and $t > 1$, so that $a+b^t = z^t-1 > 0$. Now $z^t > z^t-1 > 0$, using the monotony of the log function, we have that $\log z^t > \log(z^t - 1)$ and now we get that

$$z^t \log(z^t) > (z^t - 1)\log(z^t - 1).$$

This implies by the first claim that $f'_{-1,z}(t) > 0$. Therefore, for for $m > n > 1$ we have $f_{-1,z}(n) < f_{-1,z}(m)$, that is,

$$0 < (z^n - 1)^{\frac{1}{n}} < (z^m - 1)^{\frac{1}{m}}.$$

Raising the inequality to the mn-th power gives

$$(z^n - 1)^m < (z^m - 1)^n.$$

For the other case, let $a = 1$, $z > 1$, $b = \frac{1}{z}$, and $t > 1$. Now $0 < \frac{1}{z^t} < 1$, and hence

$$\frac{1}{z^t}\log\frac{1}{z^t} < 0 < \left(1 + \frac{1}{z^t}\right)\log\left(1 + \frac{1}{z^t}\right),$$

which implies that $f'_{1,\frac{1}{z}}(t) < 0$. Then for $m > n > 1$ we have $f_{1,\frac{1}{z}}(m) < f_{1,\frac{1}{z}}(n)$, using the first claim, which implies

$$\begin{aligned}
(1 + \frac{1}{z^m})^{\frac{1}{m}} &< (1 + \frac{1}{z^n})^{\frac{1}{n}} \\
(1 + \frac{1}{z^m})^n &< (1 + \frac{1}{z^n})^m \\
(\frac{z^m + 1}{z^m})^n &< (\frac{z^n + 1}{z^n})^m \\
(z^m + 1)^n &< (z^n + 1)^m.
\end{aligned}$$

□

We will now prove a lemma concerning the p-adic valuation of a factorial, which will be needed in the proof of Cassels' theorem.

Lemma 5.3. Let q be a prime number and $R > 0$ an integer. Let

$$R = R_0 + R_1 q + \cdots + R_m q^m$$

be the q-adic expansion of R, and let

$$s = R_0 + R_1 + \cdots + R_m.$$

Then

$$v_q(R!) = \frac{R - s}{q - 1}.$$

Proof. Let us first show that the claim holds in the case of $R = rq^m$ for $m \geq 0$ and $0 < r \leq q - 1$. Then $s = r$. If $m = 0$ then $R = r < q$ and $v_q(R) = 0 = \frac{r-r}{q-1}$. Suppose $m \geq 1$.

Let $1 \leq i \leq m-1$. Then there are exactly $r(q-1)q^{m-1-i}$ integers n in the interval $1 \leq n \leq rq^m$ such that $q^i \mid n$, but $q^{i+1} \nmid n$, which is to say that $v_q(n) = i$. Indeed, in this interval the multiples of q^i are precisely the integers

$$1 \cdot q^i, 2 \cdot q^i, 3 \cdot q^i, \ldots, rq^{m-i} \cdot q^i,$$

which counts up to rq^{m-i} numbers in total. Similarly, the multiples of q^{i+1} counts up to rq^{m-i-1}, which means that the number of integers $1 \leq n \leq rq^m$ such that $v_q(n) = i$ equals $rq^{m-i} - rq^{m-i-1} = r(q-1)q^{m-1-i}$. The multiples of q^m in the interval $[1, rq^m]$ are $q^m, 2q^m, \ldots, rq^m$, which makes r numbers in total.

Now we may write

$$\begin{aligned} v_q\left[(rq^m)!\right] &= \sum_{n=1}^{rq^m} v_q(n) = \sum_{i=1}^{m} \sum_{\substack{v_q(n)=i \\ 1 \leq n \leq rq^m}} i \\ &= \sum_{i=1}^{m-1} ir(q-1)q^{m-1-i} + rm = r(q-1)\sum_{i=1}^{m-1} iq^{m-1-i} + rm \\ &= r(q-1)\frac{q^m - 1 - m(q-1)}{(q-1)^2} + rm = \frac{rq^m - r}{q-1} \end{aligned}$$

so the claim holds for $R = rq^m$.

Let us now proceed by induction. Suppose that the claim holds for $R = R_n q^n + \cdots + R_m q^m \neq 0$, where $1 \leq n \leq m$, and $0 \leq R_i \leq q-1$ for $i = n, n+1, \ldots, m$. Let $s = R_n + R_{n+1} + \cdots + R_m$.

Let us show that the claim holds for $L = R_{n-1}q^{n-1} + R$ where $0 \leq R_{n-1} \leq q-1$. If $R_{n-1} = 0$ then $L = R$. Hence suppose that $R_{n-1} > 0$. Then the q-adic expansion of L is $R_{n-1}q^{n-1} + R_n q^n + \cdots + R_m q^m$, and denote $s' = R_{n-1} + s$.

Now

$$v_q(L!) = v_q\left[(R_{n-1}q^{n-1} + R)!\right] = v_q(R!) + v_q\left[(R+1)(R+2)\cdots(R+R_{n-1}q^{n-1})\right].$$

Since $n \leq v_q(R) < \infty$ and $q^n \nmid i$ for $1 \leq i \leq R_{n-1}q^{n-1}$, implying that $v_q(i) < n$, it follows that $v_q(R+i) = v_q(i)$ for $1 \leq i \leq R_{n-1}q^{n-1}$. Hence

$$\begin{aligned} v_q\left[(R+1)(R+2)\cdots(R+R_{n-1}q^{n-1})\right] &= \sum_{i=1}^{R_{n-1}q^{n-1}} v_q(R+i) = \sum_{i=1}^{R_{n-1}q^{n-1}} v_q(i) \\ &= v_q\left[(R_{n-1}q^{n-1})!\right], \end{aligned}$$

and using the induction hypothesis, we have that

$$v_q(L!) = v_q(R!) + v_q\left[(R_{n-1}q^{n-1})!\right] = \frac{R-s}{q-1} + \frac{R_{n-1}q^{n-1} - R_{n-1}}{q-1} = \frac{L-s'}{q-1}.$$

□

Lemma 5.4. If r, m, n are positive integers and l is a prime number such that $l \nmid n$, then

$$v_l(r!) \leq v_l\left[\frac{m}{n}\left(\frac{m}{n} - 1\right)\cdots\left(\frac{m}{n} - (r-1)\right)\right].$$

Proof. Let $a = \frac{m}{n}\left(\frac{m}{n}-1\right)\cdots\left(\frac{m}{n}-(r-1)\right)$ and let $v_l(a) = e < \infty$. Since $l \nmid n$, by Lemma 2.1, there exists $n' \geq 1$, $l \nmid n'$, such that $nn' \equiv 1 \pmod{l^{e+1}}$. Let $m' = mn'$ and let $a' = m'(m'-1)\cdots(m'-(r-1))$. Now

$$\begin{aligned}
v_l(a) &= v_l\left[\frac{m}{n}\left(\frac{m}{n}-1\right)\cdots\left(\frac{m}{n}-(r-1)\right)\right] \\
&= v_l\left[\frac{m}{n}\left(\frac{m-n}{n}\right)\cdots\left(\frac{m-n(r-1)}{n}\right)\right] \\
&= v_l\left[m(m-n)\cdots(m-n(r-1))\right] \\
&= \sum_{k=0}^{r-1} v_l(m-kn) \\
&= \sum_{k=0}^{r-1} \left[v_l(m-kn) + v_l(n')\right] \\
&= \sum_{k=0}^{r-1} v_l(m'-knn') \\
&= v_l\left[m'(m'-nn')\cdots(m'-nn'(r-1))\right]
\end{aligned}$$

where

$$m'(m'-nn')\cdots(m'-nn'(r-1)) \equiv m'(m'-1)\cdots(m'-(r-1)) = a' \pmod{l^{e+1}},$$

which implies $m'(m'-nn')\cdots(m'-nn'(r-1)) = a' + dl^{e+1}$ for some integer d. Then

$$v_l(a) = v_l(a' + dl^{e+1}).$$

If $v_l(a') \geq e+1$ then $e = v_l(a) = v_l(a' + dl^{e+1}) \geq e+1$, which is a contradiction. Thus $v_l(a') < e+1$, which implies $v_l(a) = v_l(a' + dl^{e+1}) = v_l(a')$. Since $\frac{a'}{r!} = \binom{m'}{r}$ is an integer, we have that $v_l(r!) \leq v_l(a') = v_l(a)$. □

Lemma 5.5. If $p > q$ where p and q are odd primes and $x, y \geq 2$ are integers such that $x^p - y^q = \pm 1$, then

$$(x \mp 1)^p q^{(p-1)q} > (y \pm 1)^q.$$

Proof. Since $x \mp 1 \geq \frac{x}{2}$, $x^p = y^q \pm 1 > \frac{y^q}{2}$, and $y > \frac{y \pm 1}{2}$, we have the inequality

$$(x \mp 1)^p \geq \left(\frac{x}{2}\right)^p > \frac{y^q}{2^{p+1}} > \frac{(y \pm 1)^q}{2^{p+q+1}}.$$

Because $p > q$ are odd primes, clearly $p \geq q+2$, hence

$$(p-1)(q-1) \geq (q+1)(q-1) = q^2 - 1 > 2 + q$$

since $q \geq 3$. Now $(p-1)q > p+q+1$, implying $q^{(p-1)q} > 2^{p+q+1}$, and we get that $(x \mp 1)^p > \frac{(y \pm 1)^q}{q^{(p-1)q}}$, which proves the claim. □

The following theorem is called Cassels' Theorem. It was originally proved by Cassels in 1960. We present the proof from [1].

Theorem 5.6 (Cassels' Theorem)**.** If p, q are distinct odd primes and $x, y > 0$ are integers such that $x^p - y^q = \pm 1$, then $p \mid y$ and $q \mid x$.

Proof. We may assume $p > q$ and $x, y \geq 2$: if the claim is true in the case of $p > q$, then any odd primes $q' > p'$ satisfying the equation $x^{p'} - y^{q'} = \pm 1$, where $x, y > 0$, also satisfy $y^{q'} - x^{p'} = \mp 1$, so by assumption $q' \mid x$ and $p' \mid y$ as desired. If $x = 1$, then $y^q = 0$ or 2, which is impossible. Likewise, if $y = 1$, then $x^p = 0$ or 2, which similarly leads to a contradiction.

Let us show that $q \mid x$. Assume on the contrary that $q \nmid x$, which implies that $q \nmid x^p = y^q \pm 1 = (y \pm 1)\frac{y^q \pm 1}{y \pm 1}$. By Theorem 3.1, the $gcd\left(y \pm 1, \frac{y^q \pm 1}{y \pm 1}\right) = 1$ or q, so the gcd must be 1. Then there exists an integer $d > 0$ such that $y \pm 1 = d^p$.

Case 1: suppose $y + 1 = d^p$. Then $d \geq 2$, and

$$x^p = y^q + 1 = (d^p - 1)^q + 1 < d^{pq}.$$

Therefore, $x < d^q$ and, moreover, $x \leq d^q - 1$. Since $q < p$, by Lemma 5.2 we have the inequality $(d^q - 1)^p < (d^p - 1)^q$. Now

$$y^q + 1 = x^p \leq (d^q - 1)^p < (d^p - 1)^q = y^q,$$

which is a contradiction.

Case 2: suppose $y - 1 = d^p$. Since $q < p$, we have $2 \leq x < y$, so $d \geq 2$. Now

$$x^p = y^q - 1 = (d^p + 1)^q - 1 > d^{pq}.$$

Therefore, $x > d^q$ and, moreover, $x \geq d^q + 1$. Since $q < p$, by Lemma 5.2 we have the inequality $(d^p + 1)^q < (d^q + 1)^p$, so now

$$y^q - 1 = x^p \geq (d^q + 1)^p > (d^p + 1)^q = y^q,$$

which is a contradiction. Therefore, $q \mid x$.

Let us show next that $p \mid y$. Since $q \mid x$, by Lemma 3.2 there exists integers $b, c > 0$ such that

$$\begin{cases} y \pm 1 = q^{p-1}b^p \\ \dfrac{y^q \pm 1}{y \pm 1} = qc^p \end{cases}$$

where $q \nmid c$ and $x = qbc$. We will prove next that $c > 1$. The inequality

$$\frac{y^q \pm 1}{y \pm 1} \geq \frac{y^3 \pm 1}{y \pm 1} = 1 \mp y + y^2 \geq y \pm 1$$

holds whenever $1 \mp y + y^2 \geq y \pm 1$, which is equivalent with

$$y \geq 1 \pm 1 + \frac{\pm 1 - 1}{y}, \tag{9}$$

which is true since $y \geq 2$ and the right side of the inequality (9) is either 2 or -1. Thus, if $c = 1$, we have $\frac{y^q \pm 1}{y \pm 1} = q \geq y \pm 1 = q^{p-1}b^p$, which is a contradiction, so necessarily $c > 1$.

Next we show that $c \equiv 1 \pmod{q^{p-1}}$. By Lemma 5.1 we have $qc^p = \frac{y^q \pm 1}{y \pm 1} = k(y \pm 1) + q$ where

$$k = \sum_{i=0}^{q-2} \binom{q}{i} (y \pm 1)^{q-2-i} (\pm 1)^i,$$

implying that $q \mid k$. Therefore, $q(c^p - 1) \equiv 0 \pmod{q^p}$, which implies $c^p \equiv 1 \pmod{q^{p-1}}$. If $c \not\equiv 1 \pmod{q^{p-1}}$, then the order of c modulo q^{p-1} must be properly greater than 1, that is, $\mathrm{ord}_{q^{p-1}}(c) = a > 1$, and furthermore $a \mid p$, implying that $a = p$. Then $p \mid \varphi(q^{p-1}) = q^{p-2}(q-1)$, which means that $p \mid q - 1$. This contradicts the assumption that $q < p$. Hence $c \equiv 1 \pmod{q^{p-1}}$.

We have now that $x \neq qb$ since $c \neq 1$, and $x \equiv qb \pmod{q^p}$ since $c \equiv 1 \pmod{q^{p-1}}$.

Let us suppose on the contrary that $p \nmid y$. Then it follows from $y^q = (x \mp 1)\frac{x^p \mp 1}{x \mp 1}$ and Theorem 3.1 that $gcd\left(x \mp 1, \frac{x^p \mp 1}{x \mp 1}\right) = 1$ and, therefore, there exists an integer $a \geq 1$ such that

$$x \mp 1 = a^q. \tag{10}$$

By Lemma 5.5 we have

$$a^{pq} = (x \mp 1)^p > \frac{(y \pm 1)^q}{q^{(p-1)q}} = b^{pq},$$

implying $a > b$.

Next we will prove that $a^q \geq \frac{q^p}{2}$. Suppose on the contrary that $a^q < \frac{q^p}{2}$. Since $x \neq qb$ and $x \equiv qb \pmod{q^p}$, so $|x - qb| \geq q^p$, we have the inequality

$$q^p \leq |x - qb| \leq |a^q \pm 1 - qb| \leq a^q + qb \pm 1 < \frac{q^p}{2} + qb \pm 1,$$

and, therefore, $qb \pm 1 > \frac{q^p}{2} > a^q$. On the other hand, since $a > b$, $b \geq 2$, and $q \geq 3$, we have that $a^q > b^q \geq qb + 1 \geq qb \pm 1$, contradicting the previous inequality. Hence $a^q \geq \frac{q^p}{2}$.

Using equation (10), we get the lower bounds

$$\begin{aligned} x^p &= (a^q \pm 1)^p \geq (a^q - 1)^p, \text{ and} \\ y^q &= x^p \mp 1 = (a^q \pm 1)^p \mp 1 \geq (a^q - 1)^p. \end{aligned}$$

Next we show that $(1 - \frac{2}{3^p})^p > \frac{1}{3}$ by showing that $(1 - \frac{2}{3^p})^p$ is increasing with respect to p. Indeed, since

$$1 - \frac{2}{3^{p+1}} = 1 - \frac{2}{3^p} + \frac{4}{3^{p+1}},$$

we have that

$$\begin{aligned}
\left(1-\frac{2}{3^{p+1}}\right)^{p+1} &= \left[\left(1-\frac{2}{3^p}\right)+\frac{4}{3^{p+1}}\right]^{p+1} \\
&= \sum_{i=0}^{p+1}\binom{p+1}{i}\left(1-\frac{2}{3^p}\right)^i\left(\frac{4}{3^{p+1}}\right)^{p+1-i} \\
&= \left(\frac{4}{3^{p+1}}\right)^{p+1}+\sum_{i=1}^{p}\binom{p+1}{i}\left(1-\frac{2}{3^p}\right)^i\left(\frac{4}{3^{p+1}}\right)^{p+1-i}+\left(1-\frac{2}{3^p}\right)^{p+1} \\
&\geq \left(\frac{4}{3^{p+1}}\right)^{p+1}+\left(1-\frac{2}{3^p}\right)^p\sum_{i=1}^{p}\binom{p+1}{i}\left(\frac{4}{3^{p+1}}\right)^{p+1-i}+\left(1-\frac{2}{3^p}\right)^{p+1} \\
&> \left(1-\frac{2}{3^p}\right)^p\cdot\frac{4(p+1)}{3^{p+1}}+\left(1-\frac{2}{3^p}\right)^{p+1} \\
&= \left(1-\frac{2}{3^p}\right)^p\left[\frac{2(p+1)}{3}\cdot\frac{2}{3^p}+1-\frac{2}{3^p}\right] > \left(1-\frac{2}{3^p}\right)^p.
\end{aligned}$$

Hence $(1-\frac{2}{3^p})^p > 1-\frac{2}{3}=\frac{1}{3}$, and

$$\left(1-\frac{2}{q^p}\right)^p \geq \left(1-\frac{2}{3^p}\right)^p > \frac{1}{3} \geq \frac{1}{q},$$

which together with the inequality $a^q \geq \frac{q^p}{2}$ proved above gives

$$\min\{x^p, y^q\} \geq (a^q-1)^p = a^{pq}\left(1-\frac{1}{a^q}\right)^p \geq a^{pq}\left(1-\frac{2}{q^p}\right)^p > \frac{a^{pq}}{q}. \tag{11}$$

Next step is to prove an upper bound for $\left|x^{\frac{p}{q}}-y\right|$. Noting that

$$\left(x^{\frac{p}{q}}-y\right)\frac{\left(x^{\frac{p}{q}}\right)^q-y^q}{x^{\frac{p}{q}}-y} = \left(x^{\frac{p}{q}}-y\right)\sum_{i=0}^{q-1}\left(x^{\frac{p}{q}}\right)^i y^{q-1-i} = x^p-y^q = \pm 1,$$

we get

$$\left|x^{\frac{p}{q}}-y\right| = \frac{1}{\sum_{i=0}^{q-1}\left(x^{\frac{p}{q}}\right)^i y^{q-1-i}}.$$

Using inequality (11) we have for each $i=0,1,\ldots,q-1$ the inequality

$$x^{\frac{pi}{q}}y^{q-1-i} > \left(\frac{a^{pq}}{q}\right)^{\frac{i}{q}}\left(\frac{a^p}{q^{\frac{1}{q}}}\right)^{q-1-i} = \left(\frac{a^{pq}}{q}\right)^{\frac{i}{q}}\left(\frac{a^{pq}}{q}\right)^{\frac{q-1-i}{q}} = \left(\frac{a^{pq}}{q}\right)^{\frac{q-1}{q}} = \frac{a^{p(q-1)}}{q^{\frac{q-1}{q}}} > \frac{a^{p(q-1)}}{q}.$$

This gives us a useful upper bound

$$\left|x^{\frac{p}{q}}-y\right| < \frac{1}{q\cdot\frac{a^{p(q-1)}}{q}} = \frac{1}{a^{p(q-1)}}. \tag{12}$$

On the other hand, by Taylor,

$$x^{\frac{p}{q}} = (a^q \pm 1)^{\frac{p}{q}} = \sum_{r=0}^{\infty} \binom{\frac{p}{q}}{r} (\pm 1)^r \left(a^q\right)^{\frac{p}{q}-r} = \sum_{r=0}^{\infty} (\pm 1)^r \frac{\frac{p}{q}\left(\frac{p}{q}-1\right)\cdots\left(\frac{p}{q}-(r-1)\right)}{r!} a^{p-rq}.$$

Let us write for $r \geq 0$

$$t_r = (\pm 1)^r \frac{\frac{p}{q}\left(\frac{p}{q}-1\right)\cdots\left(\frac{p}{q}-(r-1)\right)}{r!} a^{p-rq} \neq 0, \tag{13}$$

so that

$$x^{\frac{p}{q}} = \sum_{r=0}^{\infty} t_r. \tag{14}$$

Let $l \neq q$ be a prime and $r \geq 1$. By Lemma 5.4 we have that

$$v_l(r!) \leq v_l\left[\frac{p}{q}\left(\frac{p}{q}-1\right)\ldots\left(\frac{p}{q}-(r-1)\right)\right],$$

which means that for $r \geq 1$ we have that

$$v_l(t_r) = v_l(a^{p-rq}) + v_l\left[\frac{\frac{p}{q}\left(\frac{p}{q}-1\right)\cdots\left(\frac{p}{q}-(r-1)\right)}{r!}\right] \geq v_l(a^{p-rq}).$$

Note that $t_0 = a^p$, so the above inequality also holds in the case of $r = 0$.

Let

$$R = \left\lfloor \frac{p}{q} \right\rfloor + 1, \qquad\qquad \rho = \left\lfloor \frac{R}{q-1} \right\rfloor.$$

Then $R > \frac{p}{q}$, and, further, $Rq > p$.

For every $r \leq R$ and prime $l \neq q$ the inequality

$$v_l\left(t_r q^{R+\rho} a^{Rq-p}\right) \geq v_l(a^{p-rq}) + v_l(a^{Rq-p}) = v_l(a^{(R-r)q}) \geq 0$$

holds. In the case of $l = q$, we have

$$\begin{aligned} v_q(t_r) &= v_q(p(p-q)\cdots(p-q(r-1))) - v_q(r!q^r) + v_q(a^{p-rq}) \\ &= 0 - v_q(r!q^r) + v_q(a^{p-rq}) \\ &= -v_q(r!) - r + v_q(a^{p-rq}), \end{aligned}$$

and, therefore, it holds for $r \leq R$ that

$$\begin{aligned} v_q\left(t_r q^{R+\rho} a^{Rq-p}\right) &= -r - v_q(r!) + v_q(a^{p-rq}) + R + \rho + v_q(a^{Rq-p}) \\ &= R - r + \rho - v_q(r!) + (R-r)q v_q(a) \\ &\geq 0 \end{aligned}$$

since by Lemma 5.3 $v_q(r!) = \frac{r-s}{q-1} \leq \frac{R}{q-1} \leq \rho$, where $r = R_0 + R_1 q + \cdots + R_m q^m$, $0 \leq R_i \leq q-1$, and $s = R_0 + R_1 + \cdots + R_m$.

Thus, for $r = 0, 1, \ldots, R$, since the l-adic valuation of $t_r q^{R+\rho} a^{Rq-p}$ is non-negative for every prime l, we conclude that $t_r q^{R+\rho} a^{Rq-p}$ is an integer. Then the number

$$I = a^{Rq-p} q^{R+\rho} \left((y - x^{\frac{p}{q}}) + \sum_{r=R+1}^{\infty} t_r \right) = a^{Rq-p} q^{R+\rho} \left(y - \sum_{r=0}^{R} t_r \right) \tag{15}$$

is an integer since $Rq - p > 0$.

Let us show that $I \neq 0$. We write $I = I_1 + I_2 + I_3$ where

$$\begin{cases} I_1 = a^{Rq-p} q^{R+\rho} \left(y - x^{\frac{p}{q}} \right) \\ I_2 = a^{Rq-p} q^{R+\rho} t_{R+1} \neq 0 \\ I_3 = a^{Rq-p} q^{R+\rho} \displaystyle\sum_{r=R+2}^{\infty} t_r. \end{cases} \tag{16}$$

Since $R > \frac{p}{q}$, if $r > R$ then $\left| \frac{p}{q} - (r+i) \right| = r + i - \frac{p}{q} < r + i + 1$ for all $i \geq 0$. So for $n \geq 1$ we have that

$$\left| \frac{t_{r+n}}{t_r} \right| = \left| \frac{\left(\frac{p}{q} - r \right) \left(\frac{p}{q} - (r+1) \right) \cdots \left(\frac{p}{q} - (r+n-1) \right)}{(r+1)(r+2)\cdots(r+n)} \right| \frac{1}{a^{nq}} < \frac{1}{a^{nq}} \leq \left(\frac{2}{q^p} \right)^n$$

since $a^q \geq \frac{q^p}{2}$. Now

$$\begin{aligned} \left| \frac{I_3}{I_2} \right| = \left| \sum_{r=R+2}^{\infty} \frac{t_r}{t_{R+1}} \right| &\leq \sum_{r=R+2}^{\infty} \left| \frac{t_r}{t_{R+1}} \right| \\ &= \left| \frac{t_{R+2}}{t_{R+1}} \right| + \left| \frac{t_{R+3}}{t_{R+1}} \right| + \left| \frac{t_{R+4}}{t_{R+1}} \right| + \ldots \\ &< \frac{2}{q^p} + \left(\frac{2}{q^p} \right)^2 + \left(\frac{2}{q^p} \right)^3 + \ldots. \end{aligned}$$

and

$$\frac{2}{q^p} + \left(\frac{2}{q^p} \right)^2 + \left(\frac{2}{q^p} \right)^3 + \ldots = \frac{2}{q^p} \left(\frac{1}{1 - \frac{2}{q^p}} \right) = \frac{2}{q^p - 2} \leq \frac{2}{3^5 - 2} < \frac{1}{10}.$$

Next we show that

$$\frac{1}{q^2 (R+1)^2} \leq \left| a^{(R+1)q-p} t_{R+1} \right| \leq \frac{1}{4}. \tag{17}$$

Since $R > \frac{p}{q}$, we have $\left| \frac{p}{q} - i \right| = \frac{p}{q} - i \leq R - i$ for $i = 0, 1, \ldots, R-2$, and, therefore,

$$\begin{aligned} &\left| \frac{p}{q} \left(\frac{p}{q} - 1 \right) \cdots \left(\frac{p}{q} - (R-2) \right) \left(\frac{p}{q} - (R-1) \right) \left(\frac{p}{q} - R \right) \right| \\ &\leq R(R-1)\cdots 2 \left| \frac{p}{q} - (R-1) \right| \left| \frac{p}{q} - R \right| \\ &= R(R-1)\cdots 2 \left(\frac{p}{q} - (R-1) \right) \left(R - \frac{p}{q} \right) \\ &\leq R! \frac{1}{4}, \end{aligned}$$

because $\left(\frac{p}{q}-(R-1)\right)+\left(R-\frac{p}{q}\right)=1$ implies that their product is at most $\frac{1}{4}$. Indeed, if real numbers u,v are such that $u+v=1$, then $uv=u(1-u)=u-u^2$, which attains its highest value at $u=\frac{1}{2}$, hence $uv=\frac{1}{2}-\frac{1}{4}=\frac{1}{4}$.

