Firm Rings: Rings Canonically Isomorphic to the Endomorphism Ring of their Additive Group

Thuijs, J.

J. Thuijs

Firm rings: Rings canonically isomorphic to the endomorphism ring of their additive group

Bachelor thesis

13 July 2023

Thesis supervisor: prof.dr. H.W. Lenstra

Leiden University
Mathematical Institute

Contents

1 Introduction **3**

2 Firm rings **4**
2.1 General properties of firm rings 4
2.2 Firm subrings of $\mathbb{Q}$ 6
2.3 Firmness of the ring of p-adic integers 8

3 Firm number rings **11**
3.1 Linear Algebra 11
3.2 Commensurability and integral closures 12
3.3 Firm number rings of quadratic extensions 16

4 References **20**

1 Introduction

Suppose that R is a ring such that its additive group R^+ is isomorphic as a group to $\mathbb{Z}/n\mathbb{Z}$ for a positive integer n. Then R is isomorphic as a ring to $\mathbb{Z}/n\mathbb{Z}$. For every ring R the map $\lambda\colon R \to \mathrm{End}(R^+)$ given by $r \mapsto (x \mapsto rx)$ for $r \in R$ is an injective ring homomorphism. That R is isomorphic as a ring to $\mathbb{Z}/n\mathbb{Z}$ can be proved by noting that $\lambda(R) = \mathrm{End}((\mathbb{Z}/n\mathbb{Z})^+)$ is equivalent to the statement that for every $f \in \mathrm{End}((\mathbb{Z}/n\mathbb{Z})^+)$ with $f(1) = 0$, implies f is the zero map. If $f(1) = 0$ then $f(m) = mf(1) = 0$, so indeed we find that $R \cong \mathrm{End}((\mathbb{Z}/n\mathbb{Z})^+)$ and $\mathbb{Z}/n\mathbb{Z} \cong \mathrm{End}((\mathbb{Z}/n\mathbb{Z})^+)$. Hence we obtain that $R \cong \mathbb{Z}/n\mathbb{Z}$.

This gives rise to the following definition. Let R be a ring and denote its underlying additive group by R^+. We say R is *firm* if the ring homomorphism $\lambda\colon R \longrightarrow \mathrm{End}(R^+)$ given by $r \mapsto (x \mapsto rx)$ is a ring isomorphism. Equivalently, we say R is firm if and only if $\lambda(R) = \mathrm{End}(R^+)$. The above proof generalizes in the context of firm rings. In theorem 2.4 we will see that if R is a firm ring and E is a ring such that $R^+ = E^+$, then E itself is firm and there exists a unique ring isomorphism $\psi\colon R \longrightarrow E$.

In the section *firm number rings*, we will state one of the main results, theorem 3.19. This theorem states the following:

Theorem. *Let K be a quadratic field extension of $\mathbb{Q}$, and let R be a subring of K such that $R \not\subset \mathbb{Q}$. Then R is either*

(a) firm; and moreover, there exists a prime number p such that $\dim_{\mathbb{F}_p}(R/pR) = 1$,

(b) or R is not firm; and moreover, for all prime numbers p we have that $\dim_{\mathbb{F}_p}(R/pR) \in \{0, 2\}$, and R^+ is a free $(R \cap \mathbb{Q})$-module of rank 2.

Another main result is theorem 2.3 in section *firm rings*, which states:

Theorem. *Let R be a ring. Then R is firm if and only if $\mathrm{End}(R^+)$ is commutative.*

Other results of the section *firm rings* are: firm rings are commutative and rigid. The term rigid gives the motivation for the use of the term "firm". Given a commutative ring R, we find that if the unique ring homomorphism from $\mathbb{Z}$ to R is a ring epimorphism, then R is a firm ring. We use this to deduce that every subring of the field of rational numbers is firm. Furthermore, we prove that the ring of p-adic integers $\mathbb{Z}_p$ is firm.

Let K be a finite field extension of $\mathbb{Q}$ and let R be a subring of K. If $\dim_{\mathbb{F}_p}(R/pR) = 1$ for some prime number p then R is firm. This is one of the results of the section *firm number rings*. Another result of this section is that if R and R' are subrings of a number field and commensurable, then R is firm if and only if R' is firm. In the context of integral closures, this gives that if R is a number ring then R is firm if and only if its integral closure is firm. This particular result might be useful for generalizing theorem 3.19 to arbitrary finite field extensions of $\mathbb{Q}$.

By convention we assume that a ring R has a multiplicative identity and ring homomorphism send the multiplicative identity to the multiplicative identity and subrings have the same multiplicative identity. When R is a ring we denote the group of units by R^* and the additive group by R^+.

