On the Classification of Finite Rings

J. J. P. Schoone, s0815217

July 2012

Bachelor Thesis in Mathematics
Department of Mathematics
Radboud University, Nijmegen
Supervisor: Dr. A. R. P. van den Essen
Second reader: Dr. J. J. T. Berson

In memory of

Frans Clauwens

Abstract

In this thesis we have tried to gather as much material on the classification of finite rings as an undergraduate could grasp. The results we have obtained are probably well-known in the literature.

Some of the minor results are: the fundamental theorem of finite abelian groups, the number of rings of cube-free order, and direct formulas to determine the number of non-commutative rings of cube-free order as well as the number of rings without multiplicative identity of cube-free order.

Results not included, but known are: the number of rings of order p^3, the number of rings of order p^4, the number of rings of order p^5 and as such the number of rings of order n where the highest power in the prime factorization of n is 5. These results are due to (p^3) Antipkin and Elizarov [1] and Corbas and Williams (p^4, p^5) [3][4].

Preface

Like Colin Fletcher wrote in the introduction to his article *"Rings of small order"*, see [8], it is a pity that very little students could not even determine only nine rings of order less than 5. Knowledge of examples is what helps understand definitions, and what better examples are there, than finite examples - except maybe for $\mathbf{Z}$ which is the mother of all rings - since they can be explicitly given.

Perhaps after a little reminder that a ring can be constructed by taking an abelian group and defining a multiplication on that group which is always equal to zero, most students will be able to give the following rings:

$$\{0\}, \mathcal{C}_2(0), \mathcal{C}_3(0), \mathcal{C}_4(0), \mathbf{Z}/2\mathbf{Z}, \mathbf{Z}/3\mathbf{Z}, \mathbf{Z}/4\mathbf{Z},$$

which are already seven of the nine rings asked for. Maybe a student will remember the finite field of order 4, but that still leaves us with only eight of the nine rings. After these eight, the most easy example is $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, so we have found nine of order less than 5.

However, there are still seven more rings to be found of order less than 5. Among these are great examples, we have non-commutative rings, as well as zero-rings and fields. With this thesis I have tried to provide an easily readable text about finite rings and how many of each cube-free order there are.

My interest for this subject was sparked as early as my second year as a Mathematics student at the Radboud Universiteit Nijmegen. That year, I followed a course about group theory by Dr. Clauwens, who sadly passed away about a year ago. Due to his great lectures and well-chosen exercises, this course became one of my favourites, even until today. Later that year, I attended lectures about ring theory and field theory by Dr. van den Essen. These also boosted my interest for abstract algebra even further.

These courses were probably the major drive for me to continue studying mathematics. In September of 2011 I realised that I did not remember enough about groups, so I decided to read more about it. Somehow, I ended up reading Humphreys book about group theory, which made me wonder how many finite rings of every order there are, since the book contains a complete classification of groups of order < 32.

Then I started to think about this subject and eventually showed some of my findings to Dr. van den Essen. He was quite enthusiastic about the subject and urged me to write my thesis about it, instead of the subject I was working on at the time. At first, we were only going to classify finite commutative rings with identity, but as the articles flooded in, I realised that it was, perhaps not easier, but at least more complete, to try and classify all finite rings.

The result of about a half year's research is presented to you in shape of this thesis. I would like to thank Simeon Nieman for helping me create the titlepage and style of this thesis. Even more of my gratitude goes out to my supervisor Arno van den Essen, for making me choose this subject for the thesis as well as helping me understand Shoda's article from 1932, which is in German, as well as many other times I ran into a brick wall with a proof of any kind.

Jan Schoone, July 8th

Contents

Chapter 1

Classifying finite abelian groups

This part of this bachelor thesis will be a classification of finite abelian groups. This will prove to be important in the next part, where we shall classify finite rings. Since a ring is an abelian group with respect to the addition, it is necessary to understand which abelian groups there are. Several interesting results hold for any ring with a certain type of additive group, but now we advance too fast, let us just start with classifying the abelian groups.

1.1 Definitions

To make sure we are all talking about the same structure:

Definition 1. *Let G be a set, with a binary operation $\circ$ on G, $\circ : G \times G \to G$, that satisfies the following conditions:*

- $\mathcal{G}1$ *The operation $\circ$ is associative.*
- $\mathcal{G}2$ *There exists an identity element e for $\circ$.*
- $\mathcal{G}3$ *For each $a \in G$ there exists an inverse element (We shall denote this by a^{-1} or $-a$).*

Then we say $(G, \circ)$ is a **group**. *We shall often omit the $\circ$ altogether if it either does not matter or is clear from the context. We call a group abelian if $\circ$ also satisfies:*

- $\mathcal{G}4$ $\circ(a, b) = \circ(b, a)$

We shall call a group finite, if and only if the set G is finite. Except for some more general results, most of the time we shall only be concerned with finite abelian groups.

We shall now discuss two ways to produce more groups, if given one.

As the first of these, we discuss subgroups. Let $(G, \circ)$ be a group. Let $H \subset G$, then we call H a **subgroup** of G if and only if $(H, \circ|_{H \times H})$ is a group. It is an easy exercise to check that all subgroups of an abelian group are again abelian.

Let $X \subset G$, we shall write $\langle X \rangle$ for the intersection of all subgroups of G that contain X. Since any arbitrary intersection of subgroups again yields a subgroup of G, this is also a subgroup. Another way to construct $\langle X \rangle$, is the following:

define $X^{-1} := \{x^{-1} : x \in X\}$, then $\langle X \rangle$ is the set that one obtains by repeatedly multiplying the elements of $X \cup X^{-1}$. Instead of writing $\langle \{a\} \rangle$, we shall just write $\langle a \rangle$ if the set X is a singleton. We call $\langle X \rangle$ the **subgroup generated by** X.

The second one is a **direct product** of two groups. Let $(G, \circ_G)$ and $(H, \circ_H)$ be groups. Define $\circ_{G \times H} : (G \times H) \times (G \times H) \to G \times H$ by:

$$\circ_{G \times H}((g_1, h_1), (g_2, h_2)) = (\circ_G(g_1, g_2), \circ_H(h_1, h_2)).$$

Then $(G \times H, \circ_{G \times H})$ is a group. We shall frequently just write $G \times H$ if we mean the direct product of G and H. Again it is an easy exercise to check that $G \times H$ is indeed a group, and that if G and H are both abelian, then $G \times H$ is also abelian.

For groups $G_1, \ldots, G_n$, we also have the direct product in a similar way, let $\circ_{G_1}, \ldots, \circ_{G_n}$ denote the operations on the respective groups. We define

$$\circ_d \left((g_1, \ldots, g_n), (g_1', \ldots, g_n')\right) = \left(\circ_{G_1}(g_1, g_1'), \ldots, \circ_{G_n}(g_n, g_n')\right).$$

Then the set $\bigtimes_{i=1}^{n} G_i$ together with $\circ_d$ is also a group. We shall omit the operation $\circ_d$ in our notation unless it is strictly necessary.

Finally, two groups G and H are **isomorphic**, which means that they are essentially equal, if there exists a bijective map $\varphi : G \to H$ such that $\varphi(g_1 \circ_G g_2) = \varphi(g_1) \circ_H \varphi(g_2)$. We then write $G \simeq H$.

For example, for groups G and H, the direct products $G \times H$ and $H \times G$ are isomorphic, by the isomorphism $\varphi : G \times H \to H \times G$, $(x, y) \mapsto (y, x)$.