The above estimate gives

$$|t_{R+1}|=\frac{\left|\frac{p}{q}\left(\frac{p}{q}-1\right)\cdots\left(\frac{p}{q}-R\right)\right|}{(R+1)!}a^{p-(R+1)q}\leq\frac{a^{p-(R+1)q}}{4(R+1)}. \tag{18}$$

On the other hand, since $R-i=\left\lfloor\frac{p}{q}\right\rfloor-(i-1)<\frac{p}{q}-(i-1)$ for $i=1,2,\ldots,R-1$, we have that

$$\begin{aligned}\left|\frac{p}{q}\left(\frac{p}{q}-1\right)\cdots\left(\frac{p}{q}-R\right)\right|&\geq(R-1)(R-2)\cdots 1\left|\frac{p}{q}-(R-1)\right|\left|\frac{p}{q}-R\right|\\&=(R-1)(R-2)\cdots 1\left(\frac{p}{q}-(R-1)\right)\left(R-\frac{p}{q}\right)\\&\geq\frac{(R-1)!}{q^2},\end{aligned}$$

since $R-\frac{p}{q}\geq\frac{1}{q}$ and $\frac{p}{q}-(R-1)\geq\frac{1}{q}$, because the inequality $\frac{p}{q}-(R-1)\geq\frac{1}{q}$ is equivalent to $p-1\geq q\left\lfloor\frac{p}{q}\right\rfloor$. To see that this holds, let $p=uq+v$ where u,v are integers with $0<v<q$. Then

$$\left\lfloor\frac{p}{q}\right\rfloor=\left\lfloor u+\frac{v}{q}\right\rfloor=u\leq u+\frac{v-1}{q}=\frac{uq+v-1}{q}=\frac{p-1}{q}.$$

Now

$$|t_{R+1}|=\frac{\left|\frac{p}{q}\left(\frac{p}{q}-1\right)\cdots\left(\frac{p}{q}-R\right)\right|}{(R+1)!}a^{p-(R+1)q}\geq\frac{a^{p-(R+1)q}}{q^2R(R+1)}. \tag{19}$$

By combining estimates (18) and (19), we have proved that

$$\frac{1}{q^2(R+1)^2}\leq\frac{1}{q^2(R+1)R}\leq\left|a^{(R+1)q-p}t_{R+1}\right|\leq\frac{1}{4(R+1)}\leq\frac{1}{4}. \tag{20}$$

Using this we will show that $\left|\frac{I_1}{I_2}\right|<\frac{1}{10}$. Indeed, by (12) and (20) we have that

$$\begin{aligned}\left|\frac{I_1}{I_2}\right|=\left|\frac{x^{\frac{p}{q}}-y}{t_{R+1}}\right|&\leq\left|x^{\frac{p}{q}}-y\right|\cdot q^2(R+1)^2a^{(R+1)q-p}\\&<\frac{1}{a^{p(q-1)}}q^2(R+1)^2a^{(R+1)q-p}=\frac{q^2(R+1)^2}{a^{q(p-R-1)}}.\end{aligned} \tag{21}$$

Let us verify that

$$p-R-1\geq 2\qquad\text{and}\qquad R+1\leq p. \tag{22}$$

Writing $p=uq+v$, where u,v are integers and $0<v<q$, we have that

$$p-R-1=p-\left\lfloor\frac{p}{q}\right\rfloor-2=uq+v-u-2=u(q-1)+v-2$$

where u or v is even, and hence at least 2. If $u \geq 2$ then $u(q-1)+v-2 \geq 2 \cdot 2 + 1 - 2 \geq 2$, and if $v \geq 2$ then also $u(q-1)+v-2 \geq 1 \cdot 2 + 2 - 2 \geq 2$. This verifies the first claim in (22).

Now

$$R + 1 = \left\lfloor \frac{p}{q} \right\rfloor + 2 = u + 2 \leq uq \leq uq + v = p,$$

which is true, since $2 \leq u(q-1)$, and we have verified the second claim in (22).

Returning to (21), by the inequality $a^q \geq \frac{q^p}{2}$ and (22) we now have that

$$\begin{aligned} \frac{q^2(R+1)^2}{a^{q(p-R-1)}} &\leq \left(\frac{2}{q^p}\right)^{p-R-1} q^2(R+1)^2 \leq \left(\frac{2}{q^p}\right)^2 q^2 p^2 \\ &= \left(\frac{2p}{q^{p-1}}\right)^2 \leq \left(\frac{2p}{3^{p-1}}\right)^2 \leq \left(\frac{2 \cdot 5}{3^4}\right)^2 \leq \frac{1}{10}. \end{aligned}$$

Moreover, since $\left|\frac{I_3}{I_2}\right| \leq \frac{1}{10}$ and $\left|\frac{I_1}{I_2}\right| \leq \frac{1}{10}$, we have that

$$|I| = |I_1 + I_2 + I_3| = |I_2| \left|1 + \frac{I_1}{I_2} + \frac{I_3}{I_2}\right| \geq |I_2| \left(1 - \frac{1}{10} - \frac{1}{10}\right) \neq 0.$$

Therefore, we have proved that $I \neq 0$, and since I is an integer, it holds that $|I| \geq 1$.

By (17) and the inequality $a^q \geq \frac{q^p}{2}$, we have

$$\begin{aligned} |I_2| &= \left|a^{Rq-p} q^{R+\rho} t_{R+1}\right| = \frac{q^{R+\rho}}{a^q} \left|a^{(R+1)q-p} t_{R+1}\right| \leq \frac{q^{R+\rho}}{4a^q} \\ &\leq \frac{q^{R+\rho}}{2q^p} = \frac{q^{R+\rho-p}}{2}. \end{aligned}$$

Now

$$1 \leq |I| = |I_2| \left|1 + \frac{I_1}{I_2} + \frac{I_3}{I_2}\right| \leq \frac{q^{R+\rho-p}}{2} \left(1 + \frac{1}{10} + \frac{1}{10}\right) = \frac{3}{5} q^{R+\rho-p} < q^{R+\rho-p}.$$

Therefore, $R + \rho - p > 0$. Now if we write $p = uq + v$, where integers u, v are such that and $0 < v < q$ and $u \geq 1$, we obtain

$$\begin{aligned} R + \rho &= \left\lfloor \frac{p}{q} \right\rfloor + 1 + \left\lfloor \frac{\left\lfloor \frac{p}{q} \right\rfloor + 1}{q-1} \right\rfloor = u + 1 + \left\lfloor \frac{u+1}{q-1} \right\rfloor \\ &\leq u + 1 + \left\lfloor \frac{u+1}{2} \right\rfloor \leq u + 1 + (u+1) = 2u + 2 \\ &\leq 3u + 1 \leq qu + v = p, \end{aligned}$$

so $R + \rho - p \leq 0$, which is a contradiction. Therefore we have proved that $p \mid y$. $\square$

6 A Consequence of Cassels' theorem

We use Cassels' theorem to prove the following lemma which is from [1].

Lemma 6.1. If p, q are distinct odd primes and $x, y \geq 1$ are integers such that $x^p - y^q = 1$, then exists integers a, b, u, v such that

$$\begin{cases} x - 1 = p^{q-1}a^q \\ \dfrac{x^p - 1}{x - 1} = pu^q \end{cases}$$

where $p \nmid u$, $gcd\,(a, u) = 1$, $y = pau$, and

$$\begin{cases} y + 1 = q^{p-1}b^p \\ \dfrac{y^q + 1}{y + 1} = qv^p \end{cases}$$

where $q \nmid v$, $gcd\,(b, v) = 1$, $x = qbv$.

Proof. By Theorem 5.6 we have $p \mid y$ and $q \mid x$. Since $x^p - y^q = 1$ and $y^q - x^p = -1$, the claim follows from Lemma 3.2. □

Next we study the properties of the integers a, b, u, v and x, y of Lemma 6.1 with the aim of showing that such such integers cannot exist. It's clear that if $x^p - y^q = 1$ then $x < y$ if and only if $q < p$.

Theorem 6.2. Let p, q, x, y, a, b, u, v be as in Lemma 6.1. Then u is odd.

Proof. Suppose u is even. Since $gcd\,(a, u) = 1$ it follows that a is odd, hence $x - 1 = p^{q-1}a^q$ is odd whereby x is even. But

$$y^q = \frac{x^p - 1}{x - 1}(x - 1) = pu^q(x - 1)$$

which means y is even. This is a contradiction since x and y cannot have the same parity. □

Theorem 6.3. Let p, q, x, y, a, b, u, v be as in Lemma 6.1. Then u has at least 1 prime factor which is ≥ 7. If all prime factors of u are ≤ 7 then $p = 3$.

Proof. By Theorem 6.2 u is odd, and necessarily $u > 1$ because in the case of $u = 1$ we have the inequality

$$1 + x + \cdots + x^{p-1} = u^q p = p < p^{q-1}a^q = x - 1,$$

which is impossible. Let $u = {p_1}^{s_1} \ldots {p_r}^{s_r}$ be the canonical factorization of u. Then it follows from $x^p - y^q = 1$ that for each prime p_i, $i = 1, \ldots, r$, we have the congruence $x^p \equiv 1 \pmod{p_i}$. However, since $x - 1 = p^{q-1}a^q$ and $gcd\,(ap, u) = 1$, we must have $x \not\equiv 1 \pmod{p_i}$, which means $\mathrm{ord}_{p_i}(x) = p$, so that $p \mid p_i - 1$ and consequently $p_i - 1 = 2kp$ for some integer k as both p_i and p are odd. So now $2p < p_i$. Let us denote $\sum_{k=1}^{r} s_i = c$. Then $(2p)^c < {p_1}^{s_1} \ldots {p_r}^{s_r} = u$, so we have that

$$p < \frac{u^{1/c}}{2}. \tag{23}$$

The inequality

$$\frac{u^{1/c}}{2} \leq 5$$

is equivalent to $u \leq 10^c$, meaning that if each prime factor p' of u satisfies $p' \leq 10$ then $p < \frac{u^{1/c}}{2} \leq 5$ in which case $p = 3$. Similarly the forbidden inequality $p < \frac{u^{1/c}}{2} \leq 3$ holds whenever $u \leq 6^c$, thus u must have at least one prime factor $p' > 6$. □

Theorem 6.4. Let p, q, x, y, a, b, u, v be as in Lemma 6.1. If x is even then $4 \mid x$. If x is odd then $4 \mid y$.

Proof. Let x be even. Then $y^q = x^p - 1 \equiv 3 \pmod 4$, so that $y \equiv 3 \pmod 4$. From $y + 1 = q^{p-1}b^p$, we have $0 \equiv q^{p-1}b^p$, hence $4 \mid b$ as q is odd. Now $4 \mid qbv = x$.

If $x = qbv$ is odd then b is odd, hence $y + 1 = q^{p-1}b^p \equiv 1 \pmod 4$, so that $y \equiv 0 \pmod 4$. □

Theorem 6.5. Let p, q, x, y, a, b, u, v be as in Lemma 6.1. Then $a > 1$.

Proof. Suppose $a = 1$. Now $x - 1 = p^{q-1}a^q = p^{q-1}$, hence

$$x - 2 = p^{q-1} - 1 = (p^{\frac{q-1}{2}} - 1)(p^{\frac{q-1}{2}} + 1) \equiv 0 \pmod 4,$$

which means $2 \mid x$ and $4 \nmid x$. But, by Theorem 6.4, $4 \mid x$, which is a contradiction. □

Theorem 6.6. Let p, q, x, y, a, b, u, v be as in Lemma 6.1. If $x < y$ then $2x < u$.

Proof. Since $x < y$ we have $q < p$. By Theorem 6.2 u is odd, hence $u \neq 2x$. Suppose $u < 2x$. Then $pau = y < 2pax$, so we have that

$$\begin{aligned} y^q &< (2pax)^q \\ -1 &< (2pax)^q - x^p \\ 0 &\leq (2pax)^q - x^p. \end{aligned}$$

If $0 = (2pax)^q - x^p$ then $p \mid x$, which is false since $x \equiv 1 \pmod p$. Thus $x^p < (2pax)^q$, which implies

$$\begin{aligned} (2pa)^q > x^{p-q} \geq x^2 = (p^{q-1}a^q + 1)^2 > p^{2(q-1)}a^{2q} = p^{2q-2}a^{2q} \\ 2pa > p^{2-\frac{2}{q}}a^2 \\ 2 > p^{1-\frac{2}{q}}a > a \end{aligned}$$

so $a = 1$, which is a contradiction since by Theorem 6.5 $a > 1$. □

Theorem 6.7. Let p, q, x, y, a, b, u, v be as in Lemma 6.1. Then $pa < |x - y|$.

Proof. Suppose $y < x$. Now

$$|x - y| = x - y = p^{q-1}a^q + 1 - pau = pa(p^{q-2}a^{q-1} - u) + 1 > pa$$

since $p^{q-2}a^{q-1} - u = 0$ would imply $p \mid u$, which is a contradiction.

Suppose next that $x < y$. By Theorem 6.6 $x < 2x < u$, so that

$$|x - y| = y - x > y - u = u(ap - 1) > ap$$

whenever $u > \frac{ap}{ap-1} = 1 + \frac{1}{ap-1}$ which is true since $u > 2$ by Theorem 6.3. □

Theorem 6.8. Let p, q, x, y, a, b, u, v be as in Lemma 6.1. Then $ap < u$.

Proof. Suppose $u \leq ap$, hence $u^q \leq (ap)^q = p(x-1) < px$, which implies

$$u^q p = 1 + x + \cdots + x^{p-1} < p^2 x < x^2,$$

since $x-1 = p^{q-1}a^q$, and, therefore, $p^2 < x$. Hence $p-1 \leq 1$, which is impossible. □

A property of relatively prime positive integers, x and y satisfy $|x-y| < x$ or $|x-y| < y$. The next theorem considers the case of $|x-y| < x$.

Theorem 6.9. Let p, q, x, y, a, b, u, v be as in Lemma 6.1. Then $|x-y| < x$ if and only if $y < x$.

Proof. Let us suppose $|x-y| < x$. Thus $(x-y)^2 = x^2 - 2xy + y^2 < x^2$, which implies $y < 2x$. If $x < y$ then by Theorem 6.6 $x < u$, so that $pau = y < 2x < 2u$, which is impossible, hence $y < x$.

Next let us suppose $y < x$. If $x < |x-y|$ then both x and y are smaller than $|x-y|$, which is impossible, so we must have $|x-y| < x$. □

Theorem 6.10. One of the following conditions is true for x and y as in Lemma 6.1:

$$y < |x-y| < x \tag{24}$$

$$|x-y| < y < x \tag{25}$$

$$x < |x-y| < y \tag{26}$$

Proof. Inequalities (24) and (25) are the two possibilities of Theorem 6.9 and the equation (26) is the only option in the case of $x < y$. □

Theorem 6.11. Let $|x-y| < y < x$. Then $u^8 < r^r$ where r is the largest prime divisor of u.

Proof. Let $|x-y| < y < x$. Thus $p < q$ and $(x-y)^2 < y^2$, whereby $x < 2y$. Now $1 = x^p - y^q < 2^p y^p - y^q$, hence $2^p y^p > y^q$. By Theorem 6.5 $a > 1$, so we now have $2^p > y^{q-p} \geq y^2 = (pau)^2 > (pa(2p)^c)^2 > 2^{4c+4}$ where c is as indicated in Theorem 6.3. Then

$$p > 4(c+1). \tag{27}$$

Consequently $4c < p < \frac{u^{1/c}}{2}$ by (23), so $(8c)^c < u \leq r^c$, hence

$$c < \frac{r}{8}, \tag{28}$$

which implies $u \leq r^c < r^{\frac{r}{8}}$. □

7 Theorem of Inkeri

7.1 The p-th cyclotomic field

Next are some facts about cyclotomic fields relevant to the Theorem of Inkeri. Most of these facts are from [1].

Let $\mathbb{C}$ be the field of complex numbers, and let $i \in \mathbb{C}$ be the imaginary unit with $i^2 = -1$. Let p be an odd prime and let

$$\xi = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p},$$

so ξ is a point on the unit circle on the complex plane. By Euler's formula, we have that

$$\xi = e^{\frac{2\pi i}{p}},$$

and, therefore, for a real number k,

$$\xi^k = e^{\frac{2\pi ik}{p}} = \cos\frac{2\pi k}{p} + i\sin\frac{2\pi k}{p}$$

It follows that $\xi^k = 1$ if and only if k is an integer multiple of p. Hence $k = p$ is the smallest $k > 0$ such that $\xi^k = 1$, and, consequently, $1, \xi, \xi^2, \ldots, \xi^{p-1}$ are distinct, and they divide the unit circle into p equal parts. The complex number ξ is called the *p-th root of unity*, and its powers generate all p solutions to the equation $z^p = 1$, namely $z = 1, \xi, \ldots, \xi^{p-1}$. Its complex conjugate $\overline{\xi}$ satisfies

$$\overline{\xi} = \cos\frac{2\pi}{p} - i\sin\frac{2\pi}{p} = \xi^{-1},$$

since

$$\begin{aligned}\xi\overline{\xi} &= \left(\cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}\right)\left(\cos\frac{2\pi}{p} - i\sin\frac{2\pi}{p}\right)\\ &= \sin\left(\frac{2\pi}{p}\right)^2 + \cos\left(\frac{2\pi}{p}\right)^2\\ &= 1.\end{aligned}$$

The field $\mathbb{Q}(\xi)$, where ξ is adjoined to the field of rational numbers, is called the *p-th cyclotomic field*. Let

$$\Phi(x) = \frac{x^p - 1}{x - 1} = 1 + x + x^2 \cdots + x^{p-1}.$$

The polynomial $\Phi(x)$ is the *p-th cyclotomic polynomial*, and its zeros are $\xi, \xi^2 \ldots, \xi^{p-1}$, which are distinct as discussed before. It follows that the polynomial

$$f(x) = (x - \xi)(x - \xi^2)\cdots(x - \xi^{p-1})$$

divides $\Phi(x)$ in the polynomial ring $\mathbb{Q}(\xi)[x]$, and, since the the leading term of $f(x)$ is x^{p-1}, which is the same as the leading term of $\Phi(x)$, we have necessarily that

$$\Phi(x) = (x - \xi)(x - \xi^2)\cdots(x - \xi^{p-1}).$$

Furthermore, by substituting $x = y + 1$, and using the binomial theorem, we get that

$$\Phi(x) = \Phi(y+1) = \frac{(y+1)^p - 1}{y} = \frac{\sum_{i=0}^{p} \binom{p}{i} y^{p-i} - 1}{y} = \sum_{i=0}^{p-1} \binom{p}{i} y^{p-i-1},$$

hence

$$\Phi(y+1) = y^{p-1} + \binom{p}{1} y^{p-2} + \cdots + \binom{p}{p-2} y + p.$$

Let us show that $\Phi(x)$ is irreducible over the rational numbers by using the Eisenstein irreducibility criterion. As formulated in [2] on page 42, the Eisenstein criterion for the polynomial ring $\mathbb{Z}[x]$ states the following: If p is a prime number, and

$$f(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + x^n$$

is a polynomial in $\mathbb{Z}[x]$, such that p divides $a_0, a_1, \ldots, a_{n-1}$, and p^2 does not divide a_0, then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

In the case of $\Phi(y+1)$, since p is prime, it satisfies $p \mid \binom{p}{i}$ when $1 \leq i < p$, and $p^2 \nmid p$. Therefore, by Eisenstein's criterion, $\Phi(y+1)$ is irreducible over the rational numbers, which implies that $\Phi(x)$ is irreducible as well. Thus $\Phi(x)$ is the minimal polynomial of ξ over $\mathbb{Q}$, and the degree of the extension $\mathbb{Q}(\xi)/\mathbb{Q}$ is the degree of $\Phi(x)$, which is $p - 1$. Therefore, we have the following fact.

Theorem 7.1. The elements

$$1, \xi, \ldots, \xi^{p-2}$$

form a basis of $\mathbb{Q}(\xi)$ over $\mathbb{Q}$, so that

$$\mathbb{Q}(\xi) = \left\{ a_0 + a_1 \xi + \cdots + a_{p-2} \xi^{p-2} \,\middle|\, a_i \in \mathbb{Q} \right\}.$$

Definition 7.1. Let $\alpha \in \mathbb{Q}(\xi)$. The presentation of α as the linear combination of the elements $1, \xi, \ldots, \xi^{p-2}$ over the rationals,

$$\alpha = a_0 + a_1 \xi + \cdots + a_{p-2} \xi^{p-2},$$

is called the *canonical presentation* of α, and the coefficients, $a_i \in \mathbb{Q}$, are unique, by Theorem 7.1.

Definition 7.2. Let $\alpha \in \mathbb{Q}(\xi)$. If there exists an integer $n \geq 1$ and integers $a_0, \ldots, a_{n-1}$, such that

$$a_0 + a_1 \alpha + a_2 \alpha^2 + \cdots + a_{n-1} \alpha^{n-1} + \alpha^n = 0,$$

then α is called *an integer of* $\mathbb{Q}(\xi)$. This is equivalent to saying that there exists a monic polynomial $f(x)$ with integer coefficients, such that $f(\alpha) = 0$.

Example 7.2. The p-th root of unity ξ is an integer of $\mathbb{Q}(\xi)$, since the polynomial

$$\Phi(x) = 1 + x + \cdots + x^{p-1}$$

satisfies the equation

$$\Phi(\xi) = 1 + \xi + \cdots + \xi^{p-1} = 0.$$

Theorem 7.3. The set

$$\mathbb{Z}[\xi] = \left\{ a_0 + a_1\xi + \cdots + a_{n-1}\xi^{n-1} + a_n\xi^n \,\middle|\, n > 0, a_i \in \mathbb{Z} \right\}$$

is a subring of $\mathbb{Q}(\xi)$, and, moreover, the elements

$$1, \xi, \ldots, \xi^{p-2}$$

form a basis of $\mathbb{Z}[\xi]$ over $\mathbb{Z}$.

Proof. By the subring criterion, $\mathbb{Z}[\xi]$ is a subring of $\mathbb{Q}(\xi)$: indeed, $\mathbb{Z}[\xi]$ is closed under multiplication and subtraction, and contains the unit 1. Let $\alpha \in \mathbb{Z}[\xi]$. Then

$$\alpha = a_0 + a_1\xi + \cdots + a_{n-1}\xi^{n-1} + a_n\xi^n \tag{29}$$

where $n > 0$, and $a_0, \ldots, a_n \in \mathbb{Z}$. Since $\xi^p = 1$, and

$$\xi^{p-1} = -(1 + \xi + \cdots + \xi^{p-2}),$$

we get, from the equation (29), that

$$\alpha = b_0 + b_1\xi + \cdots + b_{p-2}\xi^{p-2},$$

where $b_0, \ldots, b_{p-2} \in \mathbb{Z}$. Thus, the elements

$$1, \xi, \ldots, \xi^{p-2} \tag{30}$$

generate the ring $\mathbb{Z}[\xi]$ over the integers. To form a basis, the elements (30) must also be linearly independent over the integers. By Theorem 7.1, we have that the elements (30) are linearly independent over $\mathbb{Q}$, hence (30) are linearly independent over $\mathbb{Z}$. Thus the elements (30) form a basis of $\mathbb{Z}[\xi]$ over $\mathbb{Z}$. □

Note, that when $p > 3$, $\mathbb{Z}[\xi]$ contains real numbers that are not integers. For example, let $k > 0$ be such that

$$2k \equiv 1 \pmod{p},$$

so that, since p is odd,

$$2k = (2n+1)p + 1$$

where $n \in \mathbb{Z}$. Since ξ^k and ξ^{-k} are in $\mathbb{Z}[\xi]$, and $\xi^{-k} = \overline{\xi^k}$, we have that the element

$$\xi^k + \xi^{-k} = 2\mathrm{Re}(\xi^k) = 2\cos\left(\frac{2\pi k}{p}\right)$$

is a real number in $\mathbb{Z}[\xi]$. And, since $2k\pi = ((2n+1)p+1)\pi$, we get that

$$\begin{aligned}
2\cos\left(\frac{2\pi k}{p}\right) &= 2\cos\left(\frac{((2n+1)p+1)\pi}{p}\right) \\
&= 2\cos\left(2np\pi + \pi + \frac{\pi}{p}\right) \\
&= 2\cos\left(\pi + \frac{\pi}{p}\right) \\
&= -2\cos\left(\frac{\pi}{p}\right),
\end{aligned}$$

Since $p > 2$, $\frac{\pi}{p}$ is in the first quarter of the unit circle, and, therefore,

$$0 < \cos\left(\frac{\pi}{p}\right) < 1,$$

hence

$$-2 < -2\cos\left(\frac{\pi}{p}\right) < 0.$$

From this, we get that, if $\xi^k + \xi^{-k}$ is an integer, then necessarily

$$\xi^k + \xi^{-k} = -2\cos\left(\frac{\pi}{p}\right) = -1,$$

so that

$$\cos\left(\frac{\pi}{p}\right) = \frac{1}{2},$$

but this false, since $\frac{\pi}{p}$ is not of the form $2\pi m \pm \frac{\pi}{3}$, where $m \in \mathbb{Z}$, because $p > 3$. Thus, $\xi^k + \xi^{-k}$ is not an integer.

Let us denote by A the set of integers of $\mathbb{Q}(\xi)$. We make the following definitions.

- If $\alpha \in A$ is such that $\alpha\beta = 1$ for some $\beta \in A$ then α is said to be a *unit of* A, or simply a *unit*.
- If $\alpha, \beta \in \mathbb{Q}(\xi)$ and there exists $\gamma \in A$ such that $\beta = \gamma\alpha$, it is said that α *divides* β, which is denoted by $\alpha \mid \beta$.
- If $\alpha, \beta \in \mathbb{Q}(\xi)$ and $\alpha \mid \beta$ and $\beta \mid \alpha$ then α and β are said to be *associate*, denoted by $\alpha \sim \beta$.

Theorem 7.4. Let $\alpha, \beta \in \mathbb{Q}(\xi)$. Then $\alpha \sim \beta$ if and only if $\alpha = \gamma\beta$, where $\gamma \in A$ is a unit.

Proof. Since $\alpha \sim \beta$, by definition there exists $\gamma, \gamma' \in A$, such that

$$\begin{aligned} \alpha &= \gamma\beta, \text{ and} \\ \beta &= \gamma'\alpha. \end{aligned}$$

Hence

$$\alpha = \gamma\beta = \gamma\gamma'\alpha,$$

from which we get that $1 = \gamma\gamma'$, and, therefore, γ is a unit of A. □

The purpose of the following set of results is to eventually establish that $A = \mathbb{Z}[\xi]$. The first theorem to that end shows that A does not contain non-integer rational numbers.

Theorem 7.5. $A \cap \mathbb{Q} = \mathbb{Z}$.

Proof. Since $\mathbb{Z} \subseteq A$, it suffices to show that the only rational numbers in A are the integers. Let $a, b \in \mathbb{Z}$ be such that $b \neq 0$ and $\frac{a}{b} \notin \mathbb{Z}$, so that we may assume that a and b are relatively prime. Suppose on the contrary that $\frac{a}{b} \in A$. Then there exists $n > 0$ such that

$$0 = a_0 + a_1\frac{a}{b} + \cdots + a_{n-1}\left(\frac{a}{b}\right)^{n-1} + \left(\frac{a}{b}\right)^n$$

for some integers $a_0, \ldots, a_{n-1}$. Multiplying the equation by b^{n-1}, we get that

$$0 = a_0 b^{n-1} + a_1 b^{n-2} a + \cdots + a_{n-1}a^{n-1} + \frac{a^n}{b},$$

hence $\frac{a^n}{b} \in \mathbb{Z}$, which is a contradiction, since it was assumed that $\frac{a}{b} \notin \mathbb{Z}$, and $gcd\,(a, b) = 1$. □

Lemma 7.6. Let $b \in \mathbb{Z}, b \neq 0$, and let

$$\alpha = a_0 + a_1\xi + \cdots + a_{p-2}\xi^{p-2} \in \mathbb{Z}[\xi],$$

where $a_0, \ldots, a_{p-2} \in \mathbb{Z}$. Then $b \mid \alpha$ in $\mathbb{Z}[\xi]$ if and only if $b \mid a_i$ for $i = 0, \ldots, p-2$.