2 Firm rings

2.1 General properties of firm rings

Definition 1 (Firm ring)**.** A ring R is *firm* if $\lambda\colon R \longrightarrow \mathrm{End}(R^+)$ given by $r \mapsto (x \mapsto rx)$ is a ring isomorphism.

For every ring R the map $\lambda\colon R \to \mathrm{End}(R^+)$ is an injective ring homomorphism. So in fact for a ring R it is only necessary to verify whether the map $\lambda\colon R \to \mathrm{End}(R^+)$ is surjective in order to determine whether the ring is firm. Therefore, an equivalent definition would be: R is firm if and only if $\lambda(R) = \mathrm{End}(R^+)$.

For example, when we take the ring $\mathbb{Z}$ we get a unique ring homomorphism $\lambda\colon \mathbb{Z} \to \mathrm{End}(\mathbb{Z}^+)$. Since every group endomorphism of $\mathbb{Z}$ is completely determined by the image of 1, it follows that λ is surjective.

Definition 2 (Rigid ring)**.** A ring R is *rigid* if $\mathrm{Aut}(R) = \{\mathrm{id}_R\}$. In other words a ring is *rigid* if the identity is the only ring automorphism.

The name "firm" is motivated by the fact that every firm ring is a rigid ring as well. This we will prove in the following proposition.

Proposition 2.1. *Let R be a ring. Then the following statements hold:*

(a) R is firm if and only if every $f \in \mathrm{End}(R^+)$ with $f(1) = 0$ is equal to the zero map.

(b) If R is firm then R is a commutative ring.

(c) If R is firm then R is a rigid ring.

Proof. For (a), suppose that R is firm. Then f is of the form $x \mapsto rx$, so it holds that $f(1) = r$. This gives that $f(1) = 0$ if and only if $r = 0$, so f is the zero map. Suppose that every $f \in \mathrm{End}(R^+)$ with $f(1) = 0$ is equal to the zero map. Then define $\mathrm{ev}_1\colon \mathrm{End}(R^+) \to R$ by $f \mapsto f(1)$. Then ev_1 is a group homomorphism such that $\mathrm{ev}_1 \circ \lambda = \mathrm{id}_R$. Suppose that $f \in \ker \mathrm{ev}_1$, then $f(1) = 0$, and thus by assumption f is the zero map. This gives that ev_1 is injective and as ev_1 is clearly surjective we find that ev_1 is a group isomorphism with inverse λ. Now λ is a group isomorphism and a ring homomorphism and thus a ring isomorphism. Therefore our ring R is firm.

For (b), let $r \in R$, then $x \mapsto rx$ and $x \mapsto xr$ are endomorphisms of R^+. Suppose that R is firm, then $\mathrm{ev}_1(x \mapsto rx - xr) = 0$. Thus $rx - xr = 0$ by (a) for all $x \in R$. We find that $rx = xr$ for all $x, r \in R$ and thus R is a commutative ring.

For (c), suppose that R is a firm ring, then $\lambda\colon R \to \mathrm{End}(R^+)$ given by $r \mapsto (x \mapsto rx)$ is a ring isomorphism. Now suppose that $\phi\colon R \to R$ is a ring automorphism, then ϕ is a group automorphism as well when we restrict ourselves to addition. So if ϕ is a ring automorphism it should be of the form $x \mapsto rx$ with $r \in R$. A ring automorphism should send the multiplicative identity to itself, so $1 \mapsto r \cdot 1 = 1$ and therefore $r = 1$. So every ring automorphism is equal to

$x \mapsto x$ and therefore a firm ring R is rigid. ■

Let $n \in \mathbb{Z}_{>0}$ and let $f \in \text{End}(\mathbb{Z}/n\mathbb{Z}^+)$. Then if $f(1) = 0$, it follows that f is zero map and thus $\mathbb{Z}/n\mathbb{Z}$ is firm with proposition 2.1. Hence for every $n \in \mathbb{Z}_{>0}$ the ring $\mathbb{Z}/n\mathbb{Z}$ is firm. In particular the field $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ is firm for every prime p.

Thus every firm ring is a commutative ring and as the ring is firm the map $\lambda\colon R \xrightarrow{\sim} \text{End}(R^+)$ is a ring isomorphism. It is clear that $\text{End}(R^+)$ needs to be commutative if R is firm. However, this condition is not only necessary, it is sufficient as well as we will show in theorem 2.3.

Definition 3 (Centralizer)**.** Let $S \subset R$ be a subset of a ring R. Then the *centralizer* of S in R is

$$\mathrm{C}_R(S) := \{r \in R : rs = sr \text{ for all } s \in S\}.$$

One can easily verify that the centralizer of S in R is a subring of R for every subset $S \subset R$.