1.2 Useful results in group theory

A result which is very useful for determining all finite groups of orders p and p^2 is Lagrange's theorem:

Theorem 1.1. *(Lagrange) Let G be a finite group and let H be a subgroup of G. Then the number of distinct left cosets of H in G is equal to $|G|/|H|$.*

Before we shall prove this theorem, let us first recapitulate the notion of a left coset. A **left coset** is denoted by gH and describes the following set:

$$gH = \{gh : h \in H\}.$$

We can similarly define right cosets, but we do not need them here.

Proposition 1.2. *Let* H *be a subgroup of* G*. Define a relation* $\mathcal{R}$ *on* G *by:*

$$x\mathcal{R}y \text{ if and only if } x^{-1}y \in H.$$

Then the relation $\mathcal{R}$ *is an equivalence relation and the equivalence class of a certain* $g \in G$ *is equal to the left coset* gH*.*

Proof. Since H is a subgroup of G, we know that $x^{-1}x = e$ is an element of H. Therefore $x\mathcal{R}x$ for all $x \in G$. This shows that $\mathcal{R}$ is reflexive.

Secondly, suppose $x\mathcal{R}y$, then $x^{-1}y \in H$. Since H is a subgroup, then also $(x^{-1}y)^{-1} = y^{-1}x \in H$. This shows that $\mathcal{R}$ is symmetric.

Thirdly, if both $x\mathcal{R}y$ and $y\mathcal{R}z$, then we have $x^{-1}y \in H$ and $y^{-1}z \in H$. Then since H is a subgroup, we find that also $(x^{-1}y)(y^{-1}z) = x^{-1}z \in H$. This shows that $\mathcal{R}$ is transitive.

So $\mathcal{R}$ is an equivalence relation.

Now let $[g]_{\mathcal{R}}$ denote the equivalence class of g.

If x is equivalent to g, then $g^{-1}x = h$ for some $h \in H$. Therefore $x = gh$ and thus $x \in gH$. Thus $[g]_{\mathcal{R}} \subset gH$.

Conversely, let gh be an element of gH. Since $g^{-1}(gh) = h \in H$ we find that $g\mathcal{R}gh$ and thus that $gh \in [g]_{\mathcal{R}}$. We have now also proven that $gH \subset [g]_{\mathcal{R}}$. □

Proposition 1.3. *Let* G *be a group and let* H *be a subgroup of* G*. Then for every* $g \in G$ *there exists a bijection* ϑ_g *between* H *and* gH*.*

Proof. We define $\vartheta_g : H \to gH$ by $\vartheta_g(h) = gh$. Then the inverse map is given by $\vartheta_{g^{-1}}$. □

Now the proof of Lagrange's theorem is quite simple:

Proof. Define $\mathcal{R}$ on G as above. Then the equivalence classes partition G. But the equivalence classes are precisely the left cosets of H. Also all left cosets have cardinality equal to H. Say that there are k left cosets. Clearly $|G| = k|H|$, and thus the number of left cosets of H is equal to $|G|/|H|$. □

So now we know that for a finite group G, the order of any subgroup H of G divides the order of G. From this we have an easy corollary:

Corollary 1.4. *Let* G *be a finite group. Then the order of any* $g \in G$ *divides the order of* G*.*

Proof. Use Lagrange's theorem, setting $H = \langle g \rangle$. □

Now we are ready to determine the number of groups of order p. Note that we will determine all groups, not just the abelian ones, however this will turn out to be the same.

Corollary 1.5. *Let* p *be a prime integer, and* G *be a group with* p *elements. Then* G *is cyclic.*

Proof. Let $g \in G$ be a non-identity element. By the corollary to Lagrange's theorem, the order of g divides p. Thus the order of g is either 1 or p. It cannot be 1, since g is a non-identity element. Therefore the order of g is p.

But then the order of $\langle g \rangle$ is also p, and thus $\langle g \rangle = G$. Thus G is cyclic. □

There is only one group of order p, which is the cyclic group of order p (which we shall denote by $\mathcal{C}_p$), and thus is abelian. So the first step in the classification of finite abelian groups is made.

Another important result about finite abelian groups is the following, it originates from 1872 and was found by Sylow.

Theorem 1.6. *(Sylow, 1872) Let G be a finite group of order $p^m q$ such that p is a prime integer that does not divide q. Then there exists a subgroup of G of order p^m. Such a group is called a Sylow p-subgroup.*

For a proof of this theorem, see for example [2] chapter 7, or [10] chapter 11. The following result is a direct corollary of Sylow's theorem.

Proposition 1.7. *Let G be a finite abelian group of order $n = p_1^{e_1} \cdots p_k^{e_k}$, then G is isomorphic to $G_1 \times \ldots \times G_k$, where $|G_i| = p_i^{e_i}$ for each $1 \leqslant i \leqslant k$ and each G_i is a subgroup of G.*

Proof. Clearly, a subgroup G_i of order $p_i^{e_i}$ exists, due to Sylow's theorem.

Since each G_i is a group, we know that the elements $g \in G_i$ all follow the rule:

$$|G_i| g = 0.$$

In particular, $p_i^{e_i} g = 0$ for each $g \in G_i$.

Now we need to show that all the $G_i \cap G_j$ are trivial and we have proven our result:

Let $g_i \in G_i$ and $g_j \in G_j$ for $i \neq j$. Then $p_i^{e_i} g_i g_j = p_j^{e_j} g_i g_j = 0$. Since $\gcd(p_i, p_j) = 1$, we also find that $\gcd(p_i^{e_i}, p_j^{e_j}) = 1$. Therefore, there exist $c, d \in \mathbf{Z}$ such that $p_i^{e_i} c + p_j^{e_j} d = 1$.

Now multiply both sides of this equation by $g_i g_j$ and we find that $g_i g_j = 0$.

Hence, $H := G_1 G_2 \cdots G_k$ is a subgroup of G with $p_1^{e_1} \cdots p_k^{e_k} = n$ elements, with $H \simeq G_1 \times \ldots \times G_k$. Since both H and G have n elements, we find that $H = G$.

Thus clearly $G \simeq G_1 \times \ldots \times G_k$. □

In the next section we shall state an excellent theorem for classifying finite abelian groups, in the section thereafter, we shall make this classification.

1.3 Fundamental theorem on finite abelian groups

The main result of this part of the thesis is the theorem that classifies all finite abelian groups. It is called the fundamental theorem on finite abelian groups, and was first discovered by Kronecker in 1870:

Theorem 1.8. *(Fundamental theorem on finite abelian groups) Let* G *be a finite abelian group. Then there exists a unique decomposition of* G *of the form:*

$$\mathcal{C}_{n_1} \times \mathcal{C}_{n_2} \times \ldots \times \mathcal{C}_{n_r}$$

where each n_j *divides* n_i *for* $j > i$ *with* $n_r \geqslant 2$*, and* $|G| = n_1 n_2 \cdots n_r$.

This requires quite an extensive proof involving quite a few steps. We shall sketch the outline of the proof, for the statements without proof, we refer to [10].

We first define a p**-group** as a group for which each element has order a power of p.

Proposition 1.9. *Let* G *be a finite abelian* p*-group of order* p^n*. Then* G *is a direct product of cyclic subgroups of orders* $p^{e_1}, p^{e_2}, \ldots, p^{e_r}$ *where* $e_1 \geqslant e_2 \geqslant \ldots \geqslant e_r \geqslant 1$ *and* $e_1 + e_2 + \ldots + e_r = n$.

Corollary 1.10. *A finite abelian group* G *of order* n *can be written as a direct product* $\mathcal{C}_{n_1} \times \ldots \times \mathcal{C}_{n_r}$*, where* n_j *divides* n_i *for* $j > i$ *and* $n_r \geqslant 2$*. Obviously* $n_1 n_2 \ldots n_r = n$.