Proof. If $b \mid a_i$ for $i = 0, \ldots, p-2$, then

$$\alpha = b\left(\frac{a_0}{b} + \frac{a_1}{b}\xi + \cdots + \frac{a_{p-2}}{b}\xi^{p-2}\right),$$

where $\frac{a_i}{b} \in \mathbb{Z}$ for $i = 0, \ldots, p-2$, hence

$$\frac{a_0}{b} + \frac{a_1}{b}\xi + \cdots + \frac{a_{p-2}}{b}\xi^{p-2} \in \mathbb{Z}[\xi],$$

so $b \mid \alpha$.

Let us now suppose that $b \mid \alpha$, meaning that there exists $\beta \in \mathbb{Z}[\xi]$, such that $\alpha = b\beta$. Then

$$\beta = c_0 + c_1\xi + \cdots + c_{p-2}\xi^{p-2},$$

for some $c_0, \ldots, c_{p-2} \in \mathbb{Z}$, and, therefore,

$$\alpha = b\beta = bc_0 + bc_1\xi + \cdots + bc_{p-2}\xi^{p-2}.$$

By theorem 7.1, this canonical presentation of α is unique, so the claim is true for α.

□

Let us make the following definitions for the purpose of upcoming theorems.

Definition 7.3. Commutative, non-zero ring R is called an *integral domain*, if $ab \neq 0$ for all non-zero $a, b \in R$.

Definition 7.4. Let $B \subseteq C$ be two rings. If $x \in C$, and

$$0 = b_0 + b_1 x \cdots + b_{n-1}x^{n-1} + x^n,$$

for some $n > 0$, and $b_0, \ldots, b_{n-1} \in B$, the element $x \in C$ is said to be *integral over* B. A subset $S \subseteq C$ is likewise said to be *integral over* B if every $x \in S$ is integral over B.

For example, A is by its construction integral over $\mathbb{Z}$. Let us recall the definition of a module.

Definition 7.5. Let R be a ring. An Abelian group $(M,+)$ is called an *R-module*, if it satisfies the following postulates.

RM0. $ax \in M$ for all $a \in R, x \in M$,

RM1. $a(x+y) = ax + ay$ for all $a \in R, x, y \in M$,

RM2. $(a+b)x = ax + bx$ for all $a, b \in R, x \in M$,

RM3. $(ab)x = a(bx)$ for all $a, b \in R, x \in M$,

RM4. $1x = x$ for all $x \in M$.

Definition 7.6. If M is an R-module, and a subset $N \subseteq M$ is also an R-module, then N is called a *submodule* of M.

Definition 7.7. An R-module M is called *finitely generated*, if for some $n \in \mathbb{N}$ and $m_1 \ldots, m_n \in M$, we have that

$$M = \{r_1 m_1 + \cdots + r_n m_n | \, r_i \in R\}.$$

The following provides submodule criteria.

Theorem 7.7. Let M be an R-module. Then a subset N of M is an M submodule if it satisfies the following conditions.

AM1. $N \neq \emptyset$,

AM2. if $x, y \in N$ then $x + y \in N$,

AM3. if $a \in R$ and $x \in N$, then $ax \in N$.

The next theorem, which is from [6], will be used, among other things, to prove that A is a ring.

Theorem 7.8. Let $B \subseteq C$ be two rings. Then $\alpha \in C$ is integral over B if and only if there exists a finitely generated, non-zero $B-$module $M \subseteq C$, such that $\alpha M \subseteq M$.

Proof. Suppose that $\alpha \in C$ is integral over B, so that

$$0 = u_0 + u_1\alpha + \cdots + \alpha^n,$$

where $n \geq 1$ and $u_i \in B$. Let

$$M = \left\{ b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} \middle| \, b_0, \ldots, b_{n-1} \in B \right\}.$$

Thus M is a finitely generated $B-$module, and for $\beta = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} \in M$, we have that

$$\begin{aligned}
\alpha\beta &= \alpha(b_0 + b_1\alpha + \cdots + b_{n-2}\alpha^{n-2} + b_{n-1}\alpha^{n-1}) \\
&= b_0\alpha + b_1\alpha^2 + \cdots + b_{n-2}\alpha^{n-1} + b_{n-1}\alpha^n \\
&= b_0\alpha + b_1\alpha^2 + \cdots + b_{n-2}\alpha^{n-1} + b_{n-1}(-(u_0 + u_1\alpha + \cdots + u_{n-1}\alpha^{n-1})) \\
&= -b_{n-1}u_0 + (b_0 - u_1)\alpha + (b_1 - u_2)\alpha^2 + \cdots + (b_{n-2} - u_{n-1})\alpha^{n-1},
\end{aligned}$$

so $\alpha\beta \in M$, hence $\alpha M \subseteq M$. Suppose next that $\alpha \in C$, and that there exists a finitely generated $B-$module

$$M = \{b_1x_1 + \cdots + b_nx_n | \, b_1, \ldots, b_n \in B\},$$

where $x_i \in C$ and $n \geq 1$, such that $\alpha M \subseteq M$. From the condition that $\alpha M \subseteq M$, it follows that $\alpha x_i \in M$ for $i = 1, \ldots, n$, and, therefore, αx_i is of the form

$$\alpha x_i = b_{i1}x_1 + \cdots + b_{in}x_n$$

where $b_{ij} \in B$. Thus, we get the equations

$$\begin{aligned}
\alpha x_1 &= b_{11}x_1 + b_{12}x_2 + \cdots + b_{1n}x_n \\
\alpha x_2 &= b_{21}x_1 + b_{22}x_2 + \cdots + b_{2n}x_n \\
&\vdots \\
\alpha x_n &= b_{n1}x_1 + b_{n2}x_2 + \cdots + b_{nn}x_n.
\end{aligned}$$

Hence

$$\begin{aligned}
0 &= (b_{11} - \alpha)x_1 + b_{12}x_2 + \cdots + b_{1n}x_n \\
0 &= b_{21}x_1 + (b_{22} - \alpha)x_2 + \cdots + b_{2n}x_n \\
&\vdots \\
0 &= b_{n1}x_1 + b_{n2}x_2 + \cdots + (b_{nn} - \alpha)x_n.
\end{aligned}$$

Considering $(x_1, \ldots x_n)$ as a solution to this homogeneous system of linear equations, it follows that the determinant of the coefficient matrix is 0:

$$\begin{vmatrix}
b_{11} - \alpha & b_{12} & \ldots & b_{1n} \\
b_{21} & b_{22} - \alpha & \ldots & b_{2n} \\
\vdots & & & \\
b_{n1} & b_{n2} & \ldots & b_{nn} - \alpha
\end{vmatrix} = 0.$$

When calculating the determinant, the coefficient of the leading term α^n is 1 (or -1, in which case the result can be multiplied by -1 to get 1 as the coefficient). This gives a non-zero monic polynomial over B whose zero is α, and so, α is integral over B.

□

Definition 7.8. Let $B \subseteq C$ be two rings. The set of all elements of C which are integral over B is called the *integral closure of B in C*.

Theorem 7.9. Let $B \subseteq C$ be two rings. The integral closure of B in C is a ring.

Proof. Denote the integral closure of B in C by R. Since $R \subseteq C$, we check that R satisfies the subring criteria. Since B is a subring of C, $1 \in B$, and 1 is the zero of the polynomial $X - 1$, so that $1 \in R$. Next, let us show that R is additively and multiplicatively closed. Let $x, y \in R$, hence we have the equations

$$\begin{aligned}
0 &= a_0 + a_1x + \cdots + x^n, \text{ and} \\
0 &= c_0 + c_1y + \cdots + y^m,
\end{aligned} \tag{31}$$

where $a_i, c_i \in B$ and $n, m \geq 1$. Let

$$M = \left\{ \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} b_{ij} x^i y^j \,\middle|\, b_{ij} \in B \right\},$$

so that M is a finitely generated B-module. From the equations (31), we get that

$$\begin{aligned} x^n &= -(a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}), \text{ and} \\ y^m &= -(b_0 + b_1 y + \cdots + b_{m-1} y^{m-1}), \end{aligned}$$

from which $xyM \subseteq M$ and $(x-y)M \subseteq M$, so that, by Theorem 7.8, $xy, x-y \in R$, so R is a ring. □

Theorem 7.10. *A is a ring.*

Proof. By Theorem 7.9 the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\xi)$ is a ring, which is A. □

From the fact that A is a ring, we have the following result.

Theorem 7.11. *$\mathbb{Z}[\xi] \subseteq A$.*

Proof. Theorem 7.10 states that A is a ring, and since $\xi^k \in A$ and $a \in A$ for all $k \in \mathbb{Z}$ and $a \in \mathbb{Z}$, it follows that all the linear combinations of $1, \xi, \ldots, \xi^{p-2}$ over the integers are contained in A. Since the elements $1, \xi, \ldots, \xi^{p-2}$ form a basis of $\mathbb{Z}[\xi]$ over the integers by Theorem 7.3, we get that $\mathbb{Z}[\xi] \subseteq A$. □

From the fact that A is a ring, we may consider the residue ring A/I for an ideal I of A. For $\alpha, \beta \in A$, let us denote

$$\alpha \equiv \beta, \text{ if and only if } \alpha - \beta \in I$$

so that the relation $\equiv$ is an equivalence relation, and we write

$$\alpha \equiv \beta \pmod{I}.$$

In some of the following theorems we consider $A/(\alpha)$, where $\alpha \in A$, and (α) denotes the principal ideal generated by α, that is

$$\alpha A = \{\alpha x | \, x \in A\}.$$

More about ideals later.

The next theorem and its proof are from [6], and it will be used for showing that the ring of integers A is contained in the ring $\mathbb{Z}[\xi]$.

Theorem 7.12. *When $k > 0$ is an integer such that $p \nmid k$, the mapping*

$$\sigma_k : \mathbb{Q}(\xi) \longrightarrow \mathbb{Q}(\xi),$$

with the rule

$$\sigma_k(a_0 + a_1\xi + a_2\xi^2 + \cdots + a_{p-2}\xi^{p-2}) = a_0 + a_1\xi^k + a_2(\xi^k)^2 + \cdots + a_{p-2}(\xi^k)^{p-2}$$

where $a_i \in \mathbb{Q}$, is a field homomorphism.

Proof. For σ_k to be a field homomorphism, it must be additive, multiplicative, and satisfy $\sigma_k(1) = 1$. The last condition is satisfied, so next, let us show that σ_k is additive. Let

$$\begin{aligned}\alpha &= a_0 + a_1\xi + \cdots + a_{p-2}\xi^{p-2} \in \mathbb{Q}(\xi), \text{ and}\\ \beta &= b_0 + b_1\xi + \cdots + b_{p-2}\xi^{p-2} \in \mathbb{Q}(\xi).\end{aligned}$$

Now

$$\alpha + \beta = (a_0 + b_0) + (a_1 + b_1)\xi + \cdots + (a_{p-2} + b_{p-2})\xi^{p-2},$$

hence

$$\begin{aligned}\sigma_k(\alpha + \beta) &= (a_0 + b_0) + (a_1 + b_1)\xi^k + \cdots + (a_{p-2} + b_{p-2})\xi^{k(p-2)}\\ &= (a_0 + a_1\xi^k + \cdots + a_{p-2}\xi^{k(p-2)}) + (b_0 + b_1\xi^k + \cdots + b_{p-2}\xi^{k(p-2)})\\ &= \sigma_k(\alpha) + \sigma_k(\beta).\end{aligned}$$

Let us show that σ_k is multiplicative. Let

$$\begin{aligned}f(x) &= a_0 + a_1x + \cdots + a_{p-2}x^{p-2}, \text{ and}\\ g(x) &= b_0 + b_1x + \cdots + b_{p-2}x^{p-2}\end{aligned}$$

be polynomials in $\mathbb{Q}[x]$, so that $f(\xi) = \alpha$ and $g(\xi) = \beta$, and, furthermore,

$$\begin{aligned}f(\xi^k) &= \sigma_k(\alpha), \text{ and}\\ g(\xi^k) &= \sigma_k(\beta).\end{aligned} \tag{32}$$

Dividing the polynomial $f(x)g(x)$ by the $p-$th cyclotomic polynomial $\Phi(x)$ in the polynomial ring $\mathbb{Q}[x]$, we get that

$$f(x)g(x) = h(x)\Phi(x) + r(x) \tag{33}$$

for some $h(x), r(x) \in \mathbb{Q}[x]$, such that $\deg r(x) < \deg \Phi(x) = p - 1$. So $r(x)$ is of the form

$$r(x) = c_0 + c_1x + \cdots + c_{p-2}x^{p-2}.$$

Then, since $\Phi(\xi) = 0$, we get from the equation (33), that

$$\alpha\beta = f(\xi)g(\xi) = h(\xi)\Phi(\xi) + r(\xi) = r(\xi) = c_0 + c_1\xi + \cdots + c_{p-2}\xi^{(p-2)}. \tag{34}$$

Since $\deg r(x) < p-1$, and $\Phi(\xi^k) = 0$ because $p \nmid k$, we get from the equations (34), (33), and (32), that

$$\begin{aligned}\sigma_k(\alpha\beta) &= \sigma_k(r(\xi))\\ &= r(\xi^k)\\ &= h(\xi^k)\Phi(\xi^k) + r(\xi^k)\\ &= f(\xi^k)g(\xi^k)\\ &= \sigma_k(\alpha)\sigma_k(\beta),\end{aligned}$$

so σ_k is multiplicative, and thus a homomorphism.

□

From the fact that σ_k is a homomorphism when $p \nmid k$, we get the following result.

Corollary 7.13. If $\alpha \in A$ and $p \nmid k$, then $\sigma_k(\alpha) \in A$.

Proof. Suppose $\alpha \in A$, so that

$$0 = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} + \alpha^n,$$

where $a_0, \ldots, a_{n-1} \in \mathbb{Z}$. By Theorem 7.12, the mapping σ_k is a homomorphism, and, therefore,

$$\begin{aligned} 0 &= \sigma_k(a_0 + a_1\alpha + \cdots + \alpha^n) \\ &= a_0 + a_1\sigma_k(\alpha) + \cdots + a_{n-1}\sigma_k(\alpha)^{n-1} + \sigma_k(\alpha)^n, \end{aligned}$$

hence $\sigma_k(\alpha) \in A$. □

Lemma 7.14. Let $\alpha = a_0 + a_1\xi + \cdots + a_{p-2}\xi^{p-2} \in \mathbb{Q}(\xi)$. Then

$$\sum_{k=1}^{p-1} \sigma_k(\alpha) = pa_0 - (a_0 + a_1 + \cdots + a_{p-2}).$$

Proof. For $k = 1, \ldots, p-1$, we have that

$$\Phi(\xi^k) = 1 + \xi^k + \xi^{2k} + \cdots + \xi^{(p-1)k} = 0,$$

and

$$\sigma_k(\alpha) = a_0 + a_1\xi^k + a_2\xi^{2k} + \cdots + a_{p-2}\xi^{(p-2)k},$$

hence

$$\begin{aligned} \sigma_1(\alpha) + \sigma_2(\alpha) + \cdots + \sigma_{p-1}(\alpha) &= \sum_{i=0}^{p-2} a_i\xi^i + \sum_{i=0}^{p-2} a_i\xi^{2i} + \cdots + \sum_{i=0}^{p-2} a_i\xi^{(p-1)i} \\ &= (p-1)a_0 + \sum_{i=1}^{p-2} a_i(\xi + \xi^2 + \cdots + \xi^{p-1}) \\ &= (p-1)a_0 + \sum_{i=1}^{p-2} a_i(-1) \\ &= pa_0 - (a_0 + a_1 + \cdots + a_{p-2}). \end{aligned}$$

□

We use the following notation. Let

$$\alpha = a_0 + a_1\xi + \cdots + a_{p-2}\xi^{p-2} \in \mathbb{Q}(\xi).$$

Let us denote

$$S(\alpha) = a_0 + a_1 + \cdots + a_{p-2}, \tag{35}$$

which is the sum of the coefficients, $a_i \in \mathbb{Q}$, in the canonical presentation of α, as defined in Definition 7.1.

Concerning the mapping σ_k of Theorem 7.12, we have, for any $k_1, k_2 > 0$ that may be multiples of p, that

$$\sigma_{k_1}(\sigma_{k_2}(\alpha)) = \sigma_{k_1 k_2}(\alpha).$$

And, if $k_1 \equiv k_2 \pmod{p}$, then

$$\sigma_{k_1}(\alpha) = \sigma_{k_2}(\alpha).$$

In the case that $p \mid k$, we have that $\sigma_k(\alpha) = \sigma_p(\alpha) = S(\alpha)$. Note, that σ_p is not a homomorphism. Indeed, σ_p is not multiplicative, since, for example, we have that

$$\sigma_p(\xi)\sigma_p(\xi^{p-2}) = S(\xi)S(\xi^{p-2}) = 1 \cdot 1 = 1,$$

but for the product

$$\xi \cdot \xi^{p-2} = \xi^{p-1} = -1 - \xi - \cdots - \xi^{p-2},$$

we have that

$$\begin{aligned}\sigma_p(\xi \cdot \xi^{p-2}) &= \sigma_p(-1 - \xi - \cdots - \xi^{p-2}) \\ &= S(-1 - \xi - \cdots - \xi^{p-2}) \\ &= -1 - \cdots - 1 \\ &= -(p-1) \neq 1.\end{aligned}$$

But σ_p is additive. Indeed, for any $\alpha, \beta \in \mathbb{Q}(\xi)$, we have that

$$\sigma_p(\alpha) + \sigma_p(\beta) = S(\alpha) + S(\beta) = S(\alpha + \beta) = \sigma_p(\alpha + \beta).$$

Lemma 7.15. Let $\alpha = a_0 + a_1\xi + \cdots + a_{p-2}\xi^{p-2} \in \mathbb{Z}[\xi]$, $n > 0$, and let $q > 2$ be a prime number, not necessarily different different from p, and let (q) be the principal ideal of $\mathbb{Z}[\xi]$ generated by q. Then

$$\alpha^{q^n} \equiv \sigma_{q^n}(\alpha) \pmod{(q)}.$$

Proof. Let us first show that $\alpha^q \equiv \sigma_q(\alpha) \pmod{(q)}$, by induction on $0 \leq k \leq p-2$ in

$$\alpha = a_0 + a_1\xi + \cdots + a_k\xi^k \in \mathbb{Z}[\xi].$$

Note, that if $a, b \in \mathbb{Z}$, and

$$a \equiv b \pmod{q}$$

in the ordinary integers, then also

$$a \equiv b \pmod{(q)}.$$

This is due to the fact that $q\mathbb{Z} \subseteq q\mathbb{Z}[\xi] = (q)$. For $k = 0$, $\alpha = a_0$ is an ordinary integer, so by Fermat's Little Theorem, we have that

$$\alpha^q = a_0^q \equiv a_0 = \sigma_q(\alpha) \pmod{q},$$

in the ordinary integers. By the earlier remark, the same congruence holds in $\mathbb{Z}[\xi]/(q)$, so we have that

$$\alpha^q \equiv \sigma_q(\alpha) \pmod{(q)}.$$

Next, suppose that $0 \leq k \leq p-3$, and that the element

$$\alpha = a_0 + a_1\xi + \cdots + a_k\xi^k \in \mathbb{Z}[\xi]$$

satisfies

$$\alpha^q \equiv \sigma_q(\alpha) \pmod{(q)}.$$

Now, by the binomial theorem, we have that

$$(\alpha + a_{k+1}\xi^{k+1})^q = \sum_{i=0}^{q} \binom{q}{i} \alpha^i (a_{k+1}\xi^{k+1})^{q-i}.$$

Since q is a prime, q divides $\binom{q}{i}$ for $i = 1, \ldots, q-1$. Recall that σ_q is additive even if $q = p$. By the induction hypothesis, and by Fermat's Little Theorem, we have that

$$\begin{aligned}
\sum_{i=0}^{q} \binom{q}{i} \alpha^i (a_{k+1}\xi^{k+1})^{q-i} &\equiv \alpha^q + (a_{k+1}\xi^{k+1})^q \pmod{(q)} \\
&\equiv \sigma_q(\alpha) + a_{k+1}\xi^{q(k+1)} \pmod{(q)} \\
&\equiv \sigma_q(\alpha) + \sigma_q(a_{k+1}\xi^{k+1}) \pmod{(q)} \\
&= \sigma_q(\alpha + a_{k+1}\xi^{k+1}) \pmod{(q)}.
\end{aligned}$$

Thus $\alpha^q \equiv \sigma_q(\alpha) \pmod{(q)}$ for every $\alpha \in \mathbb{Q}(\xi)$. Now, if we have for some $n > 0$ that

$$\alpha^{q^n} \equiv \sigma_{q^n}(\alpha) \pmod{(q)},$$

then

$$\alpha^{q^{n+1}} = (\alpha^{q^n})^q \equiv (\sigma_{q^n}(\alpha))^q \equiv \sigma_q(\sigma_{q^n}(\alpha)) = \sigma_{q^{n+1}}(\alpha) \pmod{(q)}.$$

□

Lemma 7.16. Let $\alpha \in \mathbb{Z}[\xi]$, and let q be a prime, and $n > 0$. If $q \mid \alpha^n$, then $q \mid \alpha$, or $q = p$.

Proof. Let

$$\alpha = a_0 + a_1\xi + \cdots + a_{p-2}\xi^{p-2} \in \mathbb{Z}[\xi],$$

and let $q \neq p$ be a prime, such that $q \mid \alpha^n$. Let us show that q divides α. By Fermat's Little Theorem, we have that $q^{n(p-1)} \equiv 1 \pmod{p}$. Since $q^{n(p-1)} - n > 0$, and $q \mid \alpha^n$, we have that

$$\alpha^{q^{n(p-1)}} = \alpha^n \alpha^{q^{n(p-1)}-n} \equiv 0 \pmod{(q)}.$$

Moreover, by Lemma 7.15, we have that

$$\alpha^{q^{n(p-1)}} \equiv \sigma_{q^{n(p-1)}}(\alpha) \equiv \alpha \pmod{(q)},$$

since $q^{n(p-1)} \equiv 1 \pmod{p}$. Thus $q \mid \alpha$. □

Lemma 7.17. Let

$$\alpha = a_0 + a_1\xi + \cdots + a_{p-2}\xi^{p-2} \in \mathbb{Q}(\xi),$$

and let $n > 0$. Let

$$S(\alpha) = a_0 + a_1 + \cdots + a_{p-2},$$

as defined in the equation 35. Then

$$S(\xi\alpha) = S(\alpha) - pa_{p-2},$$

and

$$\sum_{k=1}^{p-1} \sigma_k(\xi\alpha) = -S(\alpha).$$

Proof. Since

$$\xi^{p-1} = -(1 + \xi + \cdots + \xi^{p-2}),$$

we get that

$$\begin{aligned}
\xi\alpha &= \xi(a_0 + a_1\xi + \cdots + a_{p-2}\xi^{p-2}) \\
&= a_0\xi + a_1\xi^2 + \cdots + a_{p-3}\xi^{p-2} + a_{p-2}(-(1 + \xi + \cdots + \xi^{p-2})) \\
&= -a_{p-2} + (a_0 - a_{p-2})\xi + (a_1 - a_{p-2})\xi^2 + \cdots + (a_{p-3} - a_{p-2})\xi^{p-2}.
\end{aligned}$$

Hence

$$\begin{aligned}
S(\xi\alpha) &= -a_{p-2} + (a_0 - a_{p-2}) + (a_1 - a_{p-2}) + \cdots + (a_{p-3} - a_{p-2}) \\
&= a_0 + a_1 + \cdots + a_{p-3} + (p-1)(-a_{p-2}) \\
&= -pa_{p-2} + a_0 + a_1 + \cdots + a_{p-3} + a_{p-2} \\
&= -pa_{p-2} + S(\alpha).
\end{aligned}$$

Writing the statement of Lemma 7.14 in terms of S, we have that

$$\begin{aligned}
\sum_{k=1}^{p-1} \sigma_k(\xi\alpha) &= p(-a_{p-2}) - S(\xi\alpha) \\
&= p(-a_{p-2}) - (S(\alpha) - pa_{p-2}) \\
&= -S(\alpha).
\end{aligned}$$

□

Theorem 7.18. $A \subseteq \mathbb{Z}[\xi]$.

Proof. Suppose on the contrary that there exists $\alpha \in A$, such that $\alpha \in \mathbb{Q}(\xi) \setminus \mathbb{Z}[\xi]$, so that α is of the form

$$\alpha = \frac{a_0}{b_0} + \frac{a_1}{b_1}\xi + \cdots + \frac{a_{p-2}}{b_{p-2}}\xi^{p-2},$$

where a_i, b_i are relatively prime integers, and $b_i \neq 0$, and for some index i, we have that $\frac{a_i}{b_i} \notin \mathbb{Z}$. Thus, let q be a prime divisor of a b_i, that satisfies $\frac{a_i}{b_i} \notin \mathbb{Z}$. Let d be non-zero integer, such that

$$d\alpha = \beta + \frac{\gamma}{q},$$

where $\beta, \gamma \in \mathbb{Z}[\xi]$, and

$$\gamma = c_0 + c_1\xi + \cdots + c_{p-2}\xi^{p-2} \qquad\qquad , c_j \in \mathbb{Z}$$

where $c_j = 0$ or $q \nmid c_j$, with at least one c_j being non-zero. By Theorem 7.10, A is a ring, hence $d\alpha, \beta \in A$, and consequently, we have that $\gamma' = \frac{\gamma}{q} = d\alpha - \beta \in A$, where

$$\gamma' = \frac{c_0}{q} + \frac{c_1}{q}\xi + \cdots + \frac{c_{p-2}}{q}\xi^{p-2}.$$

Since A is a ring, $\gamma'\xi^{-k}$ is in A for every $k \in \mathbb{Z}$, so we may assume that the coefficient c_0 is non-zero, and thus not a multiple of q, by assumption. Since $\gamma' = \frac{\gamma}{q} \in A$, we have that

$$0 = m_0 + m_1\frac{\gamma}{q} + \cdots + m_{n-1}\left(\frac{\gamma}{q}\right)^{n-1} + \left(\frac{\gamma}{q}\right)^{n} \tag{36}$$

for some $n > 0$ and $m_0, \ldots, m_{n-1} \in \mathbb{Z}$. Multiplying the equation (36) by q^{n-1}, we get that

$$0 = m_0q^{n-1} + m_1q^{n-2}\gamma + \cdots + m_{n-1}\gamma^{n-1} + \frac{\gamma^n}{q}.$$

Hence $\frac{\gamma^n}{q} \in \mathbb{Z}[\xi]$, which means that $q \mid \gamma^n$. By Lemma 7.16, this implies that $q \mid \gamma$ or $q = p$. If $q \mid \gamma$, then, by Lemma 7.6, we have that $q \mid c_j$ for $j = 0, \ldots, p-2$, but this is false, since $q \nmid c_0$. Thus $q = p$, so that

$$\gamma' = \frac{c_0}{p} + \frac{c_1}{p}\xi + \cdots + \frac{c_{p-2}}{p}\xi^{p-2}.$$

By Lemma 7.17, we have that

$$\begin{aligned}\sum_{i=1}^{p-1}\sigma_i(\gamma') &= p\frac{c_0}{p} - (\frac{c_1}{p} + \cdots + \frac{c_{p-2}}{p}) \\ &= c_0 - (\frac{c_1}{p} + \cdots + \frac{c_{p-2}}{p}) \\ &= c_0 - \frac{c_1 + \cdots + c_{p-2}}{p}.\end{aligned} \tag{37}$$

By Corollary 7.13, the sum on the left-hand side of the equation (37), is in A, hence

$$\sum_{i=1}^{p-1}\sigma_i(\gamma') - c_0 = -\frac{c_1 + \cdots + c_{p-2}}{p} \in A.$$

Thus

$$\frac{c_1 + \cdots + c_{p-2}}{p} \in A \cap \mathbb{Q},$$

so that $\frac{c_1+\cdots+c_{p-2}}{p}$ is necessarily an integer, by Theorem 7.5, which means that

$$c_1 + \cdots + c_{p-2} \equiv 0 \pmod{p}. \tag{38}$$

Using the S notation as defined in the equation (35), we have that

$$S(\gamma) = c_0 + c_1 + \cdots + c_{p-2},$$

and, by the equation (38), we get that

$$S(\gamma) - c_0 \equiv 0 \pmod{p}. \tag{39}$$

On the other hand, we have, by Lemma 7.17, that

$$\begin{aligned}\sum_{i=1}^{p-1} \sigma_i(\xi\gamma') &= -S(\gamma') \\ &= -(\frac{c_0}{p} + \frac{c_1}{p} + \cdots + \frac{c_{p-2}}{p}) \\ &= -\frac{c_0 + c_1 + \cdots + c_{p-2}}{p},\end{aligned}$$

and this sum is, again, an element of A, by Corollary 7.13. As before, it follows from Theorem 7.5, that

$$\frac{c_0 + c_1 + \cdots + c_{p-2}}{p} \in \mathbb{Z},$$

hence

$$c_0 + c_1 + \cdots + c_{p-2} = S(\gamma) \equiv 0 \pmod{p}.$$

But, since $S(\gamma) \equiv c_0 \pmod{p}$ by the equation (39), we have, by the above congruence, that

$$0 \equiv S(\gamma) \equiv c_0 \pmod{p},$$

which is false, since it was assumed that $p \nmid c_0$.