Lemma 2.2. *Let R be a ring. Let $\rho\colon R \longrightarrow \text{End}(R^+)$ be the map given by $r \mapsto (x \mapsto xr)$ and $\lambda\colon R \to \text{End}(R^+)$ as usual be given by $r \mapsto (x \mapsto rx)$. Then the following holds*

$$\mathrm{C}_{\text{End}(R^+)}(\rho(R)) = \lambda(R).$$

Proof. For the inclusion $\lambda(R) \subset \mathrm{C}_{\text{End}(R^+)}(\rho(R))$, we note that the endomorphisms $x \mapsto r(xs)$ and $x \mapsto (rx)s$ are the same, because of the associativity of the multiplication in the ring R. Now for the inclusion $\mathrm{C}_{\text{End}(R^+)}(\rho(R)) \subset \lambda(R)$, suppose that $f \in \mathrm{C}_{\text{End}(R^+)}(\rho(R))$ then for every $r \in R$ we have

$$f \circ \rho(r) = \rho(r) \circ f.$$

When we evaluate the above in 1 we get that

$$f(\rho(r)(1)) = \rho(r)(f(1))$$
$$f(r) = f(1)r.$$

Thus $f = \lambda(f(1))$ which proves our inclusion and therefore we have $\mathrm{C}_{\text{End}(R^+)}(\rho(R)) = \lambda(R)$. ■

Theorem 2.3. *Let R be a ring. Then R is firm if and only if $\text{End}(R^+)$ is commutative.*

Proof. Suppose that R is firm so $\lambda(R) = \text{End}(R^+)$. Then with proposition 2.1 we have that R is a commutative ring, and therefore $\text{End}(R^+)$ is commutative. Now suppose that $\text{End}(R^+)$ is commutative. Lemma 2.2 gives that

$$\mathrm{C}_{\text{End}(R^+)}(\rho(R)) = \lambda(R).$$

As every two elements in $\text{End}(R^+)$ commute we get $\mathrm{C}_{\text{End}(R^+)}(\rho(R)) = \text{End}(R^+)$. Hence we find that $\lambda(R) = \text{End}(R^+)$ and therefore R is firm. ■

Given a non-trivial field extension K of a prime field k, there exists a 2-dimensional subspace of K over k. Let us denote this subspace as U, then there exists a subspace V of K over k such that $K = U \oplus V$. Then there exists a natural inclusion of $\mathrm{End}(U^+) \times \mathrm{End}(V^+)$ into $\mathrm{End}(K^+)$ which is a ring homomorphism. Given a basis for U there exists an inclusion of $\mathrm{M}(2, k)$ into $\mathrm{End}(U^+)$, where $\mathrm{M}(2, k)$ is the 2×2 matrix ring with coefficients in k. As $\mathrm{M}(2, k)$ is a non-commutative ring, so is $\mathrm{End}(U^+)$. This gives us that $\mathrm{End}(K^+)$ is a non-commutative ring and therefore we find that K cannot be firm.

Thus it follows that if K is a field and firm, then it should be a prime field. We have seen that $\mathbb{F}_p$ is firm for every prime p and in theorem 2.8 we will see that $\mathbb{Q}$ is firm (or one directly verifies that $\mathbb{Q}$ is firm). Therefore, we obtain that a field is firm if and only if it is a prime field.

Theorem 2.4. *Let R be a firm ring and let E be a ring such that $R^+ = E^+$. Then E is firm and there exists a unique ring isomorphism $\psi\colon R \longrightarrow E$. Furthermore, if $\cdot$ denotes the multiplication on R then the multiplication on E denoted by $\cdot_u$ is given by $r \cdot_u s := r \cdot u \cdot s$ for a certain $u \in R^*$. Conversely, if $\cdot$ denotes the multiplication on R then for every $u \in R^*$ the multiplication $\cdot_u$ given by $r \cdot_u s := r \cdot u \cdot s$ defines a ring with multiplicative identity u^{-1}.*

Proof. Suppose that R is a firm ring then $\mathrm{End}(R^+)$ is commutative by theorem 2.3. As $R^+ = E^+$, we find that $\mathrm{End}(E^+)$ is commutative and thus is E a firm ring. Furthermore, as $R^+ = E^+$, we have that $\mathrm{End}(R^+) = \mathrm{End}(E^+)$. This gives that R is isomorphic to E as a ring, because they are both isomorphic as ring to $\mathrm{End}(R^+)$. Now let $\psi\colon R \to E$ and $\phi\colon E \to R$ be ring isomorphisms. Then we have by proposition 2.1 that $\psi \circ \phi = \mathrm{id}_E$. Therefore, we have that $\psi = \phi^{-1}$ and this gives that ψ and ϕ are unique.