Proof. First, use Proposition 1.7 to write G as a direct product of its subgroups.

Each of these subgroups can be rewritten by Proposition 1.9 as a direct product of cyclic groups.

Claim: Let $k_1, \ldots, k_s$ be any sequence of integers each of which is greater than 1, such that $\gcd(k_i, k_j) = 1$ for $i \neq j$. Then $\mathcal{C}_{k_i} \times \ldots \times \mathcal{C}_{k_s}$ is cyclic of order $k_1 k_2 \cdots k_s$.

We use our claim repeatedly on the first factor of each subgroup to obtain a cyclic factor of G. Then we use this claim repeatedly on the second factor of those subgroups that are not cyclic to obtain the second cyclic factor of G. Continuing in this way completes the proof. □

Now we have proven existence, but not yet uniqueness, which will again be quite some work. Like Humphreys did in [10], we shall say that a finite abelian p-group G is of type $(e_1, e_2, \ldots, e_r)$ if $G \simeq \mathcal{C}_{p^{e_1}} \times \ldots \times \mathcal{C}_{p^{e_r}}$ and $e_1 \geqslant e_2 \geqslant \ldots \geqslant e_r \geqslant 1$.

Proposition 1.11. *Let* p *be a prime integer. For any finite abelian group* G*, the subset* G_p *of* G *consisting of elements of order* 1 *or* p *is a subgroup of* G*. Also the subset* G^p *of* p*-th powers of elements of* G *is a subgroup of* G.

Let G *be an abelian* p*-group of type* $(e_1, \ldots, e_r)$*, with* t *the largest integer such that* $e_t > 1$*. Then* G *has order* p^r*, and* G^p *has type* $(e_1 - 1, \ldots, e_t - 1)$.

Proposition 1.12. *Suppose that* G *is an abelian* p*-group. Then the type of* G *is uniquely determined. Thus, if* G *is of type* $(e_1, \ldots, e_r)$ *and also of type* $(f_1, \ldots, f_s)$*, then* $r = s$ *and* $e_i = f_i$ *for* $1 \leqslant i \leqslant r$.

Now we have done enough work to prove uniqueness for the fundamental theorem of finite abelian groups.

Proof. Recall that from Corollary 1.10 we have existence. Now for the uniqueness, note that for each prime integer p dividing the order of G, the Sylow p-subgroup of G is $S_p(\mathcal{C}_{n_1}) \times \ldots \times S_p(\mathcal{C}_{n_r})$, where $S_p(K)$ denotes the Sylow p-subgroup of the abelian group K. Now apply the last proposition to this decomposition. □

We now have all we need to determine *all* finite abelian groups of any order.

1.4 Classification of finite abelian groups

In this section we shall state many corollaries to the fundamental theorem on finite abelian groups, in order to classify all finite abelian groups. From the second section, we already have:

Corollary 1.13. *Let G be a finite abelian group of order p, where p is a prime integer. Then $G \simeq \mathcal{C}_p$.*

Proof. This follows directly from Corollary 1.5. □

Now we shall start to grasp the power of the fundamental theorem on finite abelian groups. We shall determine a great many of abelian groups.

Corollary 1.14. *Let G be a finite abelian group of order p^2, where p is a prime integer. Then either $G \simeq \mathcal{C}_{p^2}$ or $G \simeq \mathcal{C}_p \times \mathcal{C}_p$.*

Proof. This follows directly from the Fundamental theorem of finite abelian groups. □

Corollary 1.15. *Let p, q be distinct prime integers and let G be a finite abelian group of order pq. Then $G \simeq \mathcal{C}_{pq}$.*

Proof. This follows directly from the Fundamental theorem of finite abelian groups. □

Corollary 1.16. *Let $n = p_1 \cdot p_2 \cdots p_k$, where all p_i are distinct primes for $1 \leqslant i \leqslant k$ and let G be a finite abelian group of order n. Then $G \simeq \mathcal{C}_n$.*

Proof. This follows directly from the Fundamental theorem of finite abelian groups. □

So for all squarefree numbers we have determined the number of abelian groups of that order: if n is a square free integer, then there exists only one abelian group of that order up to isomorphism.

Corollary 1.17. *Let p, q be distinct prime integers and let G be a finite abelian group of order p^2q. Then $G \simeq \mathcal{C}_{p^2q}$ or $\mathcal{C}_{pq} \times \mathcal{C}_p$.*

Proof. This follows directly from the Fundamental theorem of finite abelian groups. □

Corollary 1.18. *Let* p *be a prime integer and let* G *be a finite abelian group of order* p^3*. Then* $G \simeq \mathcal{C}_{p^3}, G \simeq \mathcal{C}_{p^2} \times \mathcal{C}_p$ *or* $G \simeq \mathcal{C}_p \times \mathcal{C}_p \times \mathcal{C}_p$.

Proof. This follows directly from the Fundamental theorem of finite abelian groups. □

Corollary 1.19. *Let* p *and* q *be distinct prime integers and let* G *be a finite abelian group of order* p^2q^2*. Then* $G \simeq \mathcal{C}_{p^2q^2}, G \simeq \mathcal{C}_{pq^2} \times \mathcal{C}_p, G \simeq \mathcal{C}_{p^2q} \times \mathcal{C}_q$ *or* $G \simeq \mathcal{C}_{pq} \times \mathcal{C}_{pq}$.

Proof. This follows directly from the Fundamental theorem of finite abelian groups. □

Corollary 1.20. *Let* p *be a prime integer and let* G *be a finite abelian group of order* p^4*. Then* $G \simeq \mathcal{C}_{p^4}, G \simeq \mathcal{C}_{p^3} \times \mathcal{C}_p, G \simeq \mathcal{C}_{p^2} \times \mathcal{C}_{p^2}, G \simeq \mathcal{C}_{p^2} \times \mathcal{C}_p \times \mathcal{C}_p$ *or* $G \simeq \mathcal{C}_p \times \mathcal{C}_p \times \mathcal{C}_p \times \mathcal{C}_p$.

Proof. This follows directly from the Fundamental theorem of finite abelian groups. □

Corollary 1.21. *Let* p *and* q *be distinct prime integers and let* G *be a finite abelian group of order* p^3q. *Then* $G \simeq \mathcal{C}_{p^3q}, G \simeq \mathcal{C}_{p^2q} \times \mathcal{C}_p$ *or* $G \simeq \mathcal{C}_{pq} \times \mathcal{C}_p \times \mathcal{C}_p$.

Proof. This follows directly from the Fundamental theorem of finite abelian groups. □

For further reference we have included a table containing the number of groups for each integer $1 \leqslant n \leqslant 30$. [1]

[1] The numbers in the last column are taken from [10]

		# abelian groups	# groups
1		1	1
2	p	1	1
3	p	1	1
4	p^2	2	2
5	p	1	1
6	pq	1	2
7	p	1	1
8	p^3	3	5
9	p^2	2	2
10	pq	1	2
11	p	1	1
12	p^2q	2	5
13	p	1	1
14	pq	1	2
15	pq	1	1
16	p^4	5	14
17	p	1	1
18	p^2q	2	5
19	p	1	1
20	p^2q	2	5
21	pq	1	2
22	pq	1	2
23	p	1	1
24	p^3q	3	15
25	p^2	2	2
26	pq	1	2
27	p^3	3	5
28	p^2q	2	4
29	p	1	1
30	pqr	1	4

Chapter 2

Classifying finite rings

2.1 Definitions

Definition 2. *Let* R *be a set, with two binary operation on* R*, which we shall conveniently call addition,* $+ : R \times R \to R$*, and multiplication,* $\cdot : R \times R \to R$*, that satisfy the following conditions:*

$\mathcal{R}1$. *Both operations are associative.*

$\mathcal{R}2$. *The multiplication is (left- and right-)distributive over addition.*

$\mathcal{R}3$. *The addition is commutative.*

$\mathcal{R}4$. *There exists a zero-element in* R *for the addition.*

$\mathcal{R}5$. *For each* $a \in R$ *there exists an additive inverse in* R.