□

Theorem 7.19. $A = \mathbb{Z}[\xi]$.

Proof. Theorem 7.18 states that $A \subseteq \mathbb{Z}[\xi]$, and Theorem 7.11 states that $A \subseteq \mathbb{Z}[\xi]$, hence $A = \mathbb{Z}[\xi]$. □

7.2 Ideals

Next are some definitions concerning ideals, and some of their properties.

- Subset I of $\mathbb{Q}(\xi)$ is said to be a *fractional ideal* if I has the following three properties.

  1. $\alpha - \beta \in I$ for every $\alpha, \beta \in I$
  2. $\alpha I \subseteq I$ for every $\alpha \in A$
  3. there exists a non-zero $\alpha \in A$, such that $\alpha I \subseteq A$.

- If I is a fractional ideal such that $I \subseteq A$, then I is said to be an *integral ideal*.
- If an integral ideal is proper subset of A, then I is said to be *proper ideal*.
- For fractional ideals I, J, let us define the multiplication between ideals,

$$IJ = \left\{ \sum_{i=1}^{n} a_i b_i \middle| \, n > 0, a_i \in I, b_i \in J \text{ for } i = 1, \ldots, n \right\}.$$

  Clearly $IJ = JI$, and IJ satisfies the conditions $1-3$, so that IJ is a fractional ideal. In the case that I and J are both integral ideals, then it follows from the definition that $IJ \subseteq I$, and $IJ \subseteq J$, hence $IJ \subseteq I \cap J$.
- For $\alpha \in \mathbb{Q}(\xi)$, denote $(\alpha) = \alpha A$, which clearly satisfies the conditions $1-3$, so that (α) is a fractional ideal, and it's called the *principal fractional ideal* generated by α. $(1) = A$ is called the *unit ideal*, since $AI = I$, and $(0) = \{0\}$ is the *zero ideal*.
- It it said that a fractional ideal I *divides* a fractional ideal J, if there exists an integral ideal L such that $J = LI$, which is denoted by $I \mid J$.
- A proper integral ideal I is said to be *maximal*, if I is not a proper subset of any integral ideal, other than A.

Example 7.20. Let $\mathbb{Z}$ be the ring of integers with the usual multiplication and addition. Then (2) is a maximal ideal of $\mathbb{Z}$. Indeed, if I is an ideal of $\mathbb{Z}$ such that the inclusion $(2) \subseteq I$ is proper, then I contains at least one odd integer, $2n+1 \in I$. Since $2n \in (2) \subseteq I$, it follows that $(2n+1) - 2n = 1 \in I$, hence $I = \mathbb{Z}$, so (2) is maximal.

Next are some properties of fractional ideals.

Theorem 7.21. If I, J are fractional ideals then $I \cap J$ is a fractional ideal.

Proof. If $\alpha \in I \cap J$ then $\alpha \in I$, $\alpha \in J$, and $-\alpha = (-1)\alpha$ where $-1 \in A$, so $-\alpha \in I$ and $-\alpha \in J$, so $-\alpha \in I \cap J$.

If $\alpha, \beta \in I \cap J$ then $\alpha + \beta \in I$ and $\alpha + \beta \in J$, so $\alpha + \beta \in I \cap J$.

Since I and J are fractional ideals, there exists $\gamma_1, \gamma_2 \in A$ such that $\alpha\gamma_1 \in A$ for all $\alpha \in I$ and $\beta\gamma_2 \in A$ for all $\beta \in J$. Then $\gamma_1\gamma_2\alpha \in A$ for all $\alpha \in I \cap J$, so $I \cap J$ is a fractional ideal. □

Theorem 7.22. If I and J are fractional ideals, then

$$I + J = \{\alpha + \beta | \, \alpha \in I, \beta \in J\}$$

is a fractional ideal.

Proof. Let us check that $I + J$ satisfies the fractional ideal postulates 1-3. Let $\alpha + \beta \in I + J$, where $\alpha \in I$ and $\beta \in J$, and let $\gamma \in A$. Then $\gamma\alpha \in I$ and $\gamma\beta \in J$, hence $\gamma(\alpha + \beta) = \gamma\alpha + \gamma\beta \in I + J$, so condition 2 holds.

Let

$$\alpha_1 + \beta_1 \in I + J, \text{ where } \alpha_1 \in I, \beta_1 \in J, \text{ and}$$
$$\alpha_2 + \beta_2 \in I + J, \text{ where } \alpha_2 \in I, \beta_2 \in J.$$

Then $\alpha_1 - \alpha_2 \in I$, and $\beta_1 - \beta_2 \in J$, so we have that

$$(\alpha_1 + \beta_1) - (\alpha_2 + \beta_2) = (\alpha_1 - \alpha_2) + (\beta_1 - \beta_2) \in I + J,$$

so condition 1 holds.

Since I and J are fractional ideals, there exists $\eta_1, \eta_2 \in A$, such that

$$\eta_1 I \subseteq A, \text{ and}$$
$$\eta_2 J \subseteq A.$$

Then, for $\alpha + \beta \in I + J$, where $\alpha \in I$ and $\beta \in J$, we have that

$$\eta_1\eta_2(\alpha + \beta) = \eta_2(\eta_1\alpha) + \eta_1(\eta_2\beta),$$

where $\eta_1\alpha \in A$ and $\eta_2\beta \in A$, hence $\eta_2(\eta_1\alpha) + \eta_1(\eta_2\beta) \in A$. Thus $\eta_1\eta_2(I + J) \subseteq A$, so condition 3 holds. So $I + J$ is a fractional ideal. □

Theorem 7.23. If M is a maximal ideal, then for an integral ideal I, such that $I \not\subseteq M$, we have that $M + I = A$.

Proof. By Theorem 7.22, we have that $M + I$ is an integral ideal. Since $I \setminus M$ is non-empty, the inclusion $M \subseteq M + I$ is proper, which means that $M + I$ is an ideal containing M, such that $M + I \neq M$. By the definition of maximality, this implies that $I + M = A$. □

The next result is one immediate consequence of Theorem 7.23.

Corollary 7.24. If M is a maximal ideal, and I is an integral ideal, such that $I \not\subseteq M$, then

$$\alpha + \beta = 1$$

for some $\alpha \in M$ and $\beta \in I$.

Proof. By Theorem 7.23, we have that $M + I = A$, hence $1 \in M + I$, which means that $\alpha + \beta = 1$ for some $\alpha \in M$ and $\beta \in I$. □

Next are some properties of principal fractional ideals.

Theorem 7.25. If $\alpha, \beta \in \mathbb{Q}(\xi) \setminus \{0\}$, then the following conditions hold.

1. $(\alpha\beta) = (\alpha)(\beta)$, and
2. $(\alpha) = (1)$ if and only if α is a unit of A, and
3. $(\alpha) = (\beta)$ if and only if $\alpha \sim \beta$.

Proof. Let us prove condition 1. By the definition of the principal ideal, we have that

$$(\alpha\beta) = \{x\alpha\beta |\, x \in A\},$$

and, by the definition of the product of ideals, we have that

$$\begin{aligned}(\alpha)(\beta) &= \left\{ \sum_{i=1}^{n} y_i\beta z_i\alpha \,\middle|\, n > 0, y_i, z_i \in A \right\} \\ &= \left\{ \sum_{i=1}^{n} x_i\alpha\beta \,\middle|\, n > 0, x_i \in A \right\} \\ &= \left\{ \alpha\beta \sum_{i=1}^{n} x_i \,\middle|\, n > 0, x_i \in A \right\} \\ &= \{\alpha\beta x |\, x \in A\} \\ &= (\alpha\beta).\end{aligned}$$

Let us prove condition 2. Let $(\alpha) = (1)$. Thus $\alpha \in A$, and $\alpha\gamma = 1$ for some $\gamma \in A$, so that α is a unit of A. Conversely, if α is a unit of A, then $\alpha\gamma = 1$ for some $\gamma \in A$, and, therefore, $\gamma\alpha = 1 \in (\alpha)$. Since $\alpha \in A$, we have that $(\alpha) \subseteq (1)$, and from the fact that $1 \in (\alpha)$, we get that $(1) \subseteq (\alpha)$, hence $(\alpha) = (1)$.

Let us prove condition 3. Let $(\alpha) = (\beta)$. Then $\alpha \in (\beta)$, and $\beta \in (\alpha)$, so that, for some $\gamma_1, \gamma_2 \in A$, we have that $\alpha = \beta\gamma_1$ and $\beta = \alpha\gamma_2$, hence $\alpha \mid \beta$ and $\beta \mid \alpha$, so that by Theorem 7.4, $\alpha \sim \beta$. Conversely, if $\alpha \sim \beta$, so that $\alpha = \eta\beta$ where $\eta \in A$ is a unit, then by conditions 1 and 2, we have that $(\alpha) = (\eta\beta) = (\eta)(\beta) = (\beta)$. □

We now define the concept of a prime ideal.

Definition 7.9. A proper, non-zero, integral ideal P is called a *prime ideal*, if the following condition holds for all $\alpha, \beta \in A$.

$$\text{If } \alpha\beta \in P, \text{ then } \alpha \in P \text{ or } \beta \in P.$$

Theorem 7.26. If M is a maximal integral ideal, then M is a prime ideal.

Proof. Suppose on the contrary that M is not prime, meaning that, for some α, β not in M, we have that $\alpha\beta \in M$. Thus (α) and (β) are not subsets of M, and, therefore, by Corollary 7.24, we have for some $\gamma_1, \gamma_2 \in A$ and $\eta_1, \eta_2 \in M$, that

$$\begin{aligned}\alpha\gamma_1 + \eta_1 &= 1, \text{ and} \\ \beta\gamma_2 + \eta_2 &= 1.\end{aligned}$$

Hence

$$\begin{aligned}1 &= (\alpha\gamma_1 + \eta_1)(\beta\gamma_2 + \eta_2) \\ &= \alpha\gamma_1\beta\gamma_2 + \alpha\gamma_1\eta_2 + \eta_1\beta\gamma_2 + \eta_1\eta_2 \in M.\end{aligned}$$

So $1 \in M$, meaning that $M = A$, which is a contradiction. Thus M is prime. □

Since $\mathbb{Q}(\xi)$ is a field, we may consider the residue ring $\mathbb{Q}(\xi)/I$ for fractional ideals I, with the equivalence relation

$$\alpha \equiv \beta \text{ if and only if } \alpha - \beta \in I$$

for $\alpha, \beta \in \mathbb{Q}(\xi)$, and we denote this by

$$\alpha \equiv \beta \pmod{I}.$$

Theorem 7.27. A non-zero, integral ideal P is prime, if and only if the residue ring A/P is an integral domain.

Proof. Let P be a prime ideal. Suppose that in the residue ring A/P, we have that

$$\alpha\beta \equiv 0 \pmod{P},$$

where $\alpha, \beta \in A$. Then, by the assumption that P is prime, we have that $\alpha \in P$, or $\beta \in P$, ie.

$$\alpha \equiv 0 \pmod{P}, \text{ or } \beta \equiv 0 \pmod{P},$$

in the residue ring, which is the definition of an integral domain.

Conversely, suppose that A/P is an integral domain, meaning that

$$\text{if } \alpha\beta \equiv 0 \pmod{P}, \text{ then } \alpha \equiv 0 \pmod{P}, \text{ or } \beta \equiv 0 \pmod{P}.$$

But, this is the same as saying that whenever $\alpha\beta \in P$, we have that $\alpha \in P$, or $\beta \in P$, which is the definition of a prime ideal. □

The next theorem is from [2].

Theorem 7.28. If I is a non-zero, integral ideal, then there exists a non-zero integer $k \in I \cap \mathbb{Z}$.

Proof. Let $I \neq (0)$ be an integral ideal and let $\alpha \in I \setminus \{0\}$. Since $I \subseteq A$, α is a root of some monic polynomial with integer coefficients

$$0 = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} + \alpha^n \tag{40}$$

where $n \geq 1$ and $b_0, \ldots b_{n-1} \in \mathbb{Z}$.

Suppose that $I \cap \mathbb{Z} = \{0\}$. By (40), $b_0 \in I$, so $b_0 = 0$. If $n = 1$ then $0 = b_0 + \alpha = \alpha$, which is a contradiction, so $n \geq 2$.

Suppose $b_k = 0$ for all $k = 0, \ldots, i$ where $0 \leq i \leq n-2$. Now

$$\begin{aligned} 0 &= b_{i+1}\alpha^{i+1} + \cdots + b_{n-1}\alpha^{n-1} + \alpha^n \\ &= \alpha^{i+1}(b_{i+1} + \cdots + b_{n-1}\alpha^{n-1-(i+1)} + \alpha^{n-(i+1)}). \end{aligned}$$

Since $\alpha \neq 0$ it follows that

$$0 = b_{i+1} + \cdots + b_{n-1}\alpha^{n-1-(i+1)} + \alpha^{n-(i+1)} \equiv b_{i+1} \pmod{I},$$

which implies $b_{i+1} = 0$. But then $b_1, \ldots, b_{n-1} = 0$, so $\alpha^n = 0$, which is a contradiction. □

Theorem 7.29. If I is an integral ideal then the residue ring A/I is finite.

Proof. By Theorem 7.28, there exists $k \in I \cap \mathbb{Z}$, $k \neq 0$. We may assume $k > 0$ since $-k \in I$. Thus $k\alpha \equiv 0 \pmod{I}$ for all $\alpha \in A$, so that in the sum

$$a_0 + a_1\xi + \cdots + a_{p-2}\xi^{p-2}, \qquad a_1, \ldots, a_{p-2} \in \mathbb{Z}$$

the coefficients satisfy $a_i \equiv 0, 1, \ldots, k-1 \pmod{I}$ for $i = 0, \ldots, p-2$, so the sum has at most k^{p-1} possible residues modulo I, and hence A/I is finite. □

Theorem 7.30. Let P be a proper, non-zero integral ideal. Then P is prime if and only if there exists $k > 0$, such that $\alpha^k - 1 \in P$ for all $\alpha \in A \setminus P$.

Proof. Let P be a prime ideal, and let $\alpha \in A \setminus P$. Then α is non-zero. By Theorem 7.29, the order of $A/P = d$ is finite, so that

$$\alpha^n \equiv \alpha^m \pmod{P}$$

for some $0 < n < m$. Hence

$$\alpha^n(\alpha^{m-n} - 1) \equiv 0 \pmod{P}.$$

P is prime, so $\alpha^n \notin P$, hence $\alpha^{m-n} - 1 \in P$. Thus the order of every non-zero element of A/P is finite. Let $n_1, \ldots, n_{d-1}$ be the orders of the $d-1$ different non-zero residues $\beta_1, \ldots, \beta_{d-1}$ of A modulo P. Let $k = n_1 \cdots n_{d-1}$. Then $\alpha \equiv \beta_i \pmod{P}$ for some i, and, therefore,

$$\alpha^k \equiv \beta_i^k \equiv (\beta_i^{n_i})^{kn_i^{-1}} \equiv 1 \pmod{P}.$$

Thus $\alpha^k - 1 \in P$.

Suppose that P is not prime, so that $\alpha\beta \in P$ for some $\alpha, \beta \in A \setminus P$. Suppose on the contrary, that $\alpha^k - 1, \beta^k - 1 \in P$ for some $k > 0$, hence

$$\begin{aligned} 0 &\equiv (\alpha^k - 1)(\beta^k - 1) \equiv -\alpha^k - \beta^k + 1 \pmod{P} \\ &\equiv -\alpha^k - (\beta^k - 1) \pmod{P} \\ &\equiv -\alpha^k \pmod{P}. \end{aligned}$$

Thus $\alpha^k \in P$, but, since it was assumed that $\alpha^k - 1 \in P$, we get that $1 \in P$, meaning that $P = (1)$, which is a contradiction. □

Theorem 7.31. Prime ideals are maximal.

Proof. Let P be a prime ideal. Suppose on the contrary, that there exists a proper integral ideal I, such that the inclusion $P \subseteq I$ is proper, so that there exists $\alpha \in I \setminus P$. By Theorem 7.30, we have that $\alpha^k - 1 \in P \subseteq I$ for some $k > 0$, which implies that $\alpha^k - (\alpha^k - 1) = 1 \in I$, hence $I = (1)$, which is a contradiction. □

Thus, we have the following characterization for prime ideals.

Theorem 7.32. Integral ideal I is maximal if and only if I is prime.

Proof. By Theorem 7.26, every maximal ideal is prime, and by Theorem 7.31, every prime ideal is maximal. □

7.3 Dedekind domain

In this section we define the concept of Dedekind domain, and show that the ring of integers of $\mathbb{Q}(\xi)$, which is denoted by A, is a Dedekind domain. This will be used to show that every integral ideal of A has a decomposition into prime ideals in a unique way. First, we will establish some preliminary notions. This section is based on [2] and [6].

Definition 7.10. Let D be an integral domain. The smallest field which contains D is called the *field of fractions* of D.

Theorem 7.33. The field of fractions of A is $\mathbb{Q}(\xi)$. Moreover, the elements in $\mathbb{Q}(\xi) \setminus A$ are of the form

$$\frac{\alpha}{d} \in \mathbb{Q}(\xi) \setminus A,$$

where $\alpha \in A$, and d is an integer that is relatively prime with α, meaning that, if a prime number $q \mid n$, then $\frac{\alpha}{q} \notin A$.

Proof. Let us denote by F the field of fractions of A, so that

$$F = \left\{ \frac{\alpha}{\beta} \middle| \, \alpha, \beta \in A, \beta \neq 0 \right\} \subseteq \mathbb{C}.$$

Let us show that $\mathbb{Q}(\xi) \subseteq F$. Let $\alpha \in \mathbb{Q}(\xi)$, so α is of the form

$$\alpha = \frac{a_0}{b_0} + \frac{a_1}{b_1}\xi + \cdots + \frac{a_{p-2}}{b_{p-2}}\xi^{p-2},$$

where $a_i, b_i \in \mathbb{Z}$, and $b_i \neq 0$. We may assume that a_i, b_i are relatively prime, and that $b_i = 1$ for indexes with $a_i = 0$. Let d be the least common multiple of $b_0, \ldots, b_{p-2}$. Thus $d \neq 0$, and we have that

$$\frac{a_i}{b_i} = \frac{1}{d} a_i (d b_i^{-1}),$$

where $db_i^{-1} \in \mathbb{Z}$. Let us denote

$$\alpha = \frac{\beta}{d}.$$

If q is a prime number, such that $q \mid d$, then $q \nmid \beta$. Indeed, let us suppose on the contrary, that $q \mid \beta$. Then, by Lemma 7.6, we have that

$$q \mid d b_i^{-1}$$

for every i, meaning that

$$d q^{-1} b_i^{-1} \in \mathbb{Z}$$

for every i. But then the integer dq^{-1} is a common multiple of the integers $b_0, \ldots, b_{p-2}$, which is false, since d was the least common multiple.

Since $\beta \in A$ and $d \in A$, we have that $\alpha = \frac{\beta}{d} \in F$, which shows that $\mathbb{Q}(\xi) \subseteq F$. Next, let us show that $F \subseteq \mathbb{Q}(\xi)$. Since $A \subseteq \mathbb{Q}(\xi)$, and $\mathbb{Q}(\xi)$ is a field, it follows that $\frac{\alpha}{\beta} \in \mathbb{Q}(\xi)$ for $\alpha, \beta \in A$, when $\beta \neq 0$, so that $F \subseteq \mathbb{Q}(\xi)$. Hence $F = \mathbb{Q}(\xi)$. □

Definition 7.11. An integral domain D is said to be *integrally closed* if every element of the field of fractions of D which is integral over D is in D.

For a ring R, denote by

$$R[X_1, \ldots, X_n]$$

the polynomial ring whose indeterminates are $X_1, \ldots, X_n$, and whose coefficients are in R. Thus, we have that

$$(R[X_1, \ldots, X_{n-1}])[X_n] = R[X_1, \ldots, X_n].$$

Theorem 7.34. Let $B \subseteq C$ be two rings, such that $x_1, \ldots, x_n \in C$ are integral over B. Then $B[x_1, \ldots, x_n]$ is a finitely generated B-module.

Proof. Let us proceed by induction on n. Let $x \in C$ be integral over B, so that

$$0 = b_0 + b_1 x + \cdots + x^m,$$

where $b_i \in B$, hence

$$x^m = -(b_0 + b_1 x + \cdots + b_{n-1} x^{m-1}),$$

from which we get that

$$B[x] = \left\{ y_0 + y_1 x + \cdots + y_{m-1} x^{m-1} \middle| \, y_i \in B \right\},$$

so $B[x]$ is a finitely generated B-module. Suppose that $n \geq 1$ and that $x_1, \ldots, x_n \in C$ are integral over B, and that $B[x_1, \ldots, x_n]$ is a finitely generated B-module. Let $z_1, \ldots, z_r \in B[x_1, \ldots, x_n]$ be the generators, so that

$$B[x_1, \ldots, x_n] = \{ y_1 z_1 + \cdots + y_r z_r | \, y_i \in B \}.$$

Let $x \in C$ be integral over B, so that, as before, we have that

$$B[x] = \left\{ y_0 + y_1 x + \cdots + y_{m-1} x^{m-1} \middle| \, y_i \in B \right\}.$$

Then

$$\begin{aligned} B[x_1, \ldots, x_n, x] &= (B[x_1, \ldots, x_n])[x] \\ &= \left\{ S_0 + S_1 x + \cdots + S_{m-1} x^{m-1} \middle| \, S_i = y_{i1} z_1 + \cdots + y_{ir} z_r, \text{ where } y_{ij} \in B \right\} \\ &= \left\{ \sum_{i=0}^{m-1} \sum_{j=1}^{r} u_{ij} x^i z_j \middle| \, u_{ij} \in B \right\} \end{aligned}$$

which is a B-module, generated by the elements $x^i z_j \in B[x_1, \ldots, x_n, x]$, where $0 \leq i \leq m-1$, and $1 \leq j \leq r$.

□

The following theorem is from [6].

Theorem 7.35. Let $B \subseteq C \subseteq D$ be three rings. If C is integral over B, and D is integral over C, then D is integral over B.

Proof. Let $x \in D$. Since D is integral over C, we have that

$$0 = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} + x^n,$$

where $c_i \in C$. Let

$$C_1 = B[c_0, \ldots, c_{n-1}].$$

Since $c_0, \ldots, c_{-1} \in C$ are integral over B, then, by Theorem 7.34, the ring C_1 is a finitely generated B-module. Since $c_0, \ldots, c_{n-1} \in C_1$, we have that x is integral over C_1, and, therefore, $C_1[x]$ is a finitely generated C_1-module, by Theorem 7.34 (by setting "B" $= C_1$, "C" $= D$). From the fact that C_1 is a finitely generated B-module, it follows that $C_1[x]$ is a finitely generated B-module. Moreover, $xC_1[x] \subseteq C_1[x]$, so that, by Theorem 7.8, x is integral over B. □

Theorem 7.36. *A is integrally closed.*

Proof. Since the field of fractions of A is $\mathbb{Q}(\xi)$ by Theorem 7.33, we need to show that if $\alpha \in \mathbb{Q}(\xi)$ is integral over A, then $\alpha \in A$. Let us denote by B the integral closure of A in $\mathbb{Q}(\xi)$. By Theorem 7.9, B is a ring, so that we have the inclusion

$$\mathbb{Z} \subseteq A \subseteq B,$$

for the three rings, and, therefore, by Theorem 7.35, we have that B is integral over $\mathbb{Z}$. But then $B \subseteq A$, since by definition A is the set of elements of $\mathbb{Q}(\xi)$ which are integral over the integers. Thus $B = A$, and A is integrally closed.

□

Next we define the concept of Noetherian domain, and present some facts about them.

Definition 7.12. An integral domain D is called a *Noetherian domain* if every chain of ideals of D,

$$I_1 \subseteq I_2 \subseteq \ldots,$$

terminates, meaning that for some $n > 0$, we have that $I_n = I_{n+i}$ for all $i \geq 0$.

Theorem 7.37. *$\mathbb{Z}$ is Noetherian.*

Proof. Let I be an ideal of $\mathbb{Z}$. Let us first show that $I = (m)$ for some $m \in \mathbb{Z}$. Let $m \geq 1$ be the smallest integer that divides every element of I, so that $I \subseteq (m)$, and let $nm \in I$ be the smallest positive multiple of m in I. Let $am \in I$, and let $gcd\,(a, n) = d$. Then there exists $x, y \in \mathbb{Z}$ such that $d = ax + ny$, hence $xam + ynm = m(ax + ny) = md \in I$. Hence $d = gcd\,(a, n) \geq n$, since nm was the smallest positive multiple of m in I. But then $n \mid a$. Hence mn divides every element of I, so that $n = 1$, since m was the smallest such integer. Then $m \in I$, and $(m) \subseteq I$, hence $I = (m)$. Let us show that $\mathbb{Z}$ is Noetherian. Let

$$(m_1) \subseteq (m_2) \subseteq \ldots$$

be a chain of ideals of $\mathbb{Z}$. Since $m_i \in (m_i) \subseteq (m_{i+1})$, there exists an integer n such that $m_i = nm_{i+1}$, hence $m_{i+1} \mid m_i$. Thus, if the inclusion $(m_i) \subseteq (m_{i+1})$ is proper, we have that $|m_{i+1}| < |m_i|$. Hence the sequence

$$|m_1|, |m_2|, \ldots$$

is decreasing, which means that it terminates, so that from some index $k > 0$ onwards, we have that $|m_k| = |m_{k+j}|$, hence $(m_k) = (m_{k+j})$ for all $j \geq 0$. Thus the chain $(m_1) \subseteq (m_2) \subseteq \ldots$ terminates, so $\mathbb{Z}$ is Noetherian. □

Definition 7.13. Let R be a ring. If M is an R-module, such that every chain of submodules of M,

$$N_1 \subseteq N_2 \subseteq \ldots,$$

terminates, then M is called a *Noetherian R-module*.

Lemma 7.38. Let R be a ring, and let $N \subseteq M$ be two R-modules, and in the quotient group M/N, let us define an R-action by

$$a(m + N) = am + N$$

for $a \in R, m \in M$. Then the following conditions hold.

1. M/N is a R-module.
2. If B is an M submodule, then the set

   $$I = \{m + N \in M/N | \, m \in B\}$$

   is an M/N submodule.
3. If I is an M/N submodule, then the set

   $$B = \{m \in M | \, m + N \in I\}$$

   is an M submodule.