Let $(R, +, \cdot)$ be a fixed firm ring and E a ring such that $R^+ = E^+$. Then there exists a ring isomorphism $\psi\colon R \to E$. Thus ψ is a group automorphism of R^+. Now as it holds that $R^* \cong_{\lambda_{|_{R^*}}} \mathrm{Aut}(R^+)$ we have that $\psi = \lambda(u^{-1})$ for a $u^{-1} \in R^*$. Now $\psi \circ \psi^{-1}\colon E \to E$ is a group automorphism. Let $s, r \in R$. Then we have

$$\psi(\psi^{-1}(s)\psi^{-1}(r)) = \psi(usur) = u^{-1}(usur) = sur.$$

As ψ is a ring isomorphism we have that $\psi(1) = u^{-1}$ and therefore we have that u^{-1} is the multiplicative identity for the ring E. Therefore we find that $r \cdot_u s$ is the multiplication on E with $r \cdot_u s = r \cdot u \cdot s$ where $\cdot$ is the multiplication on R and $u \in R^*$.

Let $\cdot$ denote the multiplication on R then $\cdot_u$ defined by $r \cdot_u s := r \cdot u \cdot s$ defines another multiplication on R for $u \in R^*$. With respect to the multiplication $\cdot$ is R a ring. Hence $\cdot$ is distributive and associative and therefore we have that $\cdot_u$ is distributive and associative. Furthermore, we have that $r \cdot_u u^{-1} = r \cdot 1 = r$ and $u^{-1} \cdot_u r = 1 \cdot r = r$. Thus u^{-1} is indeed the multiplicative identity. Now we get that $(R, +, \cdot_u)$ defines a ring with multiplication given by $r \cdot_u s$ for $s, r \in R$. ∎

2.2 Firm subrings of $\mathbb{Q}$

We have seen that the ring $\mathbb{Z}$ is firm and that for every $n \in \mathbb{Z}_{>0}$ the ring $\mathbb{Z}/n\mathbb{Z}$ is firm. In this section we will show that every subring of $\mathbb{Q}$ is firm. We will do this by uniquely identifying each subring of the field of rational numbers with a set of primes. Then we will use this identification to show that every subring is firm.

Lemma 2.5. *Let $\mathscr{P}$ denote the set of prime numbers. Suppose $x \in \mathbb{Q}$, then denote the smallest positive integer c such that $cx \in \mathbb{Z}$ by $\operatorname{den}(x)$. Then for every set $B \subset \mathscr{P}$ we have that $\mathbb{Z}[\frac{1}{p} : p \in B]$ is equal to the set of $x \in \mathbb{Q}$ with the property that every prime number dividing $\operatorname{den}(x)$ belongs to B.*

Proof. Let us denote the set of $x \in \mathbb{Q}$ with the property that every prime number dividing $\operatorname{den}(x)$ belongs to B by Ω_B. As $\operatorname{den}(1) = 1$ and no prime number divides 1 we get that $1 \in \Omega_B$. Furthermore, we have that if $x, y \in \mathbb{Q}$ then $\operatorname{den}(x \pm y) | \operatorname{den}(x) \cdot \operatorname{den}(y)$ and $\operatorname{den}(xy) | \operatorname{den}(x) \cdot \operatorname{den}(y)$. Hence it follows that Ω_B is a subring of $\mathbb{Q}$. Let $p \in B$ be a prime number. Then $\operatorname{den}(\frac{1}{p}) = p$ and this gives us that $\frac{1}{p} \in \Omega_B$. Now we obtain that $\mathbb{Z}[\frac{1}{p} : p \in B] \subset \Omega_B$. Suppose that $x \in \Omega_B$, then $x = \frac{a}{b}$ for $a, b \in \mathbb{Z}$ such that $\gcd(a, b) = 1$ and for all $q \in \mathscr{P} \setminus B$ we have that $q \nmid b$. Hence b is a product of primes $p \in B$. Thus $x \in \mathbb{Z}[\frac{1}{p} : p \in B]$. ■

Theorem 2.6. *Let $\mathscr{P}$ denote the set of prime numbers and denote with $\mathcal{P}(\mathscr{P})$ the power set of the set of prime numbers. Then there exists a bijection*

$$\{\textit{subrings of } \mathbb{Q}\} \longrightarrow \mathcal{P}(\mathscr{P})$$

given by $R \mapsto \{p \in \mathscr{P} : \frac{1}{p} \in R\}$ with inverse $B \mapsto \mathbb{Z}[\frac{1}{p} : p \in B]$.