We shall then call the triple $(R, +, \cdot)$ *a* **ring**.

A ring $(R, +, \cdot)$*, is called a* **ring with identity***, if and only if, there exists an identity-element for the multiplication. (i.e. there exists a* $1 \in R$ *such that* $1 \cdot a = a \cdot 1 = a$ *for all* $a \in R$*.).*

A ring $(R, +, \cdot)$ *is called a* **commutative ring***, if and only if, the multiplication is commutative.*

A ring $(R, +, \cdot)$ *is called a* **division ring***, if and only if it is a ring with identity, such that each element has a multiplicative inverse.*

Finally, a ring $(R, +, \cdot)$ *is called a* **field***, if and only if it is a commutative division ring.*

Like in the part about finite abelian groups, we define the **direct (ring) product** of two rings, by taking the Cartesian product of the sets, and defining the addition and multiplication componentwise. It is an easy exercise to check that the direct (ring) product of two rings is again a ring. We shall denote the direct product of the rings R and S by $R \times S$.

Furthermore, it is also quite easy to see that $R \times S$ is only commutative if R and S are, and that $R \times S$ has a multiplicative identity if and only if both R and S have a multiplicative identity. Since for each $a \in R$, the element $(a, 0_S)$ is a zero-divisor, $R \times S$ will never be a field.

The direct product of multiple rings $R_1, \dots, R_n$ is denoted as $\bigtimes_{i=1}^{n} R_i$.

Again, we can define **subrings**, like we did with subgroups. Let R be a ring and $T \subset R$, then T is a subring of R if and only if T is a ring with respect to the addition and multiplication of R. A special kind of subrings are **ideals**. An ideal I is a subring of R such that for each $r \in R$ we have $rI \subset I$.

We shall speak of the **additive group of a ring** $(R, +, \cdot)$, by which we shall mean the pair $(R, +)$. It is seen by definition that this forms an abelian group. Thus rings are actually abelian groups with a second operation, that follows certain rules.

Here again we are only interested in finite rings, which thus have finite abelian groups. An example of a finite ring is $\mathbf{Z}/4\mathbf{Z}$, the ring of integers modulo 4.

We shall call two rings R and S **isomorphic** if and only if there exists a bijective map φ from R to S that satisfies the following rules:

$$\varphi(a+b) = \varphi(a) + \varphi(b);$$
$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$$

both for all $a, b \in R$. This map φ is called an **isomorphism**. If φ only satisfies the two conditions, but is not bijective, it is called a **(ring)-homomorphism**.

Sometimes, it will take quite some room to write down what the operations do. Therefore, like Benjamin Fine did in [7], we shall write down a **ring presentation**. This will even replace the notation $(R, +, \cdot)$. A ring representation will look somewhat like this:

$$\langle g_1, \dots, g_k \mid m_i g_i = 0 \text{ for } i \in \{1, \dots, k\},\ g_i g_j = \sum_{t=1}^{k} c_{ij}^t g_t \text{ for } i, j \in \{1, \dots, k\}, c_{ij} \in \mathbf{Z}/m_t\mathbf{Z}\rangle.$$

Here the g_i are the generators of the additive group of the ring. Clearly, since the entire ring is finite, the additive group is finite, and thus there are only finitely many generators. The relation $m_i g_i = 0$ denotes the order of each generator, m_i is a positive integer. The products $g_i g_j = \sum_{t=1}^{k} c_{ij}^t g_t$ are actual ring products, the coefficients $c_i j^t$ range from 0 to $m_t - 1$.

Since we have determined all products of generators, we have defined the entire ring.

In reality, a ring presentation will be even shorter, since, if a product $g_i g_j$ follows from other products already included, we shall omit it. To clarify all this, an example.

Example. *We consider the ring* $\mathbf{Z}/4\mathbf{Z}$ *of integers modulo* 4. *Its presentation is given by:*

$$\langle \overline{1} \mid 4 \cdot \overline{1} = \overline{0},\ \overline{1}^2 = \overline{1}\rangle.$$

We see here that $2 \cdot \overline{1}$ *and* $3 \cdot \overline{1}$ *are elements that differ from* $\overline{1}$ *and* $\overline{0}$. *The additive table can now be easily constructed. The multiplicative table relies heavily on this, due to the distributivity laws. From this and* $\overline{1}^2 = \overline{1}$ *one can deduce this entire table as well.*

Furthermore, it can be shown by an easy construction that any ring given by $\langle a \mid 4a = 0,\ a^2 = a \rangle$ is isomorphic to $\mathbf{Z}/4\mathbf{Z}$.

2.2 Useful results in ring theory

We begin with a very useful result, which was first proven in [13] in 1930. It is useful in determining the number of rings of a certain order, as we shall see in Theorem 2.9.

Proposition 2.1. *(Shoda, 1930) Let $n = p_1^{e_1} \cdots p_k^{e_k}$, then each ring of order n can be uniquely written as the direct product of subrings $R_1, \dots, R_k$ of orders $p_1^{e_1}, \dots, p_k^{e_k}$.*

Proof. Let R be such a ring. Then we have by Proposition 1.7 that the abelian group of R can be decomposed in subgroups of prime power order. Let us call these $R_1, \dots, R_k$.

Now we see that R_1 consists of the elements r of R for which $p_1^{e_1} r = 0$ holds. Similarly for all other $1 < i \leqslant k$. It is then clear that each R_i is a ring.

The last thing we need to observe, is that if $i \neq j$ and $r_i \in R_i, r_j \in R_j$ that $r_i r_j = 0$.

This follows a similar argument as the proof of Proposition 1.7.

Thus clearly, R is the direct product of the rings $R_1, \dots, R_k$. □

Since a large class of abelian groups is the class of cyclic groups, the following proposition will come in handy when we are determining which rings we have found are commutative.

Proposition 2.2. *Let R be a ring with cyclic additive group. Then R is commutative.*

Proof. A cyclic group has a single generator, say a. Then each element in R is of the form ka for a certain $k \in \mathbf{Z}$, where

$$ka = \underbrace{a + a + \cdots + a}_{k \text{ times}}.$$

Let $g, h \in R$, then $g = k_1 a$ and $h = k_2 a$. Then

$$g \cdot h = k_1 a \cdot k_2 a = (k_1 k_2) a^2,$$

while

$$h \cdot g = k_2 a \cdot k_1 a = (k_2 k_1) a^2.$$

Since $\mathbf{Z}$ is a commutative ring, we find that also R is commutative. □

Remark. *We can characterize a finite ring of order n with cyclic additive group, just by stating what a^2 is. Here a is a generator of the additive group. We see that $a^2 = ka$ where k is an integer with $1 \leqslant k \leqslant n$. These two integers n, k determine the ring uniquely, since $k_1 a \cdot k_2 a = k_1 k_2 a^2 = k_1 k_2 k a$.*

For rings with cyclic additive group, we know that they are all commutative. We shall now show that there also exist finite non-commutative rings. In [11] MacCluer and Wilson posed the question “What is the order of the smallest noncommutative ring?”, to which in [12], half a year later, the answer (namely, that order is 4) was given by various individuals, including G.A. Heuer, who in return asked if there exist finite noncommutative rings with identity, and if they exist, what the order of the smallest one is.