Proof. Let us prove 1 by verifying the module postulates RM0-RM4 of the Definition 7.5 for M/N with the R-action $a(m + N) = rm + N \in M/N$ for $a \in R, m \in M$. Let $a, b \in R$ and $x + N, y + N \in M/N$. Then

$$a(x + N) = ax + N \in M/N,$$

so RM0 is satisfied. Since M is an R-module, we have that

$$a(x+N)+a(y+N) = (ax+N)+(ay+N) = (ax+ay)+N = a(x+y)+N = a((x+y)+N),$$

so RM1 is satisfied, and

$$(a + b)(x + N) = (a + b)x + N = (ax + bx) + N = (ax + N) + (bx + N),$$

so RM2 is satisfied, and

$$(ab)(x + N) = (ab)x + N = a(bx) + N = a(bx + N) = a(b(x + N)),$$

so RM3 is satisfied, and

$$1(x + N) = 1x + N = x + N,$$

so RM4 is satisfied. Thus M/N is an R-module.

Let us prove 2. Let B be an M submodule, and let $I = \{m + N \in M/N | \, m \in B\}$. Let us show that I is an M/N submodule by checking the submodule criterion AM1-AM3 of Theorem 7.7, which are

AM1. $I \neq \emptyset$, and

AM2. if $x, y \in I$ then $x + y \in I$, and

AM3. if $a \in R$ and $x \in I$, then $ax \in I$.

Since B is a submodule of M, $B \neq \emptyset$, hence $I \neq \emptyset$, so AM1 is satisfied. Let $x + N, y + N \in I$, where $x, y \in B$. Then $x + y \in B$, so that

$$(x + N) + (y + N) = (x + y) + N \in I,$$

so $AM2$ is satisfied. Let $a \in R$. Since B is an R-module, we have that $ax \in B$, hence

$$a(x + N) = ax + N \in I,$$

so $AM3$ is satisfied, hence I is an M/N submodule.

Let us prove 3. Let I be an M/N submodule, and let $B = \{m \in M | \, m + N \in I\}$. Let us show that B is an M submodule by using the submodule criterion of Theorem 7.7, which requires that

AM1. $B \neq \emptyset$, and

AM2. if $x, y \in B$ then $x + y \in B$, and

AM3. if $a \in R$ and $x \in B$, then $ax \in B$.

Since I is an M/N submodule, $I \neq \emptyset$, hence $B \neq \emptyset$, so AM1 is satisfied. If $x, y \in B$ then $x + N, y + N \in I$, so that, since I is a submodule of M/N, we have that

$$(x + N) + (y + N) = (x + y) + N \in I,$$

hence $x + y \in B$, so AM2 is satisfied. If $a \in R$, then, from the fact that I is an R-module, we have that

$$a(x + N) = ax + N \in I,$$

so that $ax \in B$, so AM3 is satisfied, thus B is an M submodule. □

Theorem 7.39. Let R be a ring, M an R-module, and $N \subseteq M$ an M-submodule. Then M is a Noetherian R-module if and only if both N and the quotient group M/N, with the R-action

$$a(m + N) = am + N \in M/N$$

for $a \in R, m \in M$, are Noetherian R-modules.

Proof. Let M be a Noetherian R-module, and let N be a submodule of M. Let

$$N_1 \subseteq N_2 \subseteq \ldots$$

be a chain of submodules of N. Then it is also a chain of submodules of M, so that the chain terminates, since M is Noetherian, hence N is Noetherian. Next, let us show that the quotient group M/N is Noetherian. Let

$$I_1 \subseteq I_2 \subseteq \ldots \tag{41}$$

be a chain of submodules of M/N. Let us define

$$B_i = \{m \in M | \, m + N \in I_i\}.$$

By Lemma 7.38, the sets B_i are M submodules. Since $I_i \subseteq I_{i+1}$, we have that $B_i \subseteq B_{i+1}$. Thus

$$B_1 \subseteq B_2 \subseteq \dots$$

is a chain of M submodules. Since M is Noetherian, the chain terminates, and, consequently, the chain (41) terminates, hence M/N is Noetherian.

Suppose that N and M/N are Noetherian R-modules. Let us show that M is a Noetherian R-module. Suppose on the contrary, that there exists a non-terminating chain of M submodules,

$$M_1 \subseteq M_2 \subseteq \dots.$$

Since the chain does not terminate, we may assume each inclusion is proper, and choose from each M_i an element m_i that is not a member of the preceding module. Let

$$I_i = \{m + N | \, m \in M_i\},$$

which is a submodule of M/N by Theorem 7.38, and $I_i \subseteq I_{i+1}$, since $M_i \subseteq M_{i+1}$. Since N is Noetherian, the chain

$$I_1 \subseteq I_2 \subseteq \dots$$

terminates, which means that from some index $n \geq 0$ forward, the residues of the sets M_i modulo N are identical. Thus, for the element $m_i \in M_i \setminus M_{i-1}$ in particular, when $i \geq n$, there exists $x \in M_{i-1}$, such that

$$m_i + N = x + N \in M/N,$$

hence $m_i - x \in N \cap M_i$. If $m_i - x \in M_{i-1}$, then $m_i \in M_{i-1}$, since x is in M_{i-1} which is an additive group, which contradicts the fact that $m_i \notin M_{i-1}$. Hence $m_i - x \notin M_{i-1}$, so that the inclusion $(N \cap M_{i-1}) \subseteq (N \cap M_i)$ is proper from index n onwards, and since the intersection of two modules is a module, we have a non-terminating chain of submodules of N,

$$(N \cap M_1) \subseteq (N \cap M_2) \subseteq \dots,$$

which is a contradiction. Thus M is Noetherian. □

Theorem 7.40. If R is a Noetherian ring, then any finitely generated R-module is Noetherian.

Proof. Let M be a finitely generated R-module, so that for some $n > 0$ and $m_1, \dots, m_n \in M$, we have that

$$M = \{r_1 m_1 + \dots + r_n m_n | \, r_i \in R\}.$$

Let $m = m_i$ be one of the generators of M, where $1 \leq i \leq n$, and let

$$N = \{rm | \, r \in R\}.$$

Let us show that N is a Noetherian M submodule. First, let us prove that N is an M submodule by the submodule criterion of Theorem 7.7, which requires that

AM1. $N \neq \emptyset$, and

AM2. if $x, y \in N$ then $x + y \in N$, and

AM3. if $a \in R$ and $x \in N$, then $ax \in N$.

Since $1m = m \in N$, N is non-empty. If $rm \in N$ and $r'm \in N$, then, since M is an R-module and $N \subseteq M$, we have that $rm + r'm = (r + r')m \in N$. If $r' \in R$, then for $rm \in N$, we have that $r'(rm) = (r'r)m \in N$, since M is an R-module and $N \subseteq M$. Thus N satisfies the submodule criterion, so that N is an M submodule. Let

$$N_1 \subseteq N_2 \subseteq \dots$$

be a chain of submodules of N. Since N is generated by $m \in M$, the elements of N_i are of the form rm, where $r \in R$. Let us define

$$I_i = \{r \in R | \, rm \in N_i\},$$

and let us show that I_i is an ideal of R. Let us show that I_i is an additive subgroup of R by the subgroup criterion. Since N_i is non-empty as a submodule of N, it follows that I_i is non-empty. Let $r_1, r_2 \in I_i$, so that $r_1 m, r_2 m \in N_i$. Then, since N_i is an R-module, we have that $-r_2 m \in N_i$, hence $r_1 m - r_2 m = (r_1 - r_2)m \in N_i$, which means that $r_1 - r_2 \in I_i$. Thus I_i is an additive subgroup of R. Let us show that I_i is closed under multiplication by R. Let $r \in I_i$, hence $rm \in N_i$, so that for any $a \in R$, we have that $a(rm) = (ar)m \in N_i$, since N_i is an R-module. Thus $ar \in I_i$, so we have that I_i is an ideal of R. Since R is Noetherian, the chain of ideals

$$I_1 \subseteq I_2 \subseteq \dots$$

terminates, hence the chain $N_1 \subseteq N_2 \subseteq \dots$ terminates. Thus N is Noetherian.

Let us proceed by induction on the number of generators of M. We already showed that if $n = 1$ then M is Noetherian. Suppose that for some $k \geq 1$

$$M_k = \{r_1 m_1 + \dots + r_k m_k | \, r_i \in R\}$$

is Noetherian. Let us show that

$$M_{k+1} = \{r_1 m_1 + \dots + r_k m_k + r_{k+1} m_{k+1} | \, r_i \in R\}$$

is Noetherian. Let $N = \{r m_{k+1} | \, r \in R\}$, so that N is a Noetherian submodule of M_{k+1}, since N is generated by a single element. Now we have that

$$\begin{aligned} M_{k+1}/N &= \{m + N | \, m \in M_{k+1}\} \\ &= \{m + N | \, m \in M_k\} \\ &= M_k/N. \end{aligned}$$

Since M_k is Noetherian, then, by Theorem 7.39, the quotient M_k/N is Noetherian, hence M_{k+1}/N is Noetherian. Since N is a Noetherian M_{k+1} submodule, we have, by Theorem 7.39, that M_{k+1} is Noetherian. □

Theorem 7.41. A is a Noetherian ring.

Proof. By Theorem 7.19, $A = \mathbb{Z}[\xi]$, and by Theorem 7.3, $\mathbb{Z}[\xi]$ is generated by the elements $1, \xi, \ldots, \xi^{p-2}$ over $\mathbb{Z}$, hence $\mathbb{Z}[\xi]$ is a finitely generated $\mathbb{Z}$-module. By Theorem 7.37, $\mathbb{Z}$ is a Noetherian ring, hence, by Theorem 7.40, $\mathbb{Z}[\xi]$ is Noetherian. □

Theorem 7.42. Let R be a ring, and let M be a Noetherian R-module. Then every M submodule is finitely generated.

Proof. Let $N \subseteq M$ be an M submodule. Suppose on the contrary that N is not finitely generated, so that for every $k > 0$ we have that, for any $x_1, \ldots x_k \in N$, the R-module

$$N_k = \{r_1 x_1 + \cdots + r_k x_k | \, r_i \in R\}$$

does not contain N, hence exists $x_{k+1} \in N$ such that $x_{k+1} \notin N_k$. Then the inclusion between the two M submodules

$$N_k \subseteq N_{k+1} = \{r_1 x_1 + \cdots + r_k x_k + r_{k+1} x_{k+1} | \, r \in R\}$$

is proper, hence the chain of M submodules

$$N_1 \subseteq N_2 \subseteq \ldots$$

does not terminate, which contradicts the Noetherian property of M. Thus N is finitely generated. □

The following lemma will be often used in the proofs concerning Noetherian rings, mainly A in our case.

Lemma 7.43. If R is a Noetherian ring, and Δ is any non-empty collection of ideals of R, then Δ contains a *maximal element*, meaning that there exists an ideal $M \in \Delta$, such that M is not a proper subset of any other ideal in Δ.

Proof. Suppose on the contrary, that Δ contains no maximal element. Let $I \in \Delta$. By assumption, I is not maximal, so that there exists $I' \in \Delta$, such that the inclusion $I \subseteq I'$ is proper. But then, we get, inductively, a non-terminating chain of ideals of Δ,

$$I \subseteq I' \subseteq I'' \subseteq \ldots,$$

which is a contradiction, since R is Noetherian. □

From Theorem 7.42 we get the following result.

Theorem 7.44. Every integral ideal is finitely generated as an A-module.

Proof. Since A is a Noetherian ring, and A is itself an A module, Theorem 7.42 states that every submodule of A is finitely generated. Integral ideals are A-modules, hence finitely generated. □

We define Dedekind domain in the following way.

Definition 7.14. *Dedekind domain* is an integral domain D that satisfies the following conditions.

- D is a Noetherian domain,
- D is integrally closed, and
- every prime ideal of D is maximal.

Theorem 7.45. A is a Dedekind domain.

Proof. By Theorem 7.41, A is Noetherian. By Theorem 7.36, A is integrally closed, and by Theorem 7.32, every prime ideal of A is maximal, hence A is a Dedekind domain. □

7.4 Ideal prime decomposition, and the ideal class group

In this section we will show that every integral ideal of A can be expressed as the product of prime ideals in a unique way. For this we need a few results. First, we have the following theorem, which is from [7].

Theorem 7.46. If P is a prime ideal and $I_1 \cdots I_n \subseteq P$ for integral ideals I_i, then $I_i \subseteq P$ for some i.

Proof. Suppose on the contrary that there exists $\alpha_i \in I_i \setminus P$ for $i = 1, \ldots, n$. Then $\alpha_1 \cdots \alpha_n \in I_1 \cdots I_n \subseteq P$, but none of the factors α_i are in P, which is a contradiction, since P is a prime ideal. Hence $I_i \subseteq P$ for some i. □

Theorem 7.47. If I is an integral ideal, then $I \subseteq P$ for some prime ideal P.

Proof. Let Δ be the set of all proper integral ideals that are not subsets of any prime ideals. Suppose on the contrary that Δ is non-empty. Then, by Theorem 7.43, Δ contains a maximal element, say $M \in \Delta$. The set Δ contains no prime ideals, so that M is not prime, hence M is not maximal in A, since A is a Dedekind domain, by Theorem 7.45. Then there exists an integral ideal M', such that the inclusion,

$$M \subseteq M',$$

is proper. Since M is a member of Δ, M is not a subset of a prime ideal, thus M' cannot be a subset of a prime ideal. Then, by the construction of Δ, we have that $M' \in \Delta$, which is a contradiction, since M is maximal in Δ.

□

The following lemma is from [7].

Lemma 7.48. Every non-zero integral ideal contains a product of prime ideals.

Proof. Let Δ be the set of non-zero, proper integral ideals that do not contain any products of prime ideals. Then, especially, Δ contains no prime ideals. Suppose on the contrary, that Δ is non-empty. By Theorem 7.43, Δ contains a maximal

element, say $M \in \Delta$. Since Δ contains no prime ideals, M is not prime, hence $xy \in M$ for some $x, y \in A \setminus M$. By Theorem 7.22, the sets

$$M + (x), \text{ and } M + (y)$$

are ideals, and, moreover, the inclusions

$$\begin{aligned} M &\subseteq M + (x), \text{ and} \\ M &\subseteq M + (y) \end{aligned}$$

are proper, hence neither ideal is in Δ, since M is maximal in Δ. By the construction of Δ, this means that for some prime ideals $P_1, \ldots, P_n, Q_1, \ldots, Q_k$, we have that

$$\begin{aligned} P_1 \cdots P_n &\subseteq M + (x), \text{ and} \\ Q_1 \cdots Q_k &\subseteq M + (y). \end{aligned}$$

Hence

$$P_1 \cdots P_n Q_1 \cdots Q_k \subseteq (M + (x))(M + (y)).$$

Let

$$\begin{aligned} m_1 + a_1 x &\in M + (x), \text{ and} \\ m_2 + a_2 y &\in M + (y). \end{aligned}$$

Since $xy \in M$, we get that

$$(m_1 + a_1 x)(m_2 + a_2 y) = m_1 m_2 + m_1 a_2 y + a_1 x m_2 + a_1 x a_2 y \in M,$$

Thus, all the finite sums of the elements of this form are in M, hence

$$(M + (x))(M + (y)) \subseteq M.$$

But then M contains the product of the prime ideals $P_1 \cdots P_n Q_1 \cdots Q_k$, which is a contradiction. Thus Δ is empty, so that every non-zero integral ideal contains a product of prime ideals. □

Lemma 7.49. Let I be a proper, non-zero integral ideal, and let $x \in \mathbb{Q}(\xi)$. If

$$xI \subseteq I,$$

then $x \in A$.

Proof. By Theorem 7.44, I is a finitely generated A-module, and, therefore, since $xI \subseteq I$ and $I \neq (0)$, we have by Theorem 7.8, that x is integral over A. By Theorem 7.45, A is a Dedekind domain, hence integrally closed, so $x \in A$. □

From the fact that A is a Dedekind domain, we get the following result, which is from [7].

Theorem 7.50. If P is a prime ideal of A, then

$$\overline{P} = \{x \in \mathbb{Q}(\xi) | \, xP \subseteq A\}$$

is a fractional ideal, such that $P\overline{P} = (1)$. Moreover, $\overline{P} \setminus A$ is non-empty.

Proof. Let $\overline{P}$ be as described. Let us show that $P\overline{P} = (1)$. First, let us check that $\overline{P}$ is a fractional ideal. Let $d \in P$ be a non-zero element of P, which exists, since P is prime, and by definition non-zero. Let $x \in \overline{P}$, so that $dx \in A$ by the definition of $\overline{P}$, hence $d\overline{P} \subseteq A$. Let $m \in P$, and $y \in \overline{P}$. Then $(x-y)m = xm - ym \in A$, since $xm, ym \in A$, hence $x - y \in \overline{P}$. For $a \in A$, we have that $axm \in A$, since $xm \in A$, hence $ax \in \overline{P}$. So $\overline{P}$ is a fractional ideal.

Since $\overline{P}$ is a fraction ideal, we have that the product $P\overline{P}$ is a fractional ideal, and by the definition of $\overline{P}$, we have that $P\overline{P} \subseteq A$, hence $P\overline{P}$ is an integral ideal. Since $1 \in \overline{P}$, we have that $P \subseteq P\overline{P} \subseteq A$ and $A \subseteq \overline{P}$. Since A is a Dedekind domain, its prime ideals are maximal, hence the inclusion of the integral ideals $P \subseteq P\overline{P} \subseteq A$, implies that $P\overline{P} = P$ or $P\overline{P} = A$. Suppose that $P\overline{P} = P$, and let us show that this is impossible.

Let $x \in \overline{P}$. From the assumption that $P = P\overline{P}$, we get that $xP \subseteq P$, which implies that $x \in A$, by Theorem 7.49. So we have that $\overline{P} \subseteq A$, hence

$$\overline{P} = A.$$

Let $a \in P$ be non-zero. By Theorem 7.48, (a) contains a non-empty product of prime ideals, so that

$$P_1 \cdots P_n \subseteq (a),$$

for some prime ideals $P_1, \ldots, P_n$, $n > 0$. Let us choose the smallest $n > 0$ for which such a product of primes is contained in (a). Since $a \in P$, we have that

$$P_1 \cdots P_n \subseteq (a) \subseteq P.$$

By Theorem 7.46, we have that $P_i \subseteq P$ for some $1 \leq i \leq n$. We may assume that $P_1 \subseteq P$, whereby $P_1 = P$, since P_1 is prime, and, therefore, maximal. Denote

$$B = P_2 \cdots P_n.$$

Since n was the least number of primes whose product is in (a), we have that $B \not\subseteq (a)$. In the case that $n = 1$, and $B = (1)$, then this is also true, since $(a) \subseteq P \neq A$. Hence, there exists $b \in B \setminus (a)$. Since

$$PB \subseteq (a),$$

we get that, in particular,

$$bP \subseteq (a),$$

hence, for every $p \in P$, there exists $az \in (a), z \in A$, such that $bp = az$, meaning that $bpa^{-1} = z \in A$. So, we have that

$$ba^{-1}P \subseteq A.$$

Then $ba^{-1} \in \overline{P}$, by the definition of $\overline{P}$. Since, by assumption, $\overline{P} = A$, we have that $ba^{-1} \in A$. Thus, there exists $z \in A$ such that $ba^{-1} = z$, meaning that $b = az \in (a)$, which is a contradiction, since b is not in (a). So, $\overline{P} \neq A$, and, therefore, $P \neq P\overline{P}$, so that $P\overline{P} = A$ is the only remaining option. □

The next Theorem is from [7].

Theorem 7.51. If I is a proper integral ideal, then

$$I = P_1 \cdots P_n$$

for some prime ideals $P_1, \ldots, P_n$. Furthermore, this representation of I as the product of prime ideals is unique.

Proof. Let Δ be the set of proper integral ideals that are not finite products of prime ideals. Suppose on the contrary, that Δ is non-empty. By Theorem 7.43, Δ contains a maximal element, say $M \in \Delta$. Let P be a prime ideal containing M, which exists by Theorem 7.47. Since M is not a prime ideal, we have that the inclusion

$$M \subseteq P$$

is proper, and, moreover, $P \notin \Delta$, since P is a product of itself. Let $\overline{P}$ be the inverse fractional ideal of P, which exists by Theorem 7.50. From the fact that $M \subseteq P$, we get that

$$M\overline{P} \subseteq P\overline{P} = A,$$

hence $M\overline{P}$ is an integral ideal. Since $1 \in \overline{P}$, we have that

$$M \subseteq M\overline{P}.$$

Let us show that the inclusion is proper. Suppose on the contrary, that

$$M = M\overline{P}.$$

Let $x \in \overline{P} \setminus A$, which exists by Theorem 7.47. Then we get from the assumption $M = M\overline{P}$, that $xM \subseteq M$, hence $x \in A$, by Theorem 7.49, which is a contradiction, since $x \notin A$. Hence the inclusion $M \subseteq M\overline{P}$ is proper. Since M is maximal in Δ, it follows that $M\overline{P} \notin \Delta$, so that, by the construction of Δ, we have that

$$M\overline{P} = P_1 \cdots P_n$$

for some prime ideals $P_1, \ldots, P_n$, $n > 0$. Multiplying by P, we get that

$$M = PP_1 \cdots P_n,$$

which is a contradiction. Hence Δ is empty, meaning that every proper integral ideal is the product of finitely many primes.

Let us show that this expression of an integral ideal as the product of prime ideals is unique. Let

$$I = P_1 \cdots P_n.$$

Suppose on the contrary, that I can be expressed in another way as the product of prime ideals,

$$QJ = P_1 \cdots P_n,$$

where $Q \neq P_i$ for every $i = 1, \ldots, n$. Hence

$$P_1 \cdots P_n = QJ \subseteq Q,$$

so that, by Theorem 7.46, we have that $P_i \subseteq Q$ for some i, which is a contradiction, since primes are maximal in A, due to the fact that A is Dedekind domain, by Theorem 7.45.

□

Theorem 7.52. Let I and J be integral ideals. Then $I \mid J$ if and only if $J \subseteq I$.

Proof. If $I \mid J$, then $J = II'$ for some integral ideal I', whereby $J = II' \subseteq I$.

Let $J \subseteq I$, and let

$$J = Q_1 \cdots Q_n$$

be the prime ideal decomposition of J. Let P be some prime factor of I. Then $I \subseteq P$, and, therefore,

$$J = Q_1 \cdots Q_r \subseteq I \subseteq P.$$

Then, by Theorem 7.46, we have for some i, that $Q_i \subseteq P$, hence $Q_i = P$, so that $P \mid J$. Thus every prime factor P of I divides J, which means that I divides J. □

Non-zero integral ideals I and J are said to be *relatively prime* if the only integral ideal dividing both I and J is the unit ideal $(1) = A$, which is denoted by $gcd\,(I, J) = 1$.

Theorem 7.53. Integral ideals I and J are relatively prime if and only if $\alpha + \beta = 1$ for some $\alpha \in I$ and $\beta \in J$.

Proof. Suppose that $\alpha + \beta = 1$ for some $\alpha \in I$ and $\beta \in J$. Let us show that I and J are relatively prime. Suppose on the contrary, that a prime ideal P divides both I and J. Then, by Theorem 7.52, we have that $I \subseteq P$ and $J \subseteq P$ in which case $\alpha + \beta = 1 \in P$, so $P = (1)$, which is a contradiction.

Suppose that I and J are relatively prime. Let us show that $1 \in I + J$. If I or J is the unit ideal (1), then the claim is true, so we may assume that both I and J are proper ideals. Let

$$J = Q_1 \cdots Q_r$$

be the prime ideal factorization of J. Since $Q_i \nmid I$, by Theorem 7.52, we have that $I \not\subseteq Q_i$, so $I \setminus Q_i \neq \emptyset$. So we may choose $\alpha_i \in I \setminus Q_i$ for each i. By Theorem 7.30, there exists, for every Q_i, an integer $k_i > 0$ such that $\alpha_i^{k_i} - 1 \in Q_i$. Let

$$\beta = \prod_{i=1}^{r} (\alpha_i^{k_i} - 1).$$

Then $\beta \in Q_1 \cdots Q_r = J$, and $\beta \equiv \pm 1 \pmod{I}$, so that $\beta \mp 1 \in I$, and, therefore, $\mp\beta + 1 \in I$. Now, we have that

$$\pm\beta + (\mp\beta + 1) = 1 \in J + I.$$

□

Theorem 7.54. If q is a prime number different from p then

$$(q) = Q_1 \cdots Q_n$$

where $Q_1, \ldots, Q_n$ are distinct prime ideals.

Proof. Let $q \neq p$. Suppose on the contrary, that

$$(q) = Q^2 I,$$

where Q is a prime ideal and I is an integral ideal. Then we have that

$$(q) \subseteq Q^2 \subseteq Q. \tag{42}$$

Recall the inverse fractional ideal of Q, as defined in Theorem 7.50,

$$\overline{Q} = \{x \in \mathbb{Q}(\xi) | \, xQ \subseteq A\},$$

which satisfies $Q\overline{Q} = A$, and, moreover, the set $\overline{Q} \setminus A$ is non-empty. Then we may choose $x \in \overline{Q} \setminus Q$. Since $x \in \mathbb{Q}(\xi) \setminus A$, we have, by Theorem 7.33, that x is of the form

$$x = \frac{\alpha}{n},$$

where $\alpha \in A$, and, moreover, $\frac{\alpha}{r} \notin A$ for any prime divisor r of n. Then, since $x \in \overline{Q}$, and $(q) \subseteq Q$, we get that,

$$x(q) \subseteq xQ \subseteq A,$$

so that, in particular, we have that

$$xq = \frac{\alpha q}{n} \in A.$$

So, $n \mid q\alpha$. Let

$$\alpha = a_0 + a_1\xi + \cdots + a_{p-2}\xi^{p-2}$$

be the canonical presentation of α. Since $n \nmid \alpha$, we have for some index i, by Lemma 7.6, that

$$\frac{a_i}{n} \notin \mathbb{Z}.$$

But, since $n \mid q\alpha$, we have, by Lemma 7.6, that

$$\frac{a_i q}{n} \in \mathbb{Z}.$$

Hence $q \mid n$, so that $n = mq$, and, therefore,

$$x = \frac{\alpha}{mq}.$$

Since q is factor of n, we have that $q \nmid \alpha$. Now, multiplying (42) by $\overline{Q}^2$, we get that

$$\overline{Q}^2(q) \subseteq A.$$

Thus, from the fact that $x \in \overline{Q}$, and $q \in (q)$, we get that

$$x^2 q = \left(\frac{\alpha}{mq}\right)^2 q = \frac{\alpha^2}{m^2 q} \in \overline{Q}^2(q) \subseteq A.$$

So, we have that $q \mid \alpha^2$. But, since $q \nmid \alpha$, we have necessarily, by Theorem 7.16, that $q = p$, which is a contradiction. □

The statement of Theorem 7.54 is equivalent to saying that, for any prime number q different from p, we have that

$$q \notin Q^2,$$

for every prime ideal Q. Indeed, $q \in Q^2$ is equivalent to $(q) \subseteq Q^2$, which is equivalent to $Q^2 \mid (q)$, by Theorem 7.52, and this was shown to be false in Theorem 7.54. The next theorem gives an equivalent definition for the prime ideal.

Theorem 7.55. Let P be a proper, non-zero integral ideal. Then P is prime if and only if the following condition holds for every integral ideal I.

$$\text{If } I \mid P, \text{ then } I = (1) \text{ or } I = P. \tag{43}$$

Proof. Suppose that P is prime, and that $P = IJ$ for some integral ideals I and J. Then I and J are non-zero. By Theorem 7.51, the prime ideal P cannot be expressed as the product of prime ideals in any other way, so that, from the equation $P = IJ$, we have exactly two possibilities for the prime ideal factorizations of I and J. Either

$$I = P, \text{ and } J = (1),$$

or

$$I = (1), \text{ and } J = P,$$

since, otherwise, P would have an alternate expression as the product of primes. Hence P satisfies the condition (43).