Proof. Denote with $S(\mathbb{Q})$ the set $\{\text{subrings of } \mathbb{Q}\}$. Define $\psi \colon S(\mathbb{Q}) \to \mathcal{P}(\mathscr{P})$ by $R \mapsto \{p \in \mathscr{P} : \frac{1}{p} \in R\}$ and define $\phi \colon \mathcal{P}(\mathscr{P}) \to S(\mathbb{Q})$ by $B \mapsto \mathbb{Z}[\frac{1}{p} : p \in B]$. We will show that $\psi \circ \phi = \operatorname{id}_{\mathcal{P}(\mathscr{P})}$ and that $\phi \circ \psi = \operatorname{id}_{S(\mathbb{Q})}$.

Let $B \in \mathcal{P}(\mathscr{P})$ then

$$\begin{aligned}(\psi \circ \phi)(B) &= \psi(\phi(B)) \\ &= \psi(\mathbb{Z}[\tfrac{1}{p} : p \in B]) \\ &= \{q \in \mathscr{P} : \tfrac{1}{q} \in \mathbb{Z}[\tfrac{1}{p} : p \in B]\}.\end{aligned}$$

It is immediately clear that $B \subset \{q \in \mathscr{P} : \frac{1}{q} \in \mathbb{Z}[\frac{1}{p} : p \in B]\}$. Let $\frac{1}{q} \in \mathbb{Z}[\frac{1}{p} : p \in B]$. Suppose that $q \notin B$ then $q = \operatorname{den}(\frac{1}{q}) \notin B$. Hence with lemma 2.5 it follows that $\frac{1}{q} \notin \mathbb{Z}[\frac{1}{p} : p \in B]$. So $\frac{1}{q} \in \mathbb{Z}[\frac{1}{p} : p \in B]$ if and only if $q = p$ for some $p \in B$. Hence we find that $\{q \in \mathscr{P} : \frac{1}{q} \in \mathbb{Z}[\frac{1}{p} : p \in B]\} \subset B$ and thus $(\psi \circ \phi)(B) = B$. Let $R \in S(\mathbb{Q})$ then

$$\begin{aligned}(\phi \circ \psi)(R) &= \phi(\psi(R)) \\ &= \phi(\{p \in \mathscr{P} : \tfrac{1}{p} \in R\}) \\ &= \mathbb{Z}[\tfrac{1}{q} : q \in \{p \in \mathscr{P} : \tfrac{1}{p} \in R\}] \\ &= \mathbb{Z}[\tfrac{1}{q} : \tfrac{1}{q} \in R].\end{aligned}$$

Clearly, we have that $\mathbb{Z}[\frac{1}{q} : \frac{1}{q} \in R] \subset R$. Let $x \in R$. Then there exists an $a \in \mathbb{Z}$ such that $x = \frac{a}{\operatorname{den}(x)}$ and $\gcd(a, \operatorname{den}(x)) = 1$. Furthermore, there exists a $c \in \mathbb{Z}$ such that $ca \equiv 1 \bmod \operatorname{den}(x)$. So $cx \in R$ and $x = \frac{1}{\operatorname{den}(x)} + m$, where $m \in \mathbb{Z}$. This gives us that $\frac{1}{\operatorname{den}(x)} \in R$. Now if $p | \operatorname{den}(x)$ then $\frac{1}{p} \in R$. Hence $x \in \mathbb{Z}[\frac{1}{q} : \frac{1}{q} \in R]$. This proves that $\phi \circ \psi = \operatorname{id}_{S(\mathbb{Q})}$. ■

Definition 4 (Ring epimorphism)**.** Suppose that R and E are rings and let $\psi\colon R \longrightarrow E$ be a ring homomorphism. Then ψ is a *ring epimorphism* if for all rings M and ring homomorphisms $\phi, \varphi\colon E \longrightarrow M$ we have that $\phi \circ \psi = \varphi \circ \psi$ implies that $\phi = \varphi$.

For every ring R there exists a unique ring homomorphism $e\colon \mathbb{Z} \to R$. Suppose that this ring homomorphism is an epimorphism. Then we find that for every ring M there exists at most one ring homomorphism $\psi\colon R \to M$. This is due to the fact that the condition $\phi \circ e = \varphi \circ e$ is always satisfied for ring homomorphisms $\varphi, \phi : R \to M$, as $\phi \circ e, \varphi \circ e\colon \mathbb{Z} \to M$ is unique.

The idea of the following lemma is that under the condition that $e\colon \mathbb{Z} \to R$ is an epimorphism the ring R is firm comes from Martin Brandenburg; see [1].