Three years later, in [6], Erickson proved the following theorem, which states exactly for which orders a non-commutative rings exists.

Theorem 2.3. *(Erickson, 1966) Let $n \in \mathbf{Z}_{>0}$, then there exists a non-commutative ring of order n if and only if n is not squarefree.*

Proof. $\Leftarrow$:) Let n be a squarefree number. Then the only abelian group of that order is $\mathcal{C}_n$, see Corollary 1.16. Hence the additive group of a ring of this order has to be cyclic, so we see that a ring of squarefree order is always commutative by Proposition 2.2.

$\Leftarrow$:) This consists of two parts, just like the proof of Erickson himself. We first construct a non-commutative ring of order p^2 and then use this to show that there exists a non-commutative ring of order kp^2 for each $k \in \mathbf{Z}$.

First, the construction of a non-commutative ring R of order p^2. We now know that the additive group of R has to be $\mathcal{C}_p \times \mathcal{C}_p$, since otherwise, R would be commutative. Let a be such that $\langle a \rangle \simeq \mathcal{C}_p$, then $\langle (a,0),(0,a) \rangle \simeq \mathcal{C}_p \times \mathcal{C}_p$.

We define multiplication as follows:

$$\begin{aligned}(a,0)(a,0) = (a,0)(0,a) = (a,0);\\ (0,a)(0,a) = (0,a)(a,0) = (0,a).\end{aligned}$$

Then, from the distributive laws, it follows that:

$$\begin{aligned} & (ka,la)(ra,sa) \\ = \;& \left(\underbrace{(a,0)+\ldots+(a,0)}_{k \text{ times}} + \underbrace{(0,a)+\ldots+(0,a)}_{l \text{ times}} \right) \left(\underbrace{(a,0)+\ldots+(a,0)}_{r \text{ times}} + \underbrace{(0,a)+\ldots+(0,a)}_{s \text{ times}} \right) \\ = \;& k(r+s)(a,0) + l(r+s)(0,a) \\ = \;& (k(r+s)a, l(r+s)a) \end{aligned}$$

While on the other hand, $(ra,sa)(ka,la) = (r(k+l)a, s(k+l)a)$, this is verified similarly. Clearly this multiplication is not commutative. The associative law is an easy exercise to check. Thus we have constructed a ring of order p^2.

We now define a non-commutative ring of order kp^2 by setting $T = \mathbf{Z}/k\mathbf{Z} \times R$, where R is the ring of order p^2 defined above. This is a ring, since the direct product of two rings is again a ring. This ring T is non-commutative, since if it were, then R would be, since it is isomorphic to a subring of T. □

A good two years later, an answer to Heuer's question came in the form of [5] by Eldridge who proved:

Theorem 2.4. *(Eldridge, 1968) Let* R *be a finite ring of order* m *with identity. If* m *is cube free, then* R *is commutative.*

Here we shall follow his proof, and thus first state and prove a lemma:

Lemma 2.5. *Let* R *be a finite ring of order* p^n *with identity* e*, where* p *is a prime. If* $n < 3$*, then* R *is commutative.*

Proof. For $n = 0$, since there exists only one ring of that order, the trivial ring.

For $n = 1$, we have a ring of order p. We know there exists only 1 abelian group of that order, which is cyclic (see Corollary 1.13). Furthermore, we know form Proposition 2.2 that all rings of order p have to be commutative.

For $n = 2$, we have a ring of order p^2. There exist two abelian groups of that order, one of which is cyclic, the other is isomorphic to $\mathcal{C}_p \times \mathcal{C}_p$. In the first case, we again have that those rings are commutative, since the additive group is cyclic.

The second case is slightly harder. We know that $\mathcal{C}_p \times \mathcal{C}_p$ is generated by two elements. We can choose e to be one of those generators.

We have the following presentation for such a ring:

$$\langle e, a : pe = pa = 0,\ e^2 = e,\ ae = ea = a,\ a^2 =?\rangle.$$

We have multiple options for a^2, so we are not yet done. However, we know that for each $r \in R$ there exist certain $k_1, k_2 \in \mathbf{Z}$ such that $r = k_1e + k_2a$. Now let $r, s \in R$ be two elements.

Then

$$\begin{aligned} r \cdot s &= (k_1e + k_2a) \cdot (l_1e + l_2a) \\ &= k_1l_1e + k_1l_2a + k_2l_1a + k_2l_2a^2 \\ &= l_1k_1e + l_1k_2a + l_2k_1a + l_2k_2a^2 \\ &= (l_1e + l_2a) \cdot (k_1e + k_2a) \\ &= s \cdot r. \end{aligned}$$

Thus R is commutative. □

We are now ready for the proof of Eldridge's theorem.

Proof. Let R be a ring with identity of order m with m cube-free. Thus $m = p_1^{e_1} \cdots p_k^{e_k}$ with $e_1, \ldots, e_k < 3$.

By Theorem 2.1 we find that R is isomorphic to a direct product of rings $R_1, \ldots, R_k$ for which $|R_i| = p_i^{e_i}$ holds.

We know that R has an identity if and only if each R_i has an identity, thus each R_i has an identity.

Now by the above Lemma, since $e_i < 3$, each R_i is commutative. Then certainly R is commutative, since a direct product of commutative rings is again commutative. □

2.3 Main theorems

We want to determine the number of rings, up to isomorphism, of order n, where n is a positive integer. We shall denote this by $\mathfrak{R}(n)$.

The first of our theorems determines how many non-isomorphic rings there are with a cyclic additive group.

It was given in [14] by Waterhouse as an answer to problem 5100 "To within isomorphism, find the number of rings there are whose additive group is cyclic of order m." posed by Seth Warner in *The American Mathematical Monthly* in 1963, but another solution is mentioned by Heuer and Erickson, who found it in [9] by Fuchs.

Theorem 2.6. *(Waterhouse, 1964) Let A and B be rings with additive group $\mathcal{C}_n$ generated by a and b respectively, where $a^2 = ka$ and $b^2 = lb$. If $\gcd(k, n) = \gcd(l, n)$, then and only then are A and B isomorphic.*

Proof. The map $\varphi : A \to B,\ a \mapsto mb$ is an isomorphism if and only if $\gcd(m, n) = 1$ and $mk \equiv l \mod n$, since:

Let $a_1, a_2 \in A$, then $a_1 = k_1 a$ and $a_2 = k_2 a$.

Then $\varphi(a_1 + a_2) = \varphi(k_1 a + k_2 a) = \varphi((k_1 + k_2)a) = m(k_1 + k_2)b = k_1 mb + k_2 mb$.

And $\varphi(a_1 a_2) = \varphi(k_1 a k_2 a) = \varphi(k_1 k_2 a^2) = \varphi(k_1 k_2 k a) = mk_1 k_2 kb$.

This is equal to $k_1 k_2 b^2$ for all k_1 and k_2 if and only if $mk \equiv l \mod n$.

Now φ is surjective if and only if we can find a certain $k_1 \in \mathbf{Z}$ such that $\varphi(k_1 a) = b$. But we know that $\varphi(k_1 a) = mk_1 b$. Thus φ is surjective if and only if $mk_1 \equiv 1 \mod n$, which is equivalent to $\gcd(m, n) = 1$.

Thus we have found that there exists an isomorphism from A to B if and only if there exists an m such that $mk \equiv l \mod n$ and $\gcd(m, n) = 1$.

Now it remains for us to show that there exists such an m with $\gcd(m, n) = 1$ and $mk \equiv l \mod n$ if and only if $\gcd(k, n) = \gcd(l, n)$.