Suppose that P satisfies the condition (43). Let

$$P = Q_1 \cdots Q_n$$

be the prime ideal factorization of P, which exists by Theorem 7.51. Then $Q_i \mid P$, so by assumption $Q_i = (1)$ or $Q_i = P$. Since Q_i is a prime ideal, only $Q_i = P$ is permissible, in which case P is prime. □

Let us make a brief overview of the *class group*. The following facts are from [2].

Definition 7.15. It is said that fractional ideals I and J are *equivalent*, if

$$I = (\alpha)J$$

for some $\alpha \in \mathbb{Q}(\xi)$, which is denoted by $I \sim J$.

Theorem 7.56. The relation $\sim$ between non-zero fractional ideals is an equivalence relation.

Proof. Let I, J, and L be non-zero fractional ideals. Since $I = (1)I$, we have that $I \sim I$, so the relation $\sim$ is reflexive.

Let $I \sim J$, meaning that

$$I = (\alpha)J$$

for some non-zero $\alpha \in \mathbb{Q}(\xi)$. Then

$$J = (\alpha^{-1})I,$$

hence $J \sim I$, so the relation $\sim$ is reflexive.

If $I \sim J \sim L$, then $I = (\alpha)J$, and $J = (\beta)L$ for some non-zero $\alpha, \beta \in \mathbb{Q}(\xi)$, so we get that

$$I = (\alpha\beta)L,$$

hence $I \sim L$, so the relation $\sim$ is transitive, and an equivalence relation. □

We may now consider the resulting equivalence classes, denoted by $[I]$,

$$[I] = \{J |\, J \sim I\}.$$

Let us define a multiplication between equivalence classes, as

$$[I] \cdot [J] = [IJ].$$

Since the ordinary ideal multiplication is associate, so is the multiplication between equivalence classes. Moreover, if $I \sim I'$, and $J \sim J'$, so that $I = (\alpha)I'$ and $J = (\beta)J'$, then

$$IJ = (\alpha\beta)I'J',$$

hence $IJ \sim I'J'$. From this, we get that

$$[I][J] = [IJ] = [I'J'] = [I'][J'],$$

which shows that the multiplication is well-defined. For all non-zero $\alpha \in \mathbb{Q}(\xi)$, we get from the equation $(\alpha) = (\alpha)(1)$, that $(\alpha) \sim (1)$. Thus, for any I, we have that

$$I = (1)I \sim (\alpha)I,$$

and, therefore,

$$[I] = [(\alpha)I] = [(\alpha)][I],$$

Hence, the equivalence class $[(\alpha)] = [(1)]$ is the unit with respect to the multiplication. Let us show that each equivalence class has an inverse. Let I be a non-zero fractional ideal. By definition, there exists $\alpha \in A$ such that $(\alpha)I$ is an integral ideal. Let

$$(\alpha)I = P_1 \cdots P_n$$

be the prime ideal decomposition of $(a)I$, which exists by Theorem 7.51. By Theorem 7.50, there exists, for each P_i, an inverse fractional ideal $\overline{P_i}$, such that $P_i\overline{P_i} = (1)$. Hence

$$[I][(\alpha)\overline{P_1} \cdots \overline{P_n}] = [(\alpha)I\overline{P_1} \cdots \overline{P_n}] = [P_1 \cdots P_n\overline{P_1} \cdots \overline{P_n}] = [(1)],$$

so that $[(\alpha)\overline{P_1} \cdots \overline{P_n}]$ is the inverse of $[I]$. We have shown that the set of equivalence classes is a group.

Definition 7.16. The set of equivalence classes of non-zero fractional ideals, under the multiplication $[I][J] = [IJ]$, form a group, called the *(ideal) class group*, denoted by $C_l(\mathbb{Q}(\xi))$.

Let h_p denote the order of the ideal class group. The following Theorem is from [7], page 58.

Theorem 7.57. The order of the class group h_p is finite.

Since h_p is finite, so we have the following consequence.

Lemma 7.58. Let $k > 0$ be such that $gcd\,(k, h_p) = 1$. If I is a fractional ideal, such that

$$I^k = (\alpha),$$

where $\alpha \in \mathbb{Q}(\xi)$, then

$$I = (\beta\alpha^n)$$

for some $\beta \in \mathbb{Q}(\xi)$, and $n > 0$.

Proof. Since $gcd\,(k, h_p) = 1$, there exists $n > 0$ such that

$$kn = mh_p + 1,$$

where $m > 0$. Since $I^k = (\alpha)$, we have that $I^{kn} = (\alpha^n)$, hence

$$[(\alpha^n)] = [I^{kn}] = [I]^{kn} = [I]^{mh_p+1} = [I][I]^{mh_p} = [I].$$

Thus $I \sim (\alpha^n)$, so there exists $\beta \in \mathbb{Q}(\xi)$, such that

$$I = (\beta)(\alpha^n) = (\beta\alpha^n).$$

□

Let p be an odd prime and recall that ξ denotes the p-th root of unity.

Lemma 7.59. The elements

$$\frac{1-\xi^k}{1-\xi} = 1 + \xi + \cdots + \xi^{k-1}, \qquad \text{and} \qquad 1 + \xi^k$$

are units of A for $k = 1, \ldots, p-1$.

Proof. Let $1 \leq k \leq p-1$. Then $p \nmid k$, so there exists an integer $n > 0$ such that $nk = mp + 1$ for some m. Now

$$1 + \xi^k + (\xi^k)^2 + \cdots + (\xi^k)^{n-1} = \frac{1-\xi^{nk}}{1-\xi^k} = \frac{1-\xi^{mp+1}}{1-\xi^k} = \frac{1-\xi}{1-\xi^k} \in A,$$

hence $\frac{1-\xi^k}{1-\xi}$ is a unit of A. Let us show that $1 + \xi^k$ is a unit. Since p is odd, we have for the p-th cyclotomic polynomial Φ that

$$\begin{aligned}\Phi(\xi^k) = 0 &= 1 + \xi^k + (\xi^k)^2 + \cdots + (\xi^k)^{p-1} \\ &= (1+\xi^k)[1 + (\xi^k)^2 + (\xi^k)^4 + \cdots + (\xi^k)^{p-3}] + (\xi^k)^{p-1} \\ &= (1+\xi^k)\sum_{n=0}^{\frac{p-3}{2}}(\xi^k)^{2n} + (\xi^k)^{p-1}\end{aligned}$$

so that

$$\frac{1}{1+\xi^k} = -\xi^k \sum_{n=0}^{\frac{p-3}{2}}(\xi^k)^{2n} \in A,$$

hence $1 + \xi^k$ is a unit of A. □

Lemma 7.60. $1-\xi$ and $1-\xi^k$ are associate for $k=1,\ldots,p-1$.

Proof. In the equation

$$1-\xi^k=(1-\xi)\frac{1-\xi^k}{1-\xi}$$

the factor $\frac{1-\xi^k}{1-\xi}$ is a unit by Lemma 7.59, so $1-\xi$ and $1-\xi^k$ are associate for $k=1,\ldots,p-1$. □

Lemma 7.61. $(p)=(1-\xi)^{p-1}$

Proof. Since

$$\Phi(x)=1+x+\cdots+x^{p-1}=(x-\xi)\cdots(x-\xi^{p-1}),$$

we have, by setting $x=1$, the equality

$$p=\Phi(1)=(1-\xi)\cdots(1-\xi^{p-1}).$$

By Lemma 7.60 the factors are associate, so that there exist a unit $\alpha\in A$, such that $p=\alpha(1-\xi)^{p-1}$, and, therefore,

$$(p)=(\alpha(1-\xi)^{p-1})=(1-\xi)^{p-1}.$$

□

Lemma 7.62. $(1-\xi)$ is a prime ideal.

Proof. Let us first show that $(1-\xi)\neq(1)$. By Lemma 7.61, we have that

$$(p)=(1-\xi)^{p-1}.$$

By Theorem 7.5, we have that $\frac{1}{p}\notin A$, so p is not a unit, hence

$$(1)\neq(p)=(1-\xi)^{p-1},$$

from which we get that $(1-\xi)\neq(1)$.

Denote $I=(1-\xi)$, and let us show that I is prime. Let $\alpha,\beta\in A$, with

$$\begin{aligned}\alpha&=a_0+a_1\xi+\cdots+a_{p-2}\xi^{p-2},\text{ and}\\ \beta&=b_0+b_1\xi+\cdots+b_{p-2}\xi^{p-2}.\end{aligned}$$

Since $1-\xi\in I$, we have that

$$\xi\equiv 1\pmod I,$$

hence

$$\begin{aligned}\alpha&\equiv a_0+a_1+\cdots+a_{p-2}=a\pmod I,\text{ and}\\ \beta&\equiv b_0+b_1+\cdots+b_{p-2}=b\pmod I,\end{aligned}$$

where $a,b\in\mathbb{Z}$. Suppose that $\alpha\beta\in I$, and let us show that either α or β belongs in I. So, we have that

$$\alpha\beta\equiv ab\equiv 0\pmod I,$$

hence $ab \in I \cap \mathbb{Z}$. By Lemma 7.61, we have that $p \in I$. If $p \nmid ab$ in $\mathbb{Z}$, then there exists $x, y \in \mathbb{Z} \subseteq A$ such that

$$xp + yab = 1 \in I,$$

hence $I = (1)$, which is a contradiction. Thus, we have that $p \mid ab$ in $\mathbb{Z}$. Then $p \mid a$ or $p \mid b$ in $\mathbb{Z}$. We may assume that $a = dp$, and, since $p \in I$, we get that

$$\alpha \equiv a = dp \equiv 0 \pmod{I},$$

so $\alpha \in I$. Thus I is prime. □

The next theorem is by Kummer. A proof of the Theorem is in [8], page 3.

Theorem 7.63. Every unit of A is of form

$$\xi^k \eta$$

where $1 \leq k \leq p-1$ and $\eta \in A$ is a real unit, meaning the imaginary part of η equals 0.

Next we introduce the concept of a norm for an element of $\mathbb{Q}(\xi)$.

Definition 7.17. Let $\alpha \in \mathbb{Q}(\xi)$. Let σ_k be the homomorphism of Theorem 7.12, for $k = 1, \ldots, p-1$, and let us define the *norm* of α as

$$N(\alpha) = \prod_{k=1}^{p-1} \sigma_k(\alpha).$$

It turns out that the norm is always a rational number. For this, we need a few lemmas. The norm is also multiplicative:

Theorem 7.64. For $\alpha, \beta \in \mathbb{Q}(\xi)$, we have that $N(\alpha\beta) = N(\alpha)N(\beta)$.

Proof. The claim follows from the fact that σ_k is a homomorphism, and, therefore, $\sigma_k(\alpha)\sigma_k(\beta) = \sigma_k(\alpha\beta)$ for $k = 1, \ldots, p-1$. Thus

$$\begin{aligned} N(\alpha)N(\beta) &= \left(\prod_{k=1}^{p-1} \sigma_k(\alpha)\right)\left(\prod_{k=1}^{p-1} \sigma_k(\beta)\right) \\ &= \prod_{k=1}^{p-1} \sigma_k(\alpha)\sigma_k(\beta) \\ &= \prod_{k=1}^{p-1} \sigma_k(\alpha\beta) \\ &= N(\alpha\beta). \end{aligned}$$

□

Lemma 7.65. Let $\alpha \in \mathbb{Q}(\xi)$, $\alpha \notin \mathbb{Q}$. If $p \nmid j$, and $\sigma_{i+j}(\alpha) = \sigma_i(\alpha)$, then there exists an integer n, $n \not\equiv 1 \pmod{p}$, such that

$$\sigma_n(\alpha) = \alpha.$$

Proof. Let us first note that $\sigma_j(\alpha)$ is not in $\mathbb{Q}$. Since the rational coefficients $r_i \in \mathbb{Q}$ in the canonical presentation of α are unique,

$$\alpha = r_0 + r_1\xi + \cdots + r_{p-2}\xi^{p-2},$$

and by assumption $\alpha \notin \mathbb{Q}$, it follows that $r_s \neq 0$ for some $1 \leq s \leq p-2$. Thus

$$\sigma_j(\alpha) = r_0 + r_1\xi^j + r_2\xi^{2j} + \cdots + r_{p-2}\xi^{j(p-2)}$$

is not in $\mathbb{Q}$, since $r_s\xi^{js} \neq 0$.

If $p \mid i$, $i = dp$, then

$$\sigma_i(\alpha) = \sigma_{dp}(\alpha) = r_0 + \cdots + r_{p-2} \in \mathbb{Q},$$

which contradicts the fact that

$$\sigma_i(\alpha) = \sigma_{j+i}(\alpha) = \sigma_{j+dp}(\alpha) = \sigma_j(\alpha) \notin \mathbb{Q}$$

as noted in the beginning. Thus $p \nmid i$. So, there exists an integer l such that $li \equiv -j \pmod{p}$, and we have the congruence

$$l(i+j) \equiv li + lj \equiv -j + lj = j(l-1) \pmod{p}.$$

Taking σ_l of the equation $\sigma_{i+j}(\alpha) = \sigma_i(\alpha)$, we get that

$$\sigma_{j(l-1)}(\alpha) = \sigma_{j(-1)}(\alpha). \tag{44}$$

Let $hj \equiv -1 \pmod{p}$. Taking σ_h of the equation (44), we get that

$$\sigma_{1-l}(\alpha) = \alpha.$$

If $1 - l \equiv 1 \pmod{p}$, then $p \mid l$, but this is a contradiction, since $li \equiv -j \pmod{p}$, and by assumption $p \nmid j$. So, we may choose $n = 1 - l$.

□

Lemma 7.66. Let $\alpha \in \mathbb{Q}(\xi)$, $\alpha \notin \mathbb{Q}$. If $\sigma_i(\alpha) = \sigma_{i+j}(\alpha)$, $p \nmid j$, then the elements

$$\xi\alpha = \sigma_1(\xi\alpha), \sigma_2(\xi\alpha), \ldots, \sigma_{p-1}(\xi\alpha)$$

are pairwise distinct.

Proof. From the assumption that $\sigma_i(\alpha) = \sigma_{i+j}(\alpha)$, $p \nmid j$, we have by Lemma 7.65, that

$$\sigma_n(\alpha) = \alpha \tag{45}$$

for some n, $n \not\equiv 1 \pmod{p}$. We may assume n to be the smallest such integer. Suppose on the contrary, that there exists integers u, m such that $1 \leq u < u+m \leq p-1$, that satisfy the equation

$$\sigma_u(\xi\alpha) = \sigma_{u+m}(\xi\alpha).$$

Since $p \nmid m$, we have, by Lemma 7.65, that

$$\sigma_m(\xi\alpha) = \xi\alpha \tag{46}$$

for some integer m, $m \not\equiv 1 \pmod{p}$. Here, too, we take the smallest such m. Multiplying the equation (45) by ξ^n, we get that

$$\xi^n\alpha = \xi^n\sigma_n(\alpha) = \sigma_n(\xi\alpha), \tag{47}$$

using the fact that σ_n is multiplicative, and $\sigma_n(\xi) = \xi^n$. Recall that $\sigma_n \circ \sigma_m = \sigma_{nm}$. Applying σ_n to the equation (46), and σ_m to the equation (47), we get two new equations,

$$\sigma_{nm}(\alpha) = \sigma_n(\xi\alpha) = \xi^n\sigma_n(\alpha) = \xi^n\alpha, \tag{48}$$

and

$$\begin{aligned}\sigma_{nm}(\alpha) &= \sigma_m(\xi^n\alpha) = \xi^{nm}\sigma_m(\alpha) = \xi^{(n-1)m}\xi^m\sigma_m(\alpha) \\ &= \xi^{(n-1)m}\sigma_m(\xi\alpha) = \xi^{(n-1)m}\xi\alpha.\end{aligned} \tag{49}$$

Hence

$$\xi^n\alpha = \xi^{(n-1)m}\xi\alpha,$$

so that $\xi^n = \xi^{(n-1)m}\xi$, which implies that

$$n - 1 \equiv (n-1)m \mod p,$$

and, therefore, $p \mid (n-1)(m-1)$, which is impossible, since by assumption $n, m \not\equiv 1 \pmod{p}$. So, we have necessarily that the elements

$$\xi\alpha = \sigma_1(\xi\alpha), \sigma_2(\xi\alpha), \ldots, \sigma_{p-1}(\xi\alpha)$$

are pairwise distinct. □

Theorem 7.67. For $\alpha \in \mathbb{Q}(\xi)$, let $\mu(\alpha)(x) \in \mathbb{Q}[x]$ denote the minimal polynomial of α over $\mathbb{Q}$. Then one of the following is true.

1. $\mu(\alpha)(x) = (x - \sigma_1(\alpha))(x - \sigma_2(\alpha)) \cdots (x - \sigma_{p-1}(\alpha))$, or
2. $\mu(\alpha\xi)(x) = (x - \sigma_1(\alpha\xi))(x - \sigma_2(\alpha\xi)) \cdots (x - \sigma_{p-1}(\alpha\xi))$.

Proof. For any $\alpha \in \mathbb{Q}(\xi)$, we have that $\deg \mu(\alpha) \leq \deg \Phi(x) = p - 1$. Since α is a zero of $\mu(\alpha)$ by definition, and σ_k is a homomorphism, we have that $\sigma_k(\alpha)$ is a zero of $\mu(\alpha)$ for $k = 1, \ldots, p-1$, by the same argument as in Corollary 7.13.

Let us first suppose that the elements

$$\alpha = \sigma_1(\alpha), \sigma_2(\alpha), \ldots, \sigma_{p-1}(\alpha),$$

are distinct, and let us show that the case 1 of the claim is true. Since the polynomial

$$(x - \sigma_k(\alpha)) \in \mathbb{Q}(\xi)[x]$$

divides $\mu(\alpha)$ in the polynomial ring $\mathbb{Q}(\xi)[x]$ for $k = 1, \ldots, p-1$, and since $\sigma_k(\alpha)$ are distinct by assumption, we have that the polynomial

$$f(x) = (x - \sigma_1(\alpha))(x - \sigma_2(\alpha)) \cdots (x - \sigma_{p-1}(\alpha)) \in \mathbb{Q}(\xi)[x]$$

divides $\mu(\alpha)(x)$ in $\mathbb{Q}(\xi)[x]$. Since $\deg f = p - 1 \geq \deg \mu(\alpha)$ and both f and $\mu(\alpha)$ are monic polynomials, it follows that $f = \mu(\alpha)$, so the case 1 is true.

Next, let us suppose that

$$\sigma_n(\alpha) = \sigma_{n+m}(\alpha)$$

for some $1 \leq n < n + m \leq p - 1$. Lemma 7.66 states that $\sigma_1(\alpha\xi), \ldots, \sigma_{p-1}(\alpha\xi)$ are distinct. As these are all zeros of the minimal polynomial of $\xi\alpha$, $\mu(\xi\alpha)$, we have case 2 by what was shown before. □

Theorem 7.68. If $\alpha \in \mathbb{Q}(\xi)$, then $N(\alpha) \in \mathbb{Q}$, and if $\alpha \in A$, then $\mathbb{N}(\alpha) \in \mathbb{Z}$.

Proof. Let $\alpha \in \mathbb{Q}(\xi)$, and let us show that $N(\alpha) \in \mathbb{Q}$. By Theorem 7.67, at least one of the following is true of the minimal polynomials of α and $\xi\alpha$:

1. $\mu(\alpha)(x) = (x - \sigma_1(\alpha))(x - \sigma_2(\alpha)) \cdots (x - \sigma_{p-1}(\alpha))$, or
2. $\mu(\alpha\xi)(x) = (x - \sigma_1(\alpha\xi))(x - \sigma_2(\alpha\xi)) \cdots (x - \sigma_{p-1}(\alpha\xi))$.

Suppose that the case 1 is true. For $x = 0$, we get that

$$\begin{aligned}
\mu(\alpha)(0) &= (-\sigma_1(\alpha)) \cdots (-\sigma_{p-1}(\alpha)) \\
&= (-1)^{p-1} \prod_{k=1}^{p-1} \sigma_k(\alpha) \\
&= \prod_{k=1}^{p-1} \sigma_k(\alpha) \\
&= N(\alpha).
\end{aligned}$$

Since $\mu(\alpha) \in \mathbb{Q}[x]$, we have that $\mu(\alpha)(0) \in \mathbb{Q}$, hence $N(\alpha) \in \mathbb{Q}$.

Next, let us suppose that case 2 is true. Similarly as in the first case, by setting $x = 0$ in $\mu(\xi\alpha)$, we get that

$$\begin{aligned}
\mu(\xi\alpha)(0) &= (-\sigma_1(\xi\alpha)) \cdots (-\sigma_{p-1}(\xi\alpha)) \\
&= (-1)^{p-1} \xi^{1+2+\cdots+p-1} \prod_{k=1}^{p-1} \sigma_k(\alpha) \\
&= \xi^{\frac{p(p-1)}{2}} \prod_{k=1}^{p-1} \sigma_k(\alpha) \\
&= \prod_{k=1}^{p-1} \sigma_k(\alpha) \\
&= N(\alpha).
\end{aligned}$$

Like in the first case, since $\mu(\xi\alpha) \in \mathbb{Q}[x]$, we have that $\mu(\xi\alpha)(0) \in \mathbb{Q}$, and consequently $N(\alpha) \in \mathbb{Q}$ as claimed.

Let $\alpha \in A$, and let us show that $N(\alpha) \in \mathbb{Z}$. We already showed that $N(\alpha) \in \mathbb{Q}$. Since $\alpha \in \mathbb{Z}[\xi]$, and, therefore, $\alpha_k(\alpha) \in \mathbb{Z}[\xi]$ for every k, we have that the rational number

$$N(\alpha) = \prod_{k=1}^{p-1} \sigma_k(\alpha)$$

must be an integer. □

Using the properties of the norm, we have the following result about the units of A.

Theorem 7.69. If $\alpha \in A$ is a unit, then $N(\alpha) = \pm 1$.

Proof. By Theorem 7.64, the norm is multiplicative. By Theorem 7.68, we have that $N(\alpha)$, and $N(\alpha^{-1})$ are integers. Since $N(1) = 1$, and since $\alpha^{-1} \in A$, we get that

$$1 = N(1) = N(\alpha\alpha^{-1}) = N(\alpha)N(\alpha^{-1}),$$

meaning $N(\alpha) = \pm 1$. □

7.5 Theorem of Inkeri

The next lemma is by Inkeri and the proof is from [1].

Lemma 7.70. Let $p \neq q$ be odd primes and $x, y \geq 3$ integers such that $x^p - y^q = 1$. If $q \nmid h_p$ then there exists real units $\epsilon, \eta \in A$ such that

$$\begin{cases} \epsilon^p = \alpha^q + \overline{\alpha}^q \\ \eta x = \beta^q + \overline{\beta}^q \end{cases}$$

where $\alpha, \beta \in A$ are not units.

Proof. Let ξ denote the p-th root of unity and $A = \mathbb{Z}[\xi]$. By Lemma 6.1 there exists an integer u such that

$$pu^q = \frac{x^p - 1}{x - 1} = 1 + x + \cdots + x^{p-1} = \Phi(x) = (x - \xi) \cdots (x - \xi^{p-1}).$$

As mentioned in Theorem 6.3, $u > 1$. Since $p = \Phi(1) = (1 - \xi) \cdots (1 - \xi^{p-1})$, we may write

$$u^q = \frac{(x - \xi) \cdots (x - \xi^{p-1})}{(1 - \xi) \cdots (1 - \xi^{p-1})} = \prod_{i=1}^{p-1} \delta_i \tag{50}$$

where for $i = 1, \ldots, p - 1$

$$\delta_i = \frac{x - \xi^i}{1 - \xi^i} = \frac{x - 1}{1 - \xi^i} + 1. \tag{51}$$

Let us show that δ_i is in A for every $i = 1, \dots p-1$. By Lemma 6.1, we have that $p^2 \mid x-1$, so $x-1 = dp^2$, where $d \in \mathbb{Z}$ is non-zero. By Lemma 7.60 $1-\xi^i$ and $1-\xi$ are associate for all $i = 1, \dots, p-1$, i.e.,

$$1 - \xi^i = \alpha_i(1-\xi)$$

where $\alpha_i \in A$ is a unit. Thus

$$p = \beta(1-\xi)^{p-1},$$

where $\beta \in A$ is a unit. Now we have, from the equation (51), that

$$\delta_i = \frac{x-1}{1-\xi^i} + 1 = \frac{dp\beta(1-\xi)^{p-1}}{\alpha_i(1-\xi)} + 1 = dp\alpha_i^{-1}\beta(1-\xi)^{p-2} + 1 \in A. \tag{52}$$

Let us show that the ideals (δ_i) and (δ_j) are relatively prime for $i < j$. Suppose on the contrary, that a prime ideal P divides both (δ_i) and (δ_j), so that there exists integral ideals I, J such that

$$(\delta_i) = PI, \text{ and}$$
$$(\delta_j) = PJ.$$

Then $(\delta_i), (\delta_j) \subseteq P$, so that $\delta_i, \delta_j \in P$. Hence

$$0 \equiv (1-\xi^j)\delta_j - (1-\xi^i)\delta_i = \xi^i - \xi^j = \xi^i(1-\xi^{j-i}) \pmod{P},$$

where $\xi^i(1-\xi^{j-i})$ is associate with $1-\xi$, so $1-\xi \in P$. Thus, from the equation (52), we get that $\delta_i \equiv 1 \pmod{P}$. But $\delta_i \in P$, hence $1 \in P$, which is a contradiction, since P is prime. So, (δ_i) and (δ_j) are relatively prime.

Let us show that (δ_i) are not unit ideals. Suppose on the contrary, that

$$(\delta_i) = \left(\frac{x-\xi^i}{1-\xi^i}\right) = (1)$$

for some i. Then

$$(x-\xi^i) = (1-\xi^i),$$

meaning that $x-\xi^i$ and $1-\xi^i$ are associate, ie.

$$x - \xi^i = \eta(1-\xi^i), \tag{53}$$

where $\eta \in A$ is a unit. By Theorem 7.69, the norm of a unit is ± 1, so we have that $N(\eta) = \pm 1$. Taking norms of the equation (53), we get that

$$N(x-\xi^i) = N(\eta(1-\xi^i)) = N(\eta)N(1-\xi^i) = \pm N(1-\xi^i),$$

thus

$$\prod_{k=1}^{p-1} \sigma_k(x-\xi^i) = \pm 1 \prod_{k=1}^{p-1} \sigma_k(1-\xi^i)$$

Dividing by the right-hand side of the equation, which is non-zero, since $\sigma_k(1-\xi^i) \neq 0$ for $k = 1, \ldots, p-1$, we get that

$$\pm 1 = \prod_{k=1}^{p-1} \frac{\sigma_k(x-\xi^i)}{\sigma_k(1-\xi^i)} = \prod_{k=1}^{p-1} \frac{x-\xi^{ki}}{1-\xi^{ki}} = \prod_{k=1}^{p-1} \delta_k.$$

But this is a contradiction, since

$$\prod_{k=1}^{p-1} \delta_k = u^q \neq \pm 1.$$

So, necessarily $(\delta_i) \neq (1)$.