Lemma 2.7. *Suppose that R is a commutative ring. If $e\colon \mathbb{Z} \longrightarrow R$ is a ring epimorphism, then R is a firm ring.*

Proof. Suppose that $e\colon \mathbb{Z} \longrightarrow R$ is a ring epimorphism. Let $f \in \mathrm{End}(R^+)$. If we want to show R is firm it is sufficient to show that $f(1)r = f(r)$ for all $r \in R$. Given $R \otimes_{\mathbb{Z}} R$, defining multiplication on its generators as $(x \otimes y)(z \otimes w) = (xz) \otimes (yw)$ makes $R \otimes_{\mathbb{Z}} R$ a ring with multiplicative identity $1 \otimes 1$. As $e\colon \mathbb{Z} \to R$ is a ring epimorphism we find that the ring homomorphisms $x \mapsto x \otimes 1$ and $x \mapsto 1 \otimes x$ are equal. Thus for every $x \in R$ we have that $x \otimes 1 = 1 \otimes x$.

We note that as f is an endomorphism, the map $R \times R \to R$ given by $(x, y) \mapsto f(x)y$ is $\mathbb{Z}$-bilinear. Thus there exists a unique group homomorphism $\varphi\colon R \otimes_{\mathbb{Z}} R \to R$ such that for all $x, y \in R$ we have that $\varphi(x \otimes y) = f(x)y$. Now as $x \otimes 1 = 1 \otimes x$ for all $x \in R$, we have that

$$f(x) = \varphi(x \otimes 1) = \varphi(1 \otimes x) = f(1)x.$$

Thus we find that $f(x) = f(1)x$. So for every $f \in \mathrm{End}(R^+)$ we get that $f = \lambda(f(1))$. Therefore, we have that R is firm. ■

Theorem 2.8. *Every subring $R \subset \mathbb{Q}$ is firm. In fact every $e\colon \mathbb{Z} \longrightarrow R$ is a ring epimorphism.*

Proof. There exists a unique ring homomorphism $e\colon \mathbb{Z} \longrightarrow R$. Let M be a ring and $\psi, \phi\colon R \longrightarrow M$ be ring homomorphisms. Obviously, we have that for all $x \in \mathbb{Z}$ the following holds $\psi(x) = \phi(x)$. Theorem 2.6 tells us that $R = \mathbb{Z}[\frac{1}{p} : p \in B]$ for a $B \subset \mathscr{P}$ with theorem 2.6. Let $p \in B$. Then we have that $\psi(\frac{1}{p}) = \phi(\frac{1}{p})$, as ϕ and ψ coincide on p, they coincide on $\frac{1}{p}$, due to the uniqueness of inverses. Now we have that ϕ and ψ are the same for all $x \in \mathbb{Z}$ and all $\frac{1}{p}$ with $p \in B$, and since those elements generate $\mathbb{Z}[\frac{1}{p} : p \in B]$, we find that $\psi = \phi$.

So every two ring homomorphisms from R to M are the same and therefore the defining property in definition 4 is satisfied. As $e\colon \mathbb{Z} \longrightarrow R$ is a ring epimorphism we find using lemma 2.7 that R is a firm ring. So every subring $R \subset \mathbb{Q}$ is a firm ring. ■

2.3 Firmness of the ring of p-adic integers

Lemma 2.9. *Let R be a commutative ring. Let p be a prime number such that*

$$\#(R/pR) \leq p.$$

Then for all $n \in \mathbb{Z}_{\geq 0}$ we have that $R = (\mathbb{Z} \cdot 1_R) + p^n R$.

Although p is not necessarily an element of R, we can always view p as element of R by its image under the unique ring homomorphism from $\mathbb{Z}$ to R.

Proof. Let R be a commutative ring and p a prime such that $\#(R/pR) \leq p$. We have that R/pR is a vector space over $\mathbb{F}_p$. Thus the condition $\#(R/pR) \leq p$ is equivalent with $\dim_{\mathbb{F}_p}(R/pR) \leq 1$. Let us first assume that $\dim_{\mathbb{F}_p}(R/pR) = 0$. Then $R = pR$ and we find for every $n \in \mathbb{Z}_{\geq 0}$ that $R = p^n R$. Clearly, we obtain that $R = (\mathbb{Z} \cdot 1_R) + p^n R$.

Let us now assume that $\dim_{\mathbb{F}_p}(R/pR) = 1$. Thus we have $R/pR \cong \mathbb{F}_p$ and therefore we have that $R = (\mathbb{Z} \cdot 1_R) + pR$.