$\Rightarrow$:) We know that $\gcd(k, n)$ divides k and n, hence also mk and therefore $\gcd(k, n)$ divides l. Thus $\gcd(k, n)$ divides $\gcd(l, n)$.

Similarly, $\gcd(l, n)$ divides l and n, hence also mk. Since $\gcd(m, n) = 1$, we see that $\gcd(l, n)$ divides k. Thus $\gcd(l, n)$ divides $\gcd(k, n)$.

$\Leftarrow$:) First, suppose that $\gcd(k, n) = \gcd(l, n) = 1$. Then there exists an inverse for k in $\mathbf{Z}/n\mathbf{Z}$. We can set $m = k^{-1}l$ to obtain both $mk \equiv l \mod n$ and $\gcd(m, n) = 1$.

Now say $\gcd(k, n) = \gcd(l, n) = d$. Then we know that $\gcd(\frac{k}{d}, \frac{n}{d}) = \gcd(\frac{l}{d}, \frac{n}{d}) = 1$, for which we know that there exists an m such that $\gcd(m, \frac{n}{d}) = 1$ and $m\frac{k}{d} \equiv \frac{l}{d} \mod \frac{n}{d}$.

But clearly then also $mk \equiv l \mod n$. But $\gcd(m, n) = 1$ if and only if d does not divide m. We have two cases, either d does not divide m, or d does divide m. Then we say $m' = m + \frac{n}{d}$, then we find that d does not divide $\frac{n}{d}$ since $\gcd(m, \frac{n}{d}) = 1$, and as such that d does not divide m. Clearly m' still satisfies the relation $mk \equiv l \mod n$. □

We shall mention a direct corollary to this theorem before advancing to the next one.

Corollary 2.7. *The number of rings R, up to isomorphism, with cyclic additive group $\mathcal{C}_n$ is given by the number of divisors of n.*

For each number n, it is now very easy to calculate the number of rings that have cyclic additive group of order n.

Example. *Let $n = 6,469,693,230$, then we can also write $n = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29$, thus the number of rings of order $6,469,693,230$ (with cyclic additive group) is equal to $2^{10} = 1,024$. However, there is only 1 ring of this order that has a multiplicative identity. Note that by Corollary 1.16 the only abelian group of this order is cyclic, so we have in fact determined* all *rings of order n.*

Proposition 2.8. *Let R be a ring with additive group $\mathcal{C}_n$, such that R has a multiplicative identity. Then $R \simeq \mathbf{Z}/n\mathbf{Z}$.*

Proof. Suppose R is such a ring, say $\mathcal{C}_n$ is generated by a. We let $a^2 = ka$ for some $k \in \mathbf{Z}$. Since R has an identity, there exists a $j \in \mathbf{Z}$ such that ja is the multiplicative identity of R.

So now we have the following:

$$a = (ja)a = ja^2 = jka.$$

Clearly, $jk \equiv 1 \mod n$, and therefore $\gcd(k, n) = 1$.

Therefore $\gcd(k, n) = \gcd(1, n)$. So the ring R is isomorphic to a ring for which $a^2 = a$ holds (by Waterhouse's Theorem). But any ring for which $a^2 = a$ holds, is precisely $\mathbf{Z}/n\mathbf{Z}$, and there is no other, by the Remark on page 13. □

An important theorem about ring classification is the following:

Theorem 2.9. *Let $n = p_1^{e_1} \cdots p_k^{e_k}$ be a positive integer. Then $\mathfrak{R}(n) = \mathfrak{R}(p_1^{e_1}) \cdots \mathfrak{R}(p_k^{e_k})$, here $\mathfrak{R}(n)$ denotes the number of rings, up to isomorphism, of order n.*

Proof. We have by Proposition 2.1 that any ring of order $n = p_1^{e_1} \cdots p_k^{e_k}$ can be written as a direct product of subrings of orders $p_1^{e_1}, \ldots, p_k^{e_k}$. The number of subrings of order $p_i^{e_i}$ is equal to $\mathfrak{R}(p_1^{e_1})$. The number of non-isomorphic products of subrings with the above requirements is thus equal to $\mathfrak{R}(p_1^{e_1}) \cdots \mathfrak{R}(p_k^{e_k})$. Therefore there are that many rings of order n. □

2.4 Classification of finite rings

By Theorem 2.6 we have the following corollaries.

Corollary 2.10. *The number of rings* R*, up to isomorphism, with cyclic additive group* $\mathcal{C}_n$ *is given by the number of divisors of* n*.*

Corollary 2.11. *If* p *is a prime, then there are, up to isomorphism, exactly two rings of order* p*.*

Proof. Since the only abelian group of order p is cyclic, see Corollary 1.13, the statement follows from the Corollary 2.10, since the only divisors of p are 1 and p. □

These rings are equal to $\langle a : pa = 0,\ a^2 = a\rangle$ and $\langle a : pa = 0,\ a^2 = 0\rangle$. The first is a ring known to many, $\mathbf{Z}/p\mathbf{Z}$, the second one, is the ring where all products are designed to be 0, we write $\mathcal{C}_p(0)$ for this ring, since the additive group of this zero-ring is $\mathcal{C}_p$.

Corollary 2.12. *If* p *and* q *are distinct primes, then there are, up to isomorphism, exactly four rings of order* pq*.*

Proof. Since the only abelian group of order pq is cyclic, see Corollary 1.15, the statement follows by Corollary 2.10, since the only divisors of pq are $1, p, q$ and pq. □

These two results are special cases of the following:

Corollary 2.13. *If* $n = p_1 p_2 \cdots p_r$*, where all* p_i *are distinct primes, then there are, up to isomorphism, exactly* 2^r *rings of order* n*.*

Proof. Since the only abelian group of order n is cyclic, see Corollary 1.16, the statement follows by Corollary 2.10, since n has 2^r divisors. □

We have now determined all rings of square-free order, and have witnessed that they are all commutative.

Before we can determine the number of rings with cube-free order, we have to determine the number of rings of order p^2. We then use Theorem 2.9 to determine the number of all rings of cube-free order.

We recall that there are two abelian groups of order p^2, $\mathcal{C}_{p^2}$ and $\mathcal{C}_p \times \mathcal{C}_p$. We can split the rings of order p^2 in two categories, the rings with additive group $\mathcal{C}_{p^2}$ and the rings with additive group $\mathcal{C}_p \times \mathcal{C}_p$.

The number of rings in the first category is equal to 3, by Corollary 2.10. What is left is to determine the number of rings with additive group $\mathcal{C}_p \times \mathcal{C}_p$.

Proposition 2.14. *Let* p *be a prime number. Then the number of rings with additive group* $\mathcal{C}_p \times \mathcal{C}_p$ *is equal to* 8*.*

We omit the proof of this Proposition, but in turn prove the following, which implies it. The theorem in this form is given by Fine in [7] in 1993, we shall follow the outline of his proof.

Theorem 2.15. *(Fine, 1993) For any prime number* p *there are exactly* 11 *rings of order* p^2*, namely:*

$$\begin{aligned}
A &= \mathbf{Z}/p^2\mathbf{Z}\\
B &= \langle a : p^2a = 0, a^2 = pa\rangle\\
C &= \mathcal{C}_{p^2}(0)\\
D &= \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}\\
E &= \langle a, b : pa = pb = 0, a^2 = a, b^2 = b, ab = a, ba = b\rangle\\
F &= \langle a, b : pa = pb = 0, a^2 = a, b^2 = b, ab = b, ba = a\rangle\\
G &= \langle a, b : pa = pb = 0, a^2 = 0, b^2 = b, ab = ba = a\rangle\\
H &= \mathbf{Z}/p\mathbf{Z} \times \mathcal{C}_p(0)\\
I &= \langle a, b : pa = pb = 0, a^2 = b, ab = 0\rangle\\
J &= (\mathcal{C}_p \times \mathcal{C}_p)(0)\\
K &= \mathbb{F}_{p^2}
\end{aligned}$$

Proof. The first three rings are the rings of order p^2 with additive group $\mathcal{C}_{p^2}$. That these are non-isomorphic follows from Waterhouse's theorem.