Since (δ_i) and (δ_j) are relatively prime, and not unit ideals, it follows from the equation (50), that $(\delta_i) = J_i^q$ for some non-unit integral ideal J_i. By assumption $q \nmid h_p$, so that, by Lemma 7.58, there exists $\alpha_i \in A$ such that $J_i = (\alpha_i)$. Since $J_i \neq (1)$, α_i is not a unit. Now $(\delta_i) = (\alpha_i^q)$, so there exists a unit $\epsilon_i \in A$ such that

$$\delta_i = \epsilon_i \alpha_i^q.$$

By Theorem 7.63, for every $i = 1, \ldots, p-1$,

$$\epsilon_i = \xi^{k_i} \eta_i$$

where $1 \leq k_i \leq p-1$ and $\eta_i \in A$ is a real unit. Thus

$$x - \xi^i = \xi^{k_i} \eta_i \alpha_i^q (1-\xi^i).$$

For $i = 2$

$$x - \xi^2 = \xi^{k_2} \eta_2 \alpha_2^q (1-\xi^2) = \xi^{k_2+1} \eta_2 \alpha_2^q (\xi^{-1} - \xi). \tag{54}$$

Since $p \neq q$, there exists integers e, f such that $ep + fq = 1$, such that

$$\xi^{k_2+1} = \xi^{(k_2+1)(ep+fq)} = \xi^{(k_2+1)ep} \xi^{(k_2+1)fq} = \xi^{(k_2+1)fq}.$$

Thus (54) becomes

$$x - \xi^2 = \xi^{(k_2+1)fq} \eta_2 \alpha_2^q (\xi^{-1} - \xi) = \eta_2 \gamma^q (\xi^{-1} - \xi) \tag{55}$$

where we write $\gamma = \xi^{(k_2+1)f} \alpha_2 \in A$. Since α_2 is not a unit, γ is not a unit.

The complex conjugate satisfies for all $z_1, z_2 \in \mathbb{C}$ the identities

$$\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}, \qquad \overline{z_1 z_2} = \overline{z_1} \cdot \overline{z_2}, \qquad \overline{z_1} \cdot z_1 = |z_1|^2 \qquad \overline{\overline{z_1}} = z_1.$$

Then

$$\overline{\xi} = \frac{|\xi|^2}{\xi} = \frac{1}{\xi}$$

so that we have the equalities

$$\overline{x - \xi^2} = x - (\overline{\xi})^2 = x - \xi^{-2}$$

and

$$\overline{\xi^{-1} - \xi} = \overline{\xi^{-1}} - \overline{\xi} = \xi - \xi^{-1}.$$

Now when taking complex conjugates of (55) we get that

$$x - \xi^{-2} = \eta_2 \overline{\gamma}^q (\xi - \xi^{-1}). \tag{56}$$

Subtracting (55) from (56) we get that

$$\xi^2 - \xi^{-2} = \eta_2 (\gamma^q + \overline{\gamma}^q)(\xi - \xi^{-1})$$

and

$$\frac{\xi + \xi^{-1}}{\eta_2} = \gamma^q + \overline{\gamma}^q \in A \cap \mathbb{R}. \tag{57}$$

By Lemma 7.60 $1 - \xi^2$ and $1 - \xi^4$ are associate, so there exists a unit $u \in A$ such that $1 - \xi^4 = u(1 - \xi^2)$ whereby

$$\xi + \xi^{-1} = \frac{\xi^2 - \xi^{-2}}{\xi - \xi^{-1}} = \frac{\xi^{-2}(\xi^4 - 1)}{\xi^{-1}(\xi^2 - 1)} = \xi^{-1} u$$

is a unit. Then, from (57) we get that

$$\eta = \gamma^q + \overline{\gamma}^q = \frac{\xi + \xi^{-1}}{\eta_2} \in A \cap \mathbb{R} \tag{58}$$

is a real unit. Let us write $\epsilon = \eta^e$ and $\alpha = \eta^{-f}\gamma$. Then ϵ is a real unit and α is not a unit. Since $ep + fq = 1$, ϵ and α satisfy

$$\begin{aligned} \alpha^q + \overline{\alpha}^q &= \eta^{-fq}\gamma^q + \eta^{-fq}\overline{\gamma}^q \\ &= \eta^{ep-1}(\gamma^q + \overline{\gamma}^q) \\ &= \eta^{ep} \\ &= \epsilon^p. \end{aligned}$$

Multiplying (55) by ξ^{-2} we get that

$$\xi^{-2}x - 1 = \eta_2 \gamma^q (\xi^{-1} - \xi)\xi^{-2}.$$

Let $\beta = \xi^{-2f}\gamma$. Then β is not a unit since γ is not a unit, and

$$\xi^{-2}x - 1 = \eta_2 \beta^q (\xi^{-1} - \xi). \tag{59}$$

Taking conjugates of (59) implies that

$$\xi^2 x - 1 = \eta_2 \overline{\beta}^q (\xi - \xi^{-1}). \tag{60}$$

Subtracting (59) from (60) gives us the identity

$$(\xi^2 - \xi^{-2})x = \eta_2 (\xi - \xi^{-1})(\beta^q + \overline{\beta}^q)$$

and, therefore,

$$x = \frac{\eta_2 (\beta^q + \overline{\beta}^q)}{\xi + \xi^{-1}}$$

so that by (58) we get that

$$\eta x = \frac{\xi + \xi^{-1}}{\eta_2} \cdot \frac{\eta_2(\beta^q + \overline{\beta}^q)}{\xi + \xi^{-1}} = \beta^q + \overline{\beta}^q.$$

□

Theorem 7.71. Let $a, b \in \mathbb{Z}$. If $b \mid a$ in A, then $b \mid a$ in $\mathbb{Z}$. That is, if $a = \gamma b$, where $\gamma \in A$, then $\gamma \in \mathbb{Z}$.

Proof. Let $a, b \in \mathbb{Z}$, and let $a = \gamma b$, where $\gamma \in A$. Then $\gamma = \frac{a}{b} \in A \cap \mathbb{Q}$. Theorem 7.5 states that $A \cap \mathbb{Q} = \mathbb{Z}$, hence $\gamma \in \mathbb{Z}$, so that $b \mid a$ in $\mathbb{Z}$. □

The next theorem, *the rule of lifting the exponent*, is from [3].

Theorem 7.72. Let a, b be integers and let p be a prime number. If $a^p \equiv b^p \pmod{p}$ then $a^p \equiv b^p \pmod{p^2}$.

Proof. Let $a^p \equiv b^p \pmod{p}$. By Fermat's Little Theorem

$$\begin{aligned} a^p &\equiv a \pmod{p} \\ b^p &\equiv b \pmod{p}. \end{aligned}$$

Hence $a \equiv b \pmod{p}$. Thus in the factorization

$$a^p - b^p = (a - b) \sum_{i=1}^{p} a^{p-i} b^{i-1}$$

we have $a - b \equiv 0 \pmod{p}$ and

$$\sum_{i=1}^{p} a^{p-i} b^{i-1} \equiv \sum_{i=1}^{p} a^{p-1} = p a^{p-1} \equiv 0 \pmod{p}$$

whereby $p^2 \mid a^p - b^p$.

□

The next lemma and its proof are from [4].

Lemma 7.73. If x, y are non-zero integers and $p \neq q$ are odd primes such that $x^p - y^q = 1$, then

$$x \equiv -(p^{q-1} - 1) \pmod{q^2}, \qquad y \equiv q^{p-1} - 1 \pmod{p^2} \tag{61}$$

so that

$$\begin{aligned} &x \equiv 0 \pmod{q^2} \text{ if and only if } p^{q-1} - 1 \equiv 0 \pmod{q^2} \\ &y \equiv 0 \pmod{p^2} \text{ if and only if } q^{p-1} - 1 \equiv 0 \pmod{p^2}. \end{aligned} \tag{62}$$

Proof. By Cassels' Theorem 5.6, $q \mid x$ and $p \mid y$. By Lemma 6.1 the following equations hold

$$\begin{aligned} x - 1 &= p^{q-1}a^q \\ y + 1 &= q^{p-1}b^p \end{aligned}$$

and

$$\begin{aligned} x &= (p^{q-1} - 1)a^q + a^q + 1 \equiv 0 \pmod{q}, \text{ and} \\ y &= (q^{p-1} - 1)b^p + b^p - 1 \equiv 0 \pmod{p}. \end{aligned} \tag{63}$$

By Fermat's Little Theorem

$$\begin{aligned} p^{q-1} - 1 &\equiv 0 \pmod{q} \text{ and} \\ q^{p-1} - 1 &\equiv 0 \pmod{p} \end{aligned}$$

and using the equations (63) we get that

$$\begin{aligned} x &\equiv a^q + 1 \equiv 0 \pmod{q} \text{ and} \\ y &\equiv b^p - 1 \equiv 0 \pmod{p}. \end{aligned}$$

Hence

$$\begin{aligned} a^q &\equiv -1 = (-1)^q \pmod{q} \text{ and} \\ b^p &\equiv 1 = 1^p \pmod{p}. \end{aligned}$$

By the rule of lifting the exponent in Theorem 7.72 we get that

$$\begin{aligned} a^q &\equiv (-1)^q \equiv -1 \pmod{q^2} \text{ and} \\ b^p &\equiv 1^p \equiv 1 \pmod{p^2}. \end{aligned}$$

Now equations (63) imply that

$$\begin{aligned} x &\equiv -(p^{q-1} - 1) \pmod{q^2} \text{ and} \\ y &\equiv (q^{p-1} - 1) \pmod{p^2}. \end{aligned} \tag{64}$$

□

Lemma 7.74. If q is an odd prime, and $x, y \in A$, then

$$(x + y)^q = x^q + qxy(x + y)\delta + y^q,$$

where $\delta \in A$.

Proof. Since q is odd, we have that $q - 1$ is even, so we may write

$$\begin{aligned} (x + y)^q &= \sum_{k=0}^{q} \binom{q}{k} x^k y^{q-k} \\ &= x^q + y^q + \sum_{k=1}^{q-1} \binom{q}{k} x^k y^{q-k} \\ &= x^q + y^q + \sum_{k=1}^{\frac{q-1}{2}} \left(\binom{q}{k} x^k y^{q-k} + \binom{q}{q-k} x^{q-k} y^k \right). \end{aligned} \tag{65}$$

The binomial coefficient satisfies the identity,

$$\binom{q}{k} = \binom{q}{q-k},$$

hence

$$\binom{q}{k}(xy)^k = \binom{q}{q-k}(xy)^k,$$

so that the equation (65) becomes

$$= x^q + y^q + \sum_{k=1}^{\frac{q-1}{2}} \binom{q}{k}(xy)^k \left(y^{q-2k} + x^{q-2k}\right) \tag{66}$$

Here, $q - 2k > 0$ is odd, so that

$$x^{q-2k} + y^{q-2k} = x^{q-2k} - (-y)^{q-2k} = (x+y)\sum_{i=1}^{q-2k} x^{q-2k-i}(-y)^{i-1},$$

so we may write

$$x^{q-2k} + y^{q-2k} = (x+y)S_k.$$

Since q is prime, we have that $q \mid \binom{q}{k}$ for $1 \leq k \leq q-1$. Thus, the equation (66) becomes

$$\begin{aligned} &= x^q + y^q + \sum_{k=1}^{\frac{q-1}{2}} \binom{q}{k}(xy)^k (x+y)S_k \\ &= x^q + y^q + qxy(x+y)\sum_{k=1}^{\frac{q-1}{2}} \binom{q}{k} q^{-1}(xy)^{k-1}S_k \\ &= x^q + y^q + qxy(x+y)\delta. \end{aligned}$$

□

The next theorem is by Inkeri and its proof is from [1].

Theorem 7.75. Let $p \neq q$ be odd primes and x, y non-zero integers such that $x^p - y^q = 1$ and h_p and h_q be the orders of the ideal class groups of the p-th and q-th cyclotomic fields. Then the following implications hold.

i) If $q \nmid h_p$, then $q^2 \mid x$ and $p^{q-1} \equiv 1 \pmod{q^2}$.

ii) If $p \nmid h_q$, then $p^2 \mid y$ and $q^{p-1} \equiv 1 \pmod{p^2}$.

Proof. Let us prove i). Suppose that $q \nmid h_p$. By Lemma 7.70, we have that

$$\eta x = \beta^q + \overline{\beta}^q,$$

where $\eta \in A$ is a unit, and $\beta \in A$. By Lemma 7.74, we have that

$$\beta^q + \overline{\beta}^q - (\beta + \overline{\beta})^q = q\beta\overline{\beta}(\beta + \overline{\beta})\delta,$$

where $\delta \in A$. Then

$$\eta x = \beta^q + \overline{\beta}^q = (\beta + \overline{\beta})^q + q(\beta\overline{\beta})(\beta + \overline{\beta})\delta. \tag{67}$$

By Cassels' Theorem 5.6, we have that $q \mid x$, hence $q \mid (\beta + \overline{\beta})^q$. Then, by Theorem 7.25, we have that

$$(q) \mid (\beta + \overline{\beta})^q.$$

Let

$$(q) = Q_1 \cdots Q_n$$

be the prime ideal factorization of (q). So, we have that

$$(\beta + \overline{\beta})^q = Q_1 \cdots Q_n I,$$

where I is an integral ideal. Since $q \neq p$, we have that the prime ideals Q_i dividing (q) are distinct, by Theorem 7.54. Since q is not a unit, due to $A \cap \mathbb{Q} = \mathbb{Z}$, then $(\beta + \overline{\beta})^q$ is not the unit ideal, hence $(\beta + \overline{\beta})$ is not the unit ideal. Let

$$\beta + \overline{\beta} = P_1^{a_1} \cdots P_m^{a_m}$$

be the prime ideal factorization of $\beta + \overline{\beta}$, where P_i are distinct prime ideals, and $a_i > 0$. From $Q_i \mid (\beta + \overline{\beta})^q$, it follows that $Q_i = P_{m_i}$, where $1 \leq m_i \leq m$. Since the ideals Q_i are distinct, we get that

$$Q_1 \cdots Q_n \mid P_1 \cdots P_m,$$

and, therefore,

$$(q) \mid (\beta + \overline{\beta}).$$

Thus $q \mid \beta + \overline{\beta}$, by Theorem 7.25, so that, certainly, $q^2 \mid (\beta + \overline{\beta})^q$. Then we get, from the equation (67), that $q^2 \mid \eta x$. Since $q \mid x$, we may write $x = dq$. From the fact that $q^2 \mid \eta x$, we get that

$$\eta x = \eta dq = q^2\gamma,$$

where $\gamma \in A$, so that

$$d = q\gamma\eta^{-1},$$

where η is a unit by assumption, hence $\gamma\eta^{-1} \in A$. Thus $q \mid d$ in A, so by Theorem 7.71, we have that $q \mid d$ in $\mathbb{Z}$, and, therefore, $q^2 \mid x$ in $\mathbb{Z}$. Then, by Lemma 7.73, we have that

$$p^{q-1} - 1 \equiv 0 \pmod{q^2},$$

which completes the proof of i).

The second claim, ii), follows from i): From the equation $x^p - y^q = 1$, we get that $(-y)^q - (-x)^p = 1$. Applying the first result, i), we get that $p^2 \mid -y$, hence $p^2 \mid y$, and

$$q^{p-1} - 1 \equiv 0 \pmod{p^2}.$$

□

Consequence 7.76. The equations $x^5 - y^7 = \pm 1$ have no non-zero solutions.

Proof. Suppose that $x^5 - y^7 = 1$. By Table 1, we have that $7 \nmid h_5 = 1$, so we get from Theorem 7.75 condition i) (where $q = 7$ and $p = 5$), that $5^{7-1} \equiv 1 \pmod{7^2}$, which is false.

Let us next suppose that $x^5 - y^7 = -1$. Then $y^7 - x^5 = 1$, so by Theorem 7.75 condition ii) (where $q = 5$ and $p = 7$), we also get that either $7 \mid h_5 = 1$ or $5^{7-1} \equiv 1 \pmod{7^2}$, both of which are false. □

The next theorem involving the class number of $\mathbb{Q}(\sqrt{-p})$ is by Inkeri and it's from [1].

Theorem 7.77. Let $p, q > 3$ be odd primes and integers $x, y \neq 0$ such that $x^p - y^q = 1$ and let $H(-p)$ denote the class number of $\mathbb{Q}(\sqrt{-p})$. Then the following condition are true.

i) If $p \equiv 3 \pmod 4$ and $q \nmid H(-p)$, then $p^{q-1} \equiv 1 \pmod{q^2}$, $q^2 \mid x$, and $y \equiv -1 \pmod{q^{2p-1}}$.

ii) If $q \equiv 3 \pmod 4$ and $p \nmid H(-q)$, then $q^{p-1} \equiv 1 \pmod{p^2}$, $p^2 \mid y$, and $x \equiv 1 \pmod{p^{2q-1}}$.

iii) If $3 < q < p$, $p \equiv q \equiv 3 \pmod 4$, and $q \nmid H(-p)$, then $p^{q-1} \equiv 1 \pmod{q^2}$, $q^{p-1} \equiv 1 \pmod{p^2}$, $p^2 \mid x$, $q^2 \mid y$, $x \equiv 1 \pmod{p^{2q-1}}$, and $y \equiv -1 \pmod{q^{2p-1}}$.

Inkeri's Theorems 7.77 and 7.75 enabled the following result which gives the non-existence of non-zero solutions (x, y) for $x^p - y^q = 1$ for a large number of prime pairs (p, q).

Theorem 7.78.

i) If $p \equiv q \equiv 3 \pmod 4$ and $5 \leq p, q < 10^4$ then $x^p - y^q = 1$ has no non-zero solutions (x, y), with possible exceptions being

$$(p, q) = (83, 4871), (4871, 83).$$

ii) If $p \equiv 3 \pmod 4$, $q \equiv 1 \pmod 4$ and $5 \leq p, q < 500$ then $x^p - y^q = 1$ has non non-zero solutions (x, y), with possible exceptions being

$$(p, q) = (19, 137), (223, 349), (251, 421), (419, 173), (419, 349), (499, 109).$$

Proof. Note that a solution in integers for $x^p - y^q = 1$ implies a solution for $x^q - y^p = 1$. We begin by giving the strategy for the proof to make it easier to follow:

1) First we show that there are no solutions when

$$\begin{cases} 5 \leq p < 73 \\ 5 \leq q < 10^4 \\ p \equiv q \equiv 3 \pmod 4 \end{cases}$$

which implies that there are no solutions when

$$\begin{cases} 5 \leq p < 10^4 \\ 5 \leq q < 73 \\ p \equiv q \equiv 3 \pmod 4). \end{cases}$$

Then we show that when

$$\begin{cases} 5 \leq p < 73 \\ 5 \leq q < 500 \\ p \equiv 3 \pmod 4 \\ q \equiv 1 \pmod 4 \end{cases}$$

there are no solutions with possible exceptions of $(p, q) = (19, 137)$.

2) Next we show that when

$$\begin{cases} 73 \leq p < 10^4 \\ 73 \leq q < 10^4 \\ p \equiv q \equiv 3 \pmod 4 \end{cases}$$

there are no solutions with possible exception of

$$(p, q) \in \{(83, 4871), (4871, 83)\}.$$

3) Lastly we show that when

$$\begin{cases} 73 \leq p < 500 \\ 5 \leq q < 500 \\ p \equiv 3 \pmod 4 \\ q \equiv 1 \pmod 4 \end{cases}$$

there are no solutions with the possible exception of

$$(p, q) \in \{(223, 349), (251, 421), (419, 173), (419, 349), (499, 109)\}.$$

These parts together give the result.

For odd primes p, q, let h_q denote the class number of the q-th cyclotomic field $\mathbb{Q}(\xi_q)$, and let $H(-p)$ denote the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$. We use values for h_q for primes $q < 100$ in Table 1, which is from [5], and values for $H(-p)$ for primes $p < 10^4$ with $p \equiv 3 \pmod 4$ in Table 4. We also use the solutions of the congruence $p^{q-1} \equiv 1 \pmod{q^2}$ for primes $p < 1000$ and $q < 10^4$ in Table 3.

Suppose $x^p - y^q = 1$ has a non-trivial solution.

Let us prove the step 1). Let $5 \leq p < 73$ and $5 \leq q < 10^4$ with $p \equiv 3 \pmod 4$. Let us show that $p^{q-1} \equiv 1 \pmod{q^2}$. Suppose that $p^{q-1} \not\equiv 1 \pmod{q^2}$. Then by Theorem 7.77 $q \mid H(-p)$. By Table 4 the only candidates are $(p, q) \in \{(47, 5), (71, 7)\}$. For these candidates Table 1 gives $h_5 = h_7 = 1$, hence $p \nmid h_q$, in which case Theorem 7.75 implies $q^{p-1} \equiv 1 \pmod{p^2}$. However, by Table 3 neither pair $(p, q) = (47, 5), (71, 7)$ satisfies $q^{p-1} \equiv 1 \pmod{p^2}$, which is a contradiction. Hence $p^{q-1} \equiv 1 \pmod{q^2}$.

By Table 3 the solutions of $p^{q-1} \equiv 1 \pmod{q^2}$ with $5 \leq p < 73$, $5 \leq q < 10^4$ and $p \equiv 3 \pmod 4$ are

$$\begin{aligned} (p, q) \in \{&(7, 5), (11, 71), (19, 7), (19, 13), \\ &(19, 43), (19, 137), (23, 13), (31, 7), (31, 79), \\ &(31, 6451), (43, 5), (43, 103), (59, 2777), \\ &(67, 7), (67, 47), (71, 47), (71, 331).\} \end{aligned} \tag{68}$$

Let us first consider pairs with $q \equiv 3 \pmod 4$:

$$\begin{aligned}(p,q) \in \{&(11,71),(19,7),\\ &(19,43),(31,7),(31,79),\\ &(31,6451),(43,103),\\ &(67,7),(67,47),(71,47),(71,331).\}\end{aligned}$$

For there pairs, we see from Table 4 that $p \nmid H(-q)$, and, therefore, by Theorem 7.77 $q^{p-1} \equiv 1 \pmod{p^2}$, but this is not true as seen in Table 4 for the pairs with $q < 10^3$. The remaining pair $(31, 6451)$ is outside the range of Table 4, but by direct calculation we have that $6451^{31-1} \equiv 621 \not\equiv 1 \pmod{31^2}$.

Now consider the remaining pairs in (68) with $q \equiv 1 \pmod 4$:

$$\begin{aligned}(p,q) \in \{&(7,5),(19,13),\\ &(19,137),(23,13),\\ &(43,5),(59,2777).\}\end{aligned}$$

From Table 1 we see that $p \nmid h_q$ except possibly with $(p,q) \in \{(19,137),(59,2777)\}$ (the latter pair of which is out of our range of interest of this theorem). Therefore, by Theorem 7.75, $q^{p-1} \equiv 1 \pmod{p^2}$, which is false as seen from Table 3. This concludes the proof of part 1).

Let us prove the step 2). Let $73 \le p < 10^4$ and $73 \le q < 10^4$ with $p \equiv q \equiv 3 \pmod 4$. Let us show that $q \nmid H(-p)$. Suppose on the contrary that $q \mid H(-p)$. The class number $H(-p)$ is small for p in our range, and we see from Table 4 that with these constraints

$$\begin{aligned}(p,q) \in \{&(4391,79),(5399,79),(7127,79),(3911,83),\\ &(5039,83),(8423,83),(8231,107),(9239,139)\}\end{aligned}$$

Since the class number satisfies $H(-q) < q$, we have with these candidates $H(-q) < q < p$ hence $p \nmid H(-q)$, and, therefore, by Theorem 7.77 $q^{p-1} \equiv 1 \pmod{p^2}$. From Table 3 we see that this is not true. Hence $q \nmid H(-p)$, so by Theorem 7.77 $p^{q-1} \equiv 1 \pmod{q^2}$. Since a solution for $x^p - y^q = 1$ implies a solution for $x^q - y^p = 1$, we have also $q^{p-1} \equiv 1 \pmod{p^2}$ by the same proof as above. From Table 2 the only pair satisfying both of these congruences is $(p,q) = (83, 4871)$, which also satisfies $83 \equiv 4871 \equiv 3 \pmod 4$. Then so does $(p,q) = (4871, 83)$ as desired. This concludes part 2).