Assume it is true for n, then we will prove that it is true for $n+1$. We have that $R = (\mathbb{Z} \cdot 1) + pR$ and $R = (\mathbb{Z}\cdot 1) + p^n R$, so we can write $R = (\mathbb{Z}\cdot 1) + p\left((\mathbb{Z} \cdot 1) + p^n R\right)$. Every element of $(\mathbb{Z}\cdot 1) + p^n R$ is of the form $(k_i + p^n r_i)$ for $k \in \mathbb{Z}$ and $r \in R$, so then we get that

$$p(k + p^n r) = (pk + p^{n+1} r).$$

Now it follows that $p\left((\mathbb{Z} \cdot 1) + p^n R\right) = p(\mathbb{Z}\cdot 1) + p^{n+1} R$. This gives that $R = (\mathbb{Z}\cdot 1) + p(\mathbb{Z}\cdot 1) + p^{n+1} R$ and as $p(\mathbb{Z} \cdot 1)$ is a subgroup of $(\mathbb{Z} \cdot 1)$ we get that $R = (\mathbb{Z} \cdot 1) + p^{n+1} R$. ∎

Theorem 2.10. *Let R be a commutative ring. If there exists a prime p such that*

$$\#(R/pR) \leq p, \qquad \bigcap_{n=1}^{\infty} p^n R = (0),$$

then R is firm.

Proof. Suppose that $f \in \mathrm{End}(R^+)$, with $f(1) = 0$. Then using lemma 2.9 gives that

$$f(R) = f(\mathbb{Z} \cdot 1 + p^n R) = \mathbb{Z} \cdot f(1) + f(p^n \cdot R) = p^n f(R) \subset p^n R$$

holds for every $n \in \mathbb{Z}_{\geq 0}$. This gives that

$$f(R) \subset \bigcap_{n=1}^{\infty} p^n R = (0),$$

and so we get that $f(x) = 0$ for all $x \in R$. Therefore we find using proposition 2.1 that R is a firm ring. ∎

Definition 5 (The ring of p-adic integers)**.** Let p be a prime. Then *the ring of p-adic integers* is defined as $\mathbb{Z}_p := \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$, where $\mathbb{Q}_p$ is the field of p-adic numbers, which is the completion of $\mathbb{Q}$ with respect to the p-norm.

In [2] we find the definition as above and the statement that $\mathbb{Z}_p$ is a ring. Moreover, we find that $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to the p-norm. Furthermore, we find that $\mathbb{Z}_p$ is commutative and in corollary 3.3.6 of the same book that for $n \geq 1$ the following holds

$$\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}. \tag{1}$$

Theorem 2.11. *Let p be a prime. Then the ring $\mathbb{Z}_p$ of p-adic integers is firm.*

Proof. Let p be a prime and $\mathbb{Z}_p$ the ring of p-adic integers. Then we apply theorem 2.10 to p. We obtain using (1) that

$$\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}.$$

This gives that $\#(\mathbb{Z}_p/p\mathbb{Z}_p) = p$, so the first condition is satisfied. We have that $|p^n|_p = p^{-n}$ and therefore we get $p^n\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq p^{-n}\}$. Thus for all $x \in \bigcap_{n=1}^{\infty} p^n\mathbb{Z}_p$ we get that $|x|_p \leq p^{-n}$ for all $n \in \mathbb{Z}_{>0}$. Hence we get that $|x|_p = 0$ and thus $x = 0$. Then theorem 2.10 implies that $\mathbb{Z}_p$ is a firm ring. ■

3 Firm number rings

3.1 Linear Algebra

Lemma 3.1. *Suppose $n \in \mathbb{Z}_{\geq 0}$ and $H \subset \mathbb{Q}^n$ is an additive subgroup. Then for every $k, m \in \mathbb{Z}_{>0}$ it holds that*

$$\#(H/kmH) = \#(H/kH) \cdot \#(H/mH).$$

Proof. Suppose $n \in \mathbb{Z}_{\geq 0}$ and $H \subset \mathbb{Q}^n$ is an additive subgroup. Let $k, m \in \mathbb{Z}_{>0}$. Then

$$\#(H/kmH) = \#(H/kH) \cdot \#(kH/kmH).$$

Let $\varphi\colon H/mH \to kH/kmH$ be given by $h + mH \mapsto kh + kmH$. Then if $h \in \ker \varphi$ it follows that $kh \in kmH$. However, if $kh \in kmH$, then $h \in mH$ as multiplication with $k \neq 0$ is an automorphism of $\mathbb{Q}^n$ and therefore sends the subgroup $mH \subset \mathbb{Q}^n$ injectively to $kmH \subset \mathbb{Q}^n$. Thus we conclude that φ is injective. Furthermore, φ is clearly a surjection. Hence it is a group isomorphism. This gives that $\#(H/mH) = \#(kH/kmH)$ and hence we obtain

$$\#(H/kmH) = \#(H/kH) \cdot \#(H/mH).$$

■

Corollary 3.1.1. *Let K be a finite field extension of $\mathbb{Q}$, and $R \subset K$ a subring. Let $k, l \in \mathbb{Z}_{>0}$. Then*