It is clear that rings with non-isomorphic additive groups are not isomorphic, since a ring-homomorphism consists of a group-homomorphism with an extra requirement.

So we immediately see that none of the rings A, B or C is isomorphic to any of the others.

We now have to look at rings with additive group $\mathcal{C}_p \times \mathcal{C}_p$.

Let R be a ring with this additive group. Say the additive generators are a and b. Then we can see R as a vector space of dimension two over $\mathbb{F}_p$ since every element can be written as $ka + lb$ for certain $k, l \in \mathbf{Z}$.

What we plan to do, is show that for each pair of generators a and b, the given ring R equals one of the rings D, E, F, G, H, I, J or K. While doing so, we show that any two of these are non-isomorphic.

First, suppose that there exist these generators a and b, such that $a^2 = ma$ and $b^2 = nb$, where $m \not\equiv 0 \mod p$ and $n \not\equiv 0 \mod p$.

Then both a and b generate subrings of R that are isomorphic to $\mathbf{Z}/p\mathbf{Z}$, since the only other possibility is $\mathcal{C}_p(0)$, which occurs if $m \equiv 0$ or $n \equiv 0$.

So we may assume without loss of generality that $m = n = 1$. Now we also need to evaluate the product ab (and ba).

Let $ab = ta + ub$ for certain $t, u \in \mathbf{Z}$. Then we have

$$a^2b = aab = ta^2 + uab = ta + u(ta + ub) = (t + ut)a + u^2b.$$

Since $a^2b = ab = ta + ub$ we find that $u^2 \equiv u \mod p$, thus $u \equiv 0, 1 \mod p$. Similarly, by considering ab^2 we find that $t \equiv 0, 1 \mod p$.

If $u = t \equiv 1$, then $ab = a + b$, which implies:

$a^2b = a(a+b) = a^2 + ab = a + a + b = 2a + b \neq a + b = ab$, while $a^2b = ab$.

Thus clearly $u = t \equiv 1$ is impossible.

Similarly, we can let $ba = xa + yb$ and find that there are also only three possibilities for the pair (x, y).

We summarize the possibilities and discuss them one-by-one (in each of these cases $a^2 = a$ and $b^2 = b$):

1. $ab = 0$ and $ba = 0$;
2. $ab = 0$ and $ba = a$;
3. $ab = 0$ and $ba = b$;
4. $ab = a$ and $ba = 0$;
5. $ab = a$ and $ba = a$;
6. $ab = a$ and $ba = b$;
7. $ab = b$ and $ba = 0$;
8. $ab = b$ and $ba = a$;
9. $ab = b$ and $ba = b$.

Lemma 2.16. *Case 1 gives us a ring, which is isomorphic to* D.

Proof. Here we have:

$$R = \langle a, b : pa = pb = 0,\ a^2 = a,\ b^2 = b,\ ab = ba = 0 \rangle.$$

One only needs to check the associative and distributive laws. We construct $\varphi : R \to \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$ which is defined by setting $a \mapsto (1, 0)$ and $b \mapsto (0, 1)$. □

Lemma 2.17. *Cases 5 and 9 give us rings isomorphic to* D.

Proof. We have in Case 5:

$$R = \langle a, b : pa = pb = 0,\ a^2 = a,\ b^2 = b,\ ab = ba = a \rangle.$$

Here $\varphi : R \to \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$ is defined by $a \mapsto (1, 0)$ and $b \mapsto (1, 1)$.

Case 9 is found by exchanging the roles of a and b. □

Lemma 2.18. *Case 2,3,4 and 7 don't give rings.*

Proof. Case 2: We have $aba = 0 \cdot a = 0$, but also $aba = a \cdot a = a^2 = a \neq 0$ since a is a generator.

Case 3 is found by applying Case 2 with the roles of a and b reversed.

Case 4 is found by evaluating the product aba exactly as in 2.

Finally, case 7 is found by evaluating the product bab as in 3. □

Lemma 2.19. *Case 6 gives us a new ring, which is* E*.*

Proof. We have:

$$\langle a, b : pa = pb = 0,\ a^2 = a,\ b^2 = b,\ ab = a,\ ba = b \rangle$$

It is not isomorphic to $\mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$ since it is non-commutative. Clearly it is the ring described in E. □

Lemma 2.20. *Case 8 gives us a new ring, which is* F*.*

Proof. One might think that exchanging the roles of a and b gives the same as case 6. However this is not true.

This ring is not isomorphic to $\mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$ since this also is non-commutative. Now we need to show that it is also not isomorphic to E. We shall show that there are elements of F that do not satisfy any of the relations of E.

Let $A = ma + nb$ for certain $m, n \in \mathbf{Z}$ for which at least $m \neq 0$ or $n \neq 0$.

Now suppose that $A^2 = A$. We shall apply the relations as in F to see that:

$$(m^2 + mn)a + (n^2 + mn)b = ma + nb$$

Therefore $m^2 + mn \equiv m \mod p$ and $n^2 + mn \equiv n \mod p$. Now, if $m = 0$, then $n = 1$, if $m \neq 0$, then $m(n + m) = m$ and as such $n + m = 1$. If $n = 0$, then $m = 1$.

Clearly, if $A^2 = A$ we must have one of the following:

$$A = a;$$

$$A = b;$$

$$A = na + (1 - n)b \text{ for some } n \neq 0, 1.$$

Let B be independent of A and $B^2 = B$, then similarly:

$$B = a;$$

$$B = b;$$

$$B = xa + (1-x)b \text{ for some } x \neq 0, 1.$$

We have the following cases to check:

1. $A = a, B = a$
2. $A = a, B = b$
3. $A = a, B = xa + (1-x)b$
4. $A = b, B = a$
5. $A = b, B = b$
6. $A = b, B = xa + (1-x)b$
7. $A = na + (1-n)b, B = a$
8. $A = na + (1-n)b, B = b$
9. $A = na + (1-n)b, B = xa + (1-x)b$

Since we wanted designed A and B to be independent, cases 1 and 5 cannot occur.

Case 2: if $A = a$ and $B = b$, we find that $AB = ab = b \neq A$ and therefore our A and B clearly do not satisfy the relations in E.

Case 4 is similar to case 2.

Case 3: if $A = a$ and $B = xa + (1-x)b$ for certain $x \neq 0, 1$, then

$$AB = a(xa + (1-x)b) = xa^2 + (1-x)ab = xa + (1-x)b = B \neq A.$$

Again, it is clear that our A and B do not satisfy the relations given by E.

Cases 6, 7 and 8 are similar to case 3. What remains is case 9.

Case 9: Suppose $AB = A$ as it would be in E. Then:

$$\begin{array}{rcl} AB & = & (na + (1-n)b)(xa + (1-x)b) \\ & = & xna^2 + na(1-x)b + (1-n)bxa + (1-n)(1-x)b^2 \\ & = & xna + n(1-x)b + x(1-n)a + (1-n)(1-x)b \\ & = & x(n + 1 - n)a + (n + 1 - n)(1-x)b \\ & = & xa + (1-x)b \\ & = & B \end{array}$$

But this contradicts to A and B being independent.

Thus F is not isomorphic to E. □

We have to remind ourselves that we are not done yet, since we have only regarded the case for which a^2 is a non-zero multiple of a and b^2 is a non-zero multiple of b.