Finally, let us prove the step 3). Let $73 \le p < 500$, $5 \le q < 500$, $p \equiv 3 \pmod 4$, and $q \equiv 1 \pmod 4$. Let us show that $q \nmid H(-p)$. Suppose on the contrary that $q \mid H(-p)$. With these constraints it is seen from Table 4 that

$$\begin{aligned}(p,q) \in \{&(79,5),(103,5),(127,5),(131,5),(179,5),\\ &(191,13),(227,5),(239,5),(263,13),(347,5),\\ &(383,17),(439,5),(443,5),(479,5)\}.\end{aligned}$$

For these pairs Table 1 shows that $p \nmid h_q$. Therefore, by Theorem 7.75, $q^{p-1} \equiv 1 \pmod{p^2}$, but Table 3 shows that this is false. Hence $q \nmid H(-p)$. Now by

Theorem 7.77 $p^{q-1} \equiv 1 \pmod{q^2}$. From Table 3, with the conditions $73 \leq p < 500$, $5 \leq q < 500$, $p \equiv 3 \pmod 4$, $q \equiv 1 \pmod 4$, the only pairs satisfying the congruence $p^{q-1} \equiv 1 \pmod{q^2}$ are

$$\begin{aligned}(p,q) \in \{&(107,5),(107,97),(131,17),(151,5),\\ &(179,17),(191,13),(199,5),(223,349),(239,13),\\ &(251,5),(251,17),(251,421),(307,5),(419,173),\\ &(419,349),(443,5),(467,29),(487,41),\\ &(499,5),(499,109)\}.\end{aligned}$$

Of these pairs with $q < 100$ Table 1 shows that $p \nmid h_q$, and, therefore, by Theorem 7.75, $q^{p-1} \equiv 1 \pmod{p^2}$, but as seen from Table 3 this is not true. So the possible exceptions are the pairs with $q \geq 100$:

$$(p,q) \in \{(223,349),(251,421),(419,173),(419,349),(499,109)\}.$$

□

Table 1: h_q, $3 \leq q \leq 100$

q	h_q	q	h_q
3	1	43	211
5	1	47	$5 \cdot 139$
7	1	53	4889
11	1	59	$3 \cdot 59 \cdot 233$
13	1	61	$41 \cdot 1861$
17	1	67	$67 \cdot 12739$
19	1	71	$7 \cdot 7 \cdot 79241$
23	3	73	$89 \cdot 134353$
29	$2 \cdot 2 \cdot 2$	79	$5 \cdot 53 \cdot 377911$
31	9	83	$3 \cdot 279405653$
37	37	89	$113 \cdot 118401449$
41	$11 \cdot 11$	97	$577 \cdot 3457 \cdot 206209$

Table 2: $2 \leq p \leq 10^3$, $3 \leq q \leq 10^4$ such that $p^{q-1} \equiv 1 \pmod{q^2}$ and $q^{p-1} \equiv 1 \pmod{p^2}$

Base p	Solutions q
2	1093
83	4871

Table 3: $2 \leq p \leq 10^3$, $3 \leq q \leq 10^4$ such that $p^{q-1} \equiv 1 \pmod{q^2}$

Base p $\equiv 3$	Solutions q $\equiv 3$	Solutions q $\equiv 1$	Base p $\equiv 1$	Solutions q $\equiv 3$	Solutions q $\equiv 1 \pmod 4$
3	11		2	3511	1093
7		5	5		
11	71		13	863	
19	3 7 43	13 137	17	3	
23		13	29		
31	7 79 6451		37	3	
43	103	5	41		29
47			53	3 47 59	97
59		2777	61		
67	7 47		73	3	
71	3 47 331		89	3	13
79	7 263	3037	97	7	
83	4871		101		5
103			109	3	
107	3	5 97	113		
127	3 19 907		137	59	29
131		17	149		5
139			157		5
151	2251	5	173	3079	
163	3		181	3	101
167			193		5
179	3	17	197	3 7	653
191		13	229	31	
199	3	5	233	3 11	157
211			241	11 523 1163	
223	71	349	257	359	5
227	7		269	3 11 83	
239	11	13	277		1993
251	3 11	5 17 421	281		
263	7 23 251		293	7 19 83	5
271	3		313	7	41 149 181
283			317	107	349
307	3 19 487	5	337		13
311			349		5 197 433
331	211 359		353		
347			373	7	113
359	3 23 307		389	19	373
367	43	2213	397	3	
379	3		401	83 347	5
383			409		
419	983	173 349	421	1483	101

Base p $\equiv 3$	Solutions q $\equiv 3$	Solutions q $\equiv 1$	Base p $\equiv 1$	Solutions q $\equiv 3$	Solutions q $\equiv 1 \pmod 4$
431	3		433	3	
439	31 79		449	3	5 1789
443		5	457	11 919	5
463	1667		461		1697
467	3 743	29	509	7	41
479	47		521	3 7 31	53
487	3 11 23	41 1069	541	3	
491	7 79		557	3 7 23	5
499		5 109	569	7 263	
503	3 659	17 229	577	3 71	13 17
523	3		593	3	5
547	31		601		5 61
563			613	3	
571	23	29	617	1087	101
587	7 31	13	641	43	
599		5	653	19	13 17 1381
607	7	5	661		
619	7	73	673		61
631	3 1787		677	211	13
643	307 859	5 17	701	3	5
647	3 23		709	199 1663	17
659	23 131		733		17
683	3 1279		757	3 71	5 17
691	1091	37 509	761	907	41
719	3	41	769		
727	11		773	3	
739	3		797		
743		5	809	3 59	
751	151	5 409	821	19 83	233 293 1229
787		37 41	829	3	17
811	3 211		853		
823		13	857		5 41 157
827	3	17 29	877		
839			881	3 7 23	
859	71		929		
863	3 7 23 467		937	3	41 113 853
883	3 7		941	11 1499	
887	11 607		953	3	
907		5 17	977	11 239	17 109 401
911	127		997	1223	197
919	3				
947					
967	11 19				
971	3 11	401			

Base p $\equiv 3$	Solutions q $\equiv 3$	Solutions q $\equiv 1$	Base p $\equiv 1$	Solutions q $\equiv 3$	Solutions q $\equiv 1 \pmod 4$
983					
991	3 431	13			

Table 4: $H(-p)$, $p \equiv 3 \pmod 4$, $3 \leq p \leq 10^4$

p	$H(-p)$	Factorization	Factors $q \equiv 3 \pmod 4$	Factors $q \equiv 1 \pmod 4$
3	1			
7	1			
11	1			
19	1			
23	3	3	3	
31	3	3	3	
43	1			
47	5	5		5
59	3	3	3	
67	1			
71	7	7	7	
79	5	5		5
83	3	3	3	
103	5	5		5
107	3	3	3	
127	5	5		5
131	5	5		5
139	3	3	3	
151	7	7	7	
163	1			
167	11	11	11	
179	5	5		5
191	13	13		13
199	9	$3 \cdot 3$	3	
211	3	3	3	
223	7	7	7	
227	5	5		5
239	15	$3 \cdot 5$	3	5
251	7	7	7	
263	13	13		13
271	11	11	11	
283	3	3	3	
307	3	3	3	
311	19	19	19	
331	3	3	3	
347	5	5		5
359	19	19	19	
367	9	$3 \cdot 3$	3	
379	3	3	3	
383	17	17		17
419	9	$3 \cdot 3$	3 3	
431	21	$3 \cdot 7$	3 7	
439	15	$3 \cdot 5$	3	5

p	$H(-p)$	Factorization	Factors $q \equiv 3 \pmod 4$	Factors $q \equiv 1 \pmod 4$
443	5	5		5
463	7	7	7	
467	7	7	7	
479	25	$5 \cdot 5$		5
487	7	7	7	
491	9	$3 \cdot 3$	3 3	
499	3	3	3	
503	21	$3 \cdot 7$	3 7	
523	5	5		5
547	3	3	3	
563	9	$3 \cdot 3$	3 3	
571	5	5		5
587	7	7	7	
599	25	$5 \cdot 5$		5
607	13	13		13
619	5	5		5
631	13	13		13
643	3	3	3	
647	23	23	23	
659	11	11	11	
683	5	5		5
691	5	5		5
719	31	31	31	
727	13	13		13
739	5	5		5
743	21	$3 \cdot 7$	3 7	
751	15	$3 \cdot 5$	3	5
787	5	5		5
811	7	7	7	
823	9	$3 \cdot 3$	3	
827	7	7	7	
839	33	$3 \cdot 11$	3 11	
859	7	7	7	
863	21	$3 \cdot 7$	3 7	
883	3	3	3	
887	29	29		29
907	3	3	3	
911	31	31	31	
919	19	19	19	
947	5	5		5
967	11	11	11	
971	15	$3 \cdot 5$	3	5
983	27	$3 \cdot 3 \cdot 3$	3	
991	17	17		17
1019	13	13		13

p	$H(-p)$	Factorization	Factors $q \equiv 3 \pmod 4$	Factors $q \equiv 1 \pmod 4$
1031	35	$5 \cdot 7$	7	5
1039	23	23	23	
1051	5	5		5
1063	19	19	19	
1087	9	$3 \cdot 3$	3	
1091	17	17		17
1103	23	23	23	
1123	5	5		5
1151	41	41		41
1163	7	7	7	
1171	7	7	7	
1187	9	$3 \cdot 3$	3 3	
1223	35	$5 \cdot 7$	7	5
1231	27	$3 \cdot 3 \cdot 3$	3	
1259	15	$3 \cdot 5$	3	5
1279	23	23	23	
1283	11	11	11	
1291	9	$3 \cdot 3$	3 3	
1303	11	11	11	
1307	11	11	11	
1319	45	$3 \cdot 3 \cdot 5$	3	5
1327	15	$3 \cdot 5$	3	5
1367	25	$5 \cdot 5$		5
1399	27	$3 \cdot 3 \cdot 3$	3	
1423	9	$3 \cdot 3$	3	
1427	15	$3 \cdot 5$	3	5
1439	39	$3 \cdot 13$	3	13
1447	23	23	23	
1451	13	13		13
1459	11	11	11	
1471	23	23	23	
1483	7	7	7	
1487	37	37		37
1499	13	13		13
1511	49	$7 \cdot 7$	7	
1523	7	7	7	
1531	11	11	11	
1543	19	19	19	
1559	51	$3 \cdot 17$	3	17
1567	15	$3 \cdot 5$	3	5
1571	17	17		17
1579	9	$3 \cdot 3$	3 3	
1583	33	$3 \cdot 11$	3 11	
1607	27	$3 \cdot 3 \cdot 3$	3	
1619	15	$3 \cdot 5$	3	5

p	$H(-p)$	Factorization	Factors $q \equiv 3 \pmod 4$	Factors $q \equiv 1 \pmod 4$
1627	7	7	7	
1663	17	17		17
1667	13	13		13
1699	11	11	11	
1723	5	5		5
1747	5	5		5
1759	27	$3 \cdot 3 \cdot 3$	3	
1783	17	17		17
1787	7	7	7	
1811	23	23	23	
1823	45	$3 \cdot 3 \cdot 5$	3	5
1831	19	19	19	
1847	43	43	43	
1867	5	5		5
1871	45	$3 \cdot 3 \cdot 5$	3	5
1879	27	$3 \cdot 3 \cdot 3$	3	
1907	13	13		13
1931	21	$3 \cdot 7$	3 7	
1951	33	$3 \cdot 11$	3 11	
1979	23	23	23	
1987	7	7	7	
1999	27	$3 \cdot 3 \cdot 3$	3	
2003	9	$3 \cdot 3$	3 3	
2011	7	7	7	
2027	11	11	11	
2039	45	$3 \cdot 3 \cdot 5$	3	5
2063	45	$3 \cdot 3 \cdot 5$	3	5
2083	7	7	7	
2087	35	$5 \cdot 7$	7	5
2099	19	19	19	
2111	49	$7 \cdot 7$	7	
2131	13	13		13
2143	13	13		13
2179	7	7	7	
2203	5	5		5
2207	39	$3 \cdot 13$	3	13
2239	35	$5 \cdot 7$	7	5
2243	15	$3 \cdot 5$	3	5
2251	7	7	7	
2267	11	11	11	
2287	29	29		29
2311	29	29		29
2339	19	19	19	
2347	5	5		5
2351	63	$3 \cdot 3 \cdot 7$	3 7	

p	$H(-p)$	Factorization	Factors $q \equiv 3 \pmod 4$	Factors $q \equiv 1 \pmod 4$
2371	13	13		13
2383	29	29		29
2399	59	59	59	
2411	23	23	23	
2423	33	$3 \cdot 11$	3 11	
2447	37	37		37
2459	19	19	19	
2467	7	7	7	
2503	21	$3 \cdot 7$	3 7	
2531	17	17		17
2539	11	11	11	
2543	35	$5 \cdot 7$	7	5
2551	41	41		41
2579	21	$3 \cdot 7$	3 7	
2591	57	$3 \cdot 19$	3 19	
2647	15	$3 \cdot 5$	3	5
2659	13	13		13
2663	43	43	43	
2671	23	23	23	
2683	5	5		5
2687	51	$3 \cdot 17$	3	17
2699	15	$3 \cdot 5$	3	5
2707	7	7	7	
2711	53	53		53
2719	41	41		41
2731	11	11	11	
2767	21	$3 \cdot 7$	3 7	
2791	39	$3 \cdot 13$	3	13
2803	9	$3 \cdot 3$	3 3	
2819	21	$3 \cdot 7$	3 7	
2843	15	$3 \cdot 5$	3	5
2851	11	11	11	
2879	57	$3 \cdot 19$	3 19	
2887	25	$5 \cdot 5$		5
2903	59	59	59	
2927	31	31	31	
2939	29	29		29
2963	13	13		13
2971	11	11	11	
2999	73	73		73
3011	21	$3 \cdot 7$	3 7	
3019	7	7	7	
3023	47	47	47	
3067	7	7	7	
3079	41	41		41

p	$H(-p)$	Factorization	Factors $q \equiv 3 \pmod 4$	Factors $q \equiv 1 \pmod 4$
3083	13	13		13
3119	69	$3 \cdot 23$	3 23	
3163	9	$3 \cdot 3$	3 3	
3167	53	53		53
3187	7	7	7	
3191	69	$3 \cdot 23$	3 23	
3203	11	11	11	
3251	31	31	31	
3259	9	$3 \cdot 3$	3 3	
3271	27	$3 \cdot 3 \cdot 3$	3	
3299	27	$3 \cdot 3 \cdot 3$	3 3 3	
3307	9	$3 \cdot 3$	3 3	
3319	41	41		41
3323	17	17		17
3331	15	$3 \cdot 5$	3	5
3343	19	19	19	
3347	11	11	11	
3359	69	$3 \cdot 23$	3 23	
3371	21	$3 \cdot 7$	3 7	
3391	37	37		37
3407	57	$3 \cdot 19$	3 19	
3463	19	19	19	
3467	19	19	19	
3491	23	23	23	
3499	11	11	11	
3511	41	41		41
3527	65	$5 \cdot 13$		5 13
3539	23	23	23	
3547	9	$3 \cdot 3$	3 3	
3559	45	$3 \cdot 3 \cdot 5$	3	5
3571	15	$3 \cdot 5$	3	5
3583	29	29		29
3607	19	19	19	
3623	45	$3 \cdot 3 \cdot 5$	3	5
3631	43	43	43	
3643	9	$3 \cdot 3$	3 3	
3659	29	29		29
3671	81	$3 \cdot 3 \cdot 3 \cdot 3$	3	
3691	13	13		13
3719	67	67	67	
3727	31	31	31	
3739	11	11	11	
3767	39	$3 \cdot 13$	3	13
3779	31	31	31	
3803	15	$3 \cdot 5$	3	5

p	$H(-p)$	Factorization	Factors $q \equiv 3 \pmod 4$	Factors $q \equiv 1 \pmod 4$
3823	29	29		29
3847	23	23	23	
3851	25	$5 \cdot 5$		5 5
3863	61	61		61
3907	7	7	7	
3911	83	83	83	
3919	39	$3 \cdot 13$	3	13
3923	23	23	23	
3931	11	11	11	
3943	27	$3 \cdot 3 \cdot 3$	3	
3947	17	17		17
3967	33	$3 \cdot 11$	3 11	
4003	13	13		13
4007	57	$3 \cdot 19$	3 19	
4019	19	19	19	
4027	9	$3 \cdot 3$	3 3	
4051	11	11	11	
4079	85	$5 \cdot 17$		5 17
4091	33	$3 \cdot 11$	3 11	
4099	15	$3 \cdot 5$	3	5
4111	39	$3 \cdot 13$	3	13
4127	49	$7 \cdot 7$	7	
4139	19	19	19	
4159	31	31	31	
4211	23	23	23	
4219	15	$3 \cdot 5$	3	5
4231	51	$3 \cdot 17$	3	17
4243	9	$3 \cdot 3$	3 3	
4259	35	$5 \cdot 7$	7	5
4271	65	$5 \cdot 13$		5 13
4283	21	$3 \cdot 7$	3 7	
4327	19	19	19	
4339	17	17		17
4363	9	$3 \cdot 3$	3 3	
4391	79	79	79	
4423	33	$3 \cdot 11$	3 11	
4447	17	17		17
4451	29	29		29
4463	55	$5 \cdot 11$	11	5
4483	9	$3 \cdot 3$	3 3	
4507	13	13		13
4519	29	29		29
4523	21	$3 \cdot 7$	3 7	
4547	17	17		17
4567	33	$3 \cdot 11$	3 11	

p	$H(-p)$	Factorization	Factors $q \equiv 3 \pmod 4$	Factors $q \equiv 1 \pmod 4$
4583	61	61		61
4591	49	$7 \cdot 7$	7	
4603	7	7	7	
4639	51	$3 \cdot 17$	3	17
4643	13	13		13
4651	17	17		17
4663	33	$3 \cdot 11$	3 11	
4679	91	$7 \cdot 13$	7	13
4691	21	$3 \cdot 7$	3 7	
4703	75	$3 \cdot 5 \cdot 5$	3	5
4723	9	$3 \cdot 3$	3 3	
4751	91	$7 \cdot 13$	7	13
4759	55	$5 \cdot 11$	11	5
4783	23	23	23	
4787	25	$5 \cdot 5$		5 5
4799	63	$3 \cdot 3 \cdot 7$	3 7	
4831	33	$3 \cdot 11$	3 11	
4871	91	$7 \cdot 13$	7	13
4903	27	$3 \cdot 3 \cdot 3$	3	
4919	91	$7 \cdot 13$	7	13
4931	35	$5 \cdot 7$	7	5
4943	55	$5 \cdot 11$	11	5
4951	31	31	31	
4967	59	59	59	
4987	9	$3 \cdot 3$	3 3	
4999	33	$3 \cdot 11$	3 11	
5003	15	$3 \cdot 5$	3	5
5011	21	$3 \cdot 7$	3 7	
5023	25	$5 \cdot 5$		5
5039	83	83	83	
5051	29	29		29
5059	19	19	19	
5087	69	$3 \cdot 23$	3 23	
5099	39	$3 \cdot 13$	3	13
5107	7	7	7	
5119	39	$3 \cdot 13$	3	13
5147	19	19	19	
5167	33	$3 \cdot 11$	3 11	
5171	35	$5 \cdot 7$	7	5
5179	11	11	11	
5227	15	$3 \cdot 5$	3	5
5231	75	$3 \cdot 5 \cdot 5$	3	5
5279	87	$3 \cdot 29$	3	29
5303	55	$5 \cdot 11$	11	5
5323	15	$3 \cdot 5$	3	5

p	$H(-p)$	Factorization	Factors $q \equiv 3 \pmod 4$	Factors $q \equiv 1 \pmod 4$
5347	13	13		13
5351	93	$3 \cdot 31$	3 31	
5387	23	23	23	
5399	79	79	79	
5407	43	43	43	
5419	13	13		13
5431	57	$3 \cdot 19$	3 19	
5443	9	$3 \cdot 3$	3 3	
5471	71	71	71	
5479	43	43	43	
5483	17	17		17
5503	25	$5 \cdot 5$		5
5507	23	23	23	
5519	97	97		97
5527	19	19	19	
5531	23	23	23	
5563	15	$3 \cdot 5$	3	5
5591	99	$3 \cdot 3 \cdot 11$	3 11	
5623	33	$3 \cdot 11$	3 11	
5639	87	$3 \cdot 29$	3	29
5647	21	$3 \cdot 7$	3 7	
5651	31	31	31	
5659	19	19	19	
5683	11	11	11	
5711	109	109		109
5743	29	29		29
5779	13	13		13
5783	53	53		53
5791	33	$3 \cdot 11$	3 11	
5807	65	$5 \cdot 13$		5 13
5827	15	$3 \cdot 5$	3	5
5839	37	37		37
5843	25	$5 \cdot 5$		5 5
5851	21	$3 \cdot 7$	3 7	
5867	21	$3 \cdot 7$	3 7	
5879	101	101		101
5903	73	73		73
5923	7	7	7	
5927	71	71	71	
5939	35	$5 \cdot 7$	7	5
5987	15	$3 \cdot 5$	3	5
6007	27	$3 \cdot 3 \cdot 3$	3	
6011	27	$3 \cdot 3 \cdot 3$	3 3 3	
6043	9	$3 \cdot 3$	3 3	
6047	71	71	71	

p	$H(-p)$	Factorization	Factors $q \equiv 3 \pmod 4$	Factors $q \equiv 1 \pmod 4$
6067	15	$3 \cdot 5$	3	5
6079	57	$3 \cdot 19$	3 19	
6091	15	$3 \cdot 5$	3	5
6131	31	31	31	
6143	41	41		41
6151	59	59	59	
6163	11	11	11	
6199	39	$3 \cdot 13$	3	13
6203	17	17		17
6211	15	$3 \cdot 5$	3	5
6247	43	43	43	
6263	77	$7 \cdot 11$	7 11	
6271	51	$3 \cdot 17$	3	17
6287	51	$3 \cdot 17$	3	17
6299	43	43	43	
6311	89	89		89
6323	21	$3 \cdot 7$	3 7	
6343	33	$3 \cdot 11$	3 11	
6359	101	101		101
6367	37	37		37
6379	17	17		17
6427	9	$3 \cdot 3$	3 3	
6451	17	17		17
6491	31	31	31	
6547	11	11	11	
6551	117	$3 \cdot 3 \cdot 13$	3	13
6563	23	23	23	
6571	15	$3 \cdot 5$	3	5
6599	109	109		109
6607	45	$3 \cdot 3 \cdot 5$	3	5
6619	13	13		13
6659	23	23	23	
6679	55	$5 \cdot 11$	11	5
6691	21	$3 \cdot 7$	3 7	
6703	23	23	23	
6719	105	$3 \cdot 5 \cdot 7$	3 7	5
6763	9	$3 \cdot 3$	3 3	
6779	39	$3 \cdot 13$	3	13
6791	81	$3 \cdot 3 \cdot 3 \cdot 3$	3	
6803	19	19	19	
6823	33	$3 \cdot 11$	3 11	
6827	17	17		17
6863	81	$3 \cdot 3 \cdot 3 \cdot 3$	3	
6871	45	$3 \cdot 3 \cdot 5$	3	5
6883	9	$3 \cdot 3$	3 3	

p	$H(-p)$	Factorization	Factors $q \equiv 3 \pmod 4$	Factors $q \equiv 1 \pmod 4$
6899	35	$5 \cdot 7$	7	5
6907	17	17		17
6911	87	$3 \cdot 29$	3	29
6947	29	29		29
6959	95	$5 \cdot 19$	19	5
6967	33	$3 \cdot 11$	3 11	
6971	45	$3 \cdot 3 \cdot 5$	3 3	5
6983	57	$3 \cdot 19$	3 19	
6991	71	71	71	
7019	43	43	43	
7027	11	11	11	
7039	43	43	43	
7043	23	23	23	
7079	85	$5 \cdot 17$		5 17
7103	77	$7 \cdot 11$	7 11	
7127	79	79	79	
7151	85	$5 \cdot 17$		5 17
7159	65	$5 \cdot 13$		5 13
7187	25	$5 \cdot 5$		5 5
7207	29	29		29
7211	35	$5 \cdot 7$	7	5
7219	15	$3 \cdot 5$	3	5
7243	13	13		13
7247	47	47	47	
7283	25	$5 \cdot 5$		5 5
7307	25	$5 \cdot 5$		5 5
7331	33	$3 \cdot 11$	3 11	
7351	33	$3 \cdot 11$	3 11	
7411	25	$5 \cdot 5$		5 5
7451	35	$5 \cdot 7$	7	5
7459	15	$3 \cdot 5$	3	5
7487	65	$5 \cdot 13$		5 13
7499	33	$3 \cdot 11$	3 11	
7507	11	11	11	
7523	35	$5 \cdot 7$	7	5
7547	15	$3 \cdot 5$	3	5
7559	115	$5 \cdot 23$	23	5
7583	63	$3 \cdot 3 \cdot 7$	3 7	
7591	65	$5 \cdot 13$		5 13
7603	11	11	11	
7607	89	89		89
7639	31	31	31	
7643	29	29		29
7687	29	29		29
7691	43	43	43	

p	$H(-p)$	Factorization	Factors $q \equiv 3 \pmod 4$	Factors $q \equiv 1 \pmod 4$
7699	27	$3 \cdot 3 \cdot 3$	3 3 3	
7703	81	$3 \cdot 3 \cdot 3 \cdot 3$	3	
7723	9	$3 \cdot 3$	3 3	
7727	81	$3 \cdot 3 \cdot 3 \cdot 3$	3	
7759	49	$7 \cdot 7$	7	
7823	75	$3 \cdot 5 \cdot 5$	3	5
7867	11	11	11	
7879	49	$7 \cdot 7$	7	
7883	17	17		17
7907	21	$3 \cdot 7$	3 7	
7919	97	97		97
7927	47	47	47	
7951	51	$3 \cdot 17$	3	17
7963	13	13		13
8011	25	$5 \cdot 5$		5 5
8039	113	113		113
8059	21	$3 \cdot 7$	3 7	
8087	81	$3 \cdot 3 \cdot 3 \cdot 3$	3	
8111	121	$11 \cdot 11$	11	
8123	21	$3 \cdot 7$	3 7	
8147	37	37		37
8167	33	$3 \cdot 11$	3 11	
8171	21	$3 \cdot 7$	3 7	
8179	25	$5 \cdot 5$		5 5
8191	55	$5 \cdot 11$	11	5
8219	35	$5 \cdot 7$	7	5
8231	107	107	107	
8243	21	$3 \cdot 7$	3 7	
8263	43	43	43	
8287	45	$3 \cdot 3 \cdot 5$	3	5
8291	47	47	47	
8311	61	61		61
8363	35	$5 \cdot 7$	7	5
8387	21	$3 \cdot 7$	3 7	
8419	19	19	19	
8423	83	83	83	
8431	59	59	59	
8443	11	11	11	
8447	99	$3 \cdot 3 \cdot 11$	3 11	
8467	15	$3 \cdot 5$	3	5
8527	43	43	43	
8539	17	17		17
8543	97	97		97
8563	9	$3 \cdot 3$	3 3	
8599	63	$3 \cdot 3 \cdot 7$	3 7	

p	$H(-p)$	Factorization	Factors $q \equiv 3 \pmod 4$	Factors $q \equiv 1 \pmod 4$
8623	51	$3 \cdot 17$	3	17
8627	21	$3 \cdot 7$	3 7	
8647	31	31	31	
8663	67	67	67	
8699	35	$5 \cdot 7$	7	5
8707	15	$3 \cdot 5$	3	5
8719	53	53		53
8731	17	17		17
8747	21	$3 \cdot 7$	3 7	
8779	15	$3 \cdot 5$	3	5
8783	73	73		73
8803	9	$3 \cdot 3$	3 3	
8807	81	$3 \cdot 3 \cdot 3 \cdot 3$	3	
8819	49	$7 \cdot 7$	7 7	
8831	109	109		109
8839	77	$7 \cdot 11$	7 11	
8863	29	29		29
8867	27	$3 \cdot 3 \cdot 3$	3 3 3	
8887	43	43	43	
8923	19	19	19	
8951	135	$3 \cdot 3 \cdot 3 \cdot 5$	3	5
8963	29	29		29
8971	19	19	19	
8999	99	$3 \cdot 3 \cdot 11$	3 11	
9007	35	$5 \cdot 7$	7	5
9011	33	$3 \cdot 11$	3 11	
9043	15	$3 \cdot 5$	3	5
9059	39	$3 \cdot 13$	3	13
9067	9	$3 \cdot 3$	3 3	
9091	21	$3 \cdot 7$	3 7	
9103	57	$3 \cdot 19$	3 19	
9127	57	$3 \cdot 19$	3 19	
9151	67	67	67	
9187	21	$3 \cdot 7$	3 7	
9199	51	$3 \cdot 17$	3	17
9203	31	31	31	
9227	25	$5 \cdot 5$		5 5
9239	139	139	139	
9283	11	11	11	
9311	97	97		97
9319	41	41		41
9323	29	29		29
9343	51	$3 \cdot 17$	3	17
9371	49	$7 \cdot 7$	7 7	
9391	55	$5 \cdot 11$	11	5

p	$H(-p)$	Factorization	Factors $q \equiv 3 \pmod 4$	Factors $q \equiv 1 \pmod 4$
9403	11	11	11	
9419	35	$5 \cdot 7$	7	5
9431	91	$7 \cdot 13$	7	13
9439	75	$3 \cdot 5 \cdot 5$	3	5
9463	45	$3 \cdot 3 \cdot 5$	3	5
9467	41	41		41
9479	101	101		101
9491	45	$3 \cdot 3 \cdot 5$	3 3	5
9511	69	$3 \cdot 23$	3 23	
9539	55	$5 \cdot 11$	11	5
9547	13	13		13
9551	129	$3 \cdot 43$	3 43	
9587	23	23	23	
9619	19	19	19	
9623	95	$5 \cdot 19$	19	5
9631	77	$7 \cdot 11$	7 11	
9643	11	11	11	
9679	71	71	71	
9719	133	$7 \cdot 19$	7 19	
9739	13	13		13
9743	105	$3 \cdot 5 \cdot 7$	3 7	5
9767	89	89		89
9787	11	11	11	
9791	119	$7 \cdot 17$	7	17
9803	37	37		37
9811	21	$3 \cdot 7$	3 7	
9839	91	$7 \cdot 13$	7	13
9851	45	$3 \cdot 3 \cdot 5$	3 3	5
9859	21	$3 \cdot 7$	3 7	
9871	49	$7 \cdot 7$	7	
9883	17	17		17
9887	75	$3 \cdot 5 \cdot 5$	3	5
9907	15	$3 \cdot 5$	3	5
9923	25	$5 \cdot 5$		5 5
9931	23	23	23	
9967	39	$3 \cdot 13$	3	13

References

[1] Paulo Ribenboim (1994), Catalan's Conjecture: Are 8 and 9 the Only Consecutive Powers?, Academic Press

[2] Saban Alaca, Kenneth S. Williams, Introductory Algebraic Number Theory, Cambridge University Press

[3] Tauno Metsänkylä, Catalan's Conjecture: Another Old Diophantine Problem Solved, Bulletin of the American Mathematical Society, Volume 41, Number 1, Pages 43-57

[4] K. Inkeri, On Catalan's Conjecture, Journal of Number Theory 34, 142-152 (1990)

[5] Borevich Z.I., Shafarevich I.R., Number theory, 1966, Academic Press

[6] Serge Lang, Algebraic Number Theory

[7] Pierre Samuel, Algebraic theory of numbers

[8] Lawrence C. Washington, Introduction to Cyclotomic Fields