$$\#(R/k^l R) = (\#(R/kR))^l.$$

Proof. This follows by induction on l from lemma 3.1. ■

Proposition 3.2. *Suppose $n \in \mathbb{Z}_{\geq 0}$ and $H \subset \mathbb{Q}^n$ is an additive subgroup. Then for all $m \in \mathbb{Z}_{>0}$ the following holds:*

$$\#(H/mH) | m^n.$$

Proof. With lemma 3.1 it is sufficient to show that $\#(H/pH)|p^n$ for every prime p. Let p be a prime. Then H/pH is an $\mathbb{F}_p$-vector space. Now let V be a k-dimensional subspace of H/pH and let $(h_1 + pH, h_2 + pH, \ldots, h_k + pH)$ be a basis for V.

Suppose that $k > n$. Let $\pi\colon H \to H/pH$ be the quotient map which sends h_i to $h_i + pH$. Then the $h_i \in H$ are not linearly independent over $\mathbb{Q}$. Therefore, there exist $a_i \in \mathbb{Q}$ not all equal to zero such that $\sum_{i=1}^k a_i h_i = 0$. Without loss of generality, we can choose the $a_i \in \mathbb{Z}$ as we can multiply with the product of the denominators. Moreover, we can choose our $a_i \in \mathbb{Z}$ such that there exists an a_j with $p \nmid a_j$, because otherwise all a_i are divisible by p. Hence we can divide by p until there exists an a_j with $p \nmid a_j$. We obtain that

$$\sum_{i=1}^{k} \pi(a_i h_i) = \sum_{i=1}^{k} (a_i \bmod p)(h_i + pH) = 0.$$

Since there exists an a_j with $p \nmid a_j$ we get that $(a_j \bmod p) \neq 0$. Hence we find that $(h_1 + pH, h_2 + pH, \ldots, h_k + pH)$ cannot be a basis for V. Thus we can conclude that H/pH does not have any k-dimensional subspaces when $k > n$. Hence we obtain that H/pH itself cannot have a dimension bigger than n. Therefore, we obtain that $\#(H/pH) | p^n$. ■

3.2 Commensurability and integral closures

Definition 6 (Commensurable)**.** Let G be a group. Subgroups $H, J \subset G$ are *commensurable* if both the index $(H\colon H \cap J)$ and $(J\colon H \cap J)$ are finite.

Proposition 3.3. *Let G be an abelian group. Then commensurablility defines an equivalence relation on the set of subgroups of G.*

Proof. Let G be a group. Then for every subgroup $H \subset G$ we have that H is commensurable with H as $(H : H \cap H) = (H : H) = 1$. Thus commensurability is reflexive and it is symmetric as both $(H : H \cap J)$ and $(J : H \cap J)$ need to be finite if H is commensurable to J.

For the transitivity, assume that H and J are commensurable and that J and K are commensurable. Furthermore we have that

$$\begin{aligned}(H : H \cap J \cap K) &= (H : H \cap J) \cdot (H \cap J : H \cap J \cap K) \\ &= (H : H \cap J) \cdot ((H \cap J)K : K) \\ &\leq (H : H \cap J) \cdot (J : J \cap K).\end{aligned}$$

Now as $(H : H \cap J)$ and $(J : J \cap K)$ are both finite we find that $(H : H \cap J \cap K)$ is finite. Hence $(H : H \cap K)$ is finite. Interchanging the role of H and K gives that $(K : H \cap K)$ is finite as well. Thus we obtain that H and K are commensurable. ■

Lemma 3.4. *Let H and J be commensurable subgroups of a finite dimensional $\mathbb{Q}$-vector space. Then for all $m \in \mathbb{Z}_{>0}$ we have $\#(H/mH) = \#(J/mJ)$.*

Proof. We can assume that $J \subset H$, because if H and J are commensurable then so are $H \cap J$ and H commensurable, and similarly $H \cap J$ and J are commensurable. Let $\varphi\colon H/J \to mH/mJ$ be given by $h + J \mapsto mh + mJ$ then if $h \in \ker \varphi$ it follows that $mh \in mJ$. However, if $mh \in mJ$ then $h \in J$ and therefore we obtain that $\ker \varphi = 0$. Thus φ is injective. Moreover, φ is clearly a surjection and hence φ is a group isomorphism. Thus we have that $(H : J) = (mH : mJ)$. Furthermore, we have that $(H : mH)\cdot(mH : mJ) = (H : mJ)$ and $(H : J)\cdot(J : mJ) = (H : mJ)$. Hence it follows that $(H : mH) = (J : mJ)$, and this gives that $\#(H/mH) = \#(J/mJ)$. ■