Suppose both squares are zero, then obviously the multiplication is trivial and we find the ring $(\mathcal{C}_p \times \mathcal{C}_p)(0)$, which is J.

It is clearly non-isomorphic to any of the above.

What options do we have remaining for a^2 and b^2? There is the possibility that one of them is zero and the other is a non-zero multiple of itself. But then we may assume, without loss of generality that $a^2 = 0$ and $b^2 = b$.

Again, by setting $ab = ta + ub$ and evaluating the product ab^2, we find that $t = 0, 1$.

By evaluating a^2b however, we find that either $ab = 0$ or $u = 0$. Thus the cases that we are presented with are: $ab = 0$ or $ab = a$.

Setting $ba = xa + yb$, and evaluating b^2a we find that $x = 0, 1$. By evaluating ba^2 we find that $y = 0$ or $ba = 0$.

So we have the following possibilities:

1. $ab = 0$ and $ba = 0$;
2. $ab = 0$ and $ba = a$;
3. $ab = a$ and $ba = 0$;
4. $ab = a$ and $ba = a$.

Lemma 2.21. *Case 1 gives us ring* H *which is isomorphic to* $\mathbf{Z}/p\mathbf{Z} \times \mathcal{C}_p(0)$.

Proof. We have:

$$\langle a, b : pa = pb = 0, a^2 = 0, b^2 = b, ab = ba = 0 \rangle.$$

The isomorphism is given by $a \mapsto (0, 1)$ and $b \mapsto (1, 0)$. □

Lemma 2.22. *Case 2 and 3 do not give us new rings.*

Proof. Let R_2 denote the ring given by the relations in case 2 and let R_3 denote the ring given by the relations in case 3. Case 2: We define $\varphi : F \to R_2$ by setting $a \mapsto a + b$ and $b \mapsto b$. It is clear that the ring in case 2 follows the same rules as the ring F.

Case 3: We define $\varphi : E \to R_3$ by setting $a \mapsto a + b$ and $b \mapsto b$. It is clear that the ring in case 3 follows the same rules as the ring E. □

Lemma 2.23. *Case 4 gives us a new ring,* G.

Proof. We have

$$\langle a, b : a^2 = 0, b^2 = b, ab = ba = a\rangle.$$

In H we do not have a multiplicative identity, in G we do, so $G \not\cong H$. □

For the remaining cases we refer the reader to [7], as they are similar. □

Remark. *We can see that of these* 11 *rings,* 2 *are non-commutative, and* 4 *of these rings have a multiplicative identity.*

Now we can determine the number of rings of order n for each cube-free n.

Example. *Let* $n = 41,856,930,490,307,832,900$, *(*$n = 6,469,693,230^2$ *see the example on page 17) then the number of non-isomorphic rings of order* n *is* $11^{10} = 25,937,424,601$. *Of which* 22,450,640,200 *are non-commutative, while only* 3,486,784,401 *are commutative. Furthermore* 25,936,376,025 *of these rings do not have a multiplicative identity, while only* 1,048,576 *do.*

It should be clear that, due to Eldridge's theorem, none of the non-commutative rings have a multiplicative identity.

We shall show how we got these numbers:

Proposition 2.24. *Let* $n = p_1^2 p_2^2 \cdots p_k^2$ *where the* p_i *are* k *distinct prime integers. Then* $\mathfrak{R}(n) = \prod_{i=1}^{k} \mathfrak{R}(p_i^2) = 11^k$ *by Theorem 2.9 and Theorem 2.15. The number of non-commutative rings of order* n *is given by*

$$2 \cdot \sum_{i=1}^{k} 9^{i-1} 11^{k-i},$$

and the number of rings without a multiplicative identity of order n *is given by*

$$7 \cdot \sum_{i=1}^{k} 4^{i-1} 11^{k-i}.$$

Proof. Recall that any ring of order n is isomorphic to a direct product of subrings (Proposition 2.1).

We know that for such a direct product to be commutative, all factors must be commutative. Therefore, only one of the rings need to be non-commutative for the entire ring to be non-commutative.

Let R_i denote the subring of order p_i^2. Suppose the first ring is non-commutative, i.e. R_1 is non-commutative, then whatever the other rings are, the direct product will also be non-commutative.

For this case, we have 2 options for the first ring (2 non-commutative rings of order p^2) and 11 for the remaining $k - 1$.

Suppose now, that the first ring is commutative, but the second ring is not. Then for the first ring, we have 9 options, for the second ring we again have 2 options, and 11 again for the remaining $k-2$ rings.

We can continue in this way, counting the number of non-commutative rings where the first $i < k$ factors are commutative.

This adds up to: $\sum_{i=0}^{k-1} 9^i \cdot 2 \cdot 11^{k-1-i}$, which in turn is equal to

$$2\sum_{i=1}^{k} 9^{i-1}11^{k-i}.$$

We could also count the commutative rings of order n, therefore, all k factors should be commutative, hence there are 9^k commutative rings of order n.

Clearly, we have

$$2\sum_{i=1}^{k} 9^{i-1}11^{k-i} = 11^k - 9^k.$$

We shall determine the number of rings without a multiplicative identity in a similar way. Remember that there are 4 rings with a multiplicative identity of order p^2.

This gives us:

$$7\sum_{i=1}^{k} 4^{i-1}11^{k-i}$$

for the number of rings without a multiplicative identity of order n.

It is again clear that

$$7\sum_{i=1}^{k} 4^{i-1}11^{k-i} = 11^k - 4^k.$$

Like in the example, due to Eldridge's theorem none of the non-commutative rings have a multiplicative identity. □

Bibliography

[1] V.G. Antipkin and V.P. Elizarov. Rings of order p^3. *Sibirskii Matematicheskii Zhurnal*, **23**: pp. 9–18, 1982.

[2] F. J.-B. J. Clauwens. Symmetrie. Syllabus for a course about group theory.

[3] B. Corbas and G. D. Williams. Rings of order p^5 part i. nonlocal rings. *Journal of Algebra*, **231**: pp, 677–690, 2000.

[4] B Corbas and G. D. Williams. Rings of order p^5 part ii. local rings. *Journal of Algebra*, **231**: pp. 691–704, 2000.

[5] K.E. Eldridge. Orders for finite noncommutative rings with unity. *The American Mathematical Monthly*, **75**: pp. 512–514, 1968.

[6] D.B. Erickson. Orders for finite noncommutative rings. *The American Mathematical Monthly*, **73**: pp. 376–377, 1966.

[7] Benjamin Fine. Classification of finite rings of order p^2. *Mathematics Magazine*, **66**: pp. 248–252, 1993.

[8] Colin R. Fletcher. Rings of small order. *The Mathematical Gazette*, **64**: pp. 9–22, 1980.

[9] L. Fuchs. *Abelian groups*. Pergamon Press, 1960.

[10] John F. Humphreys. *A Course in Group Theory*. Oxford University Press, 1996.

[11] C. R. MacCluer and G. A. Wilson. Problems for solution 1529. *The American Mathematical Monthly*, **69**: pp. 667–668, 1962.

[12] C. R. MacCluer, G. A. Wilson, and J. L. Pietenpol. E1529. *The American Mathematical Monthly*, **70**: p. 441, 1963.

[13] Kenjiro Shoda. über die einheitengruppe eines endliches ringes. *Mathematische Annalen*, **102**: pp. 273–282, 1930.

[14] Seth Warner, W.C. Waterhouse, G.A. Heuer, and D.B. Erickson. 5100. *The American Mathematical Monthly*, **71**: pp. 449–450, 1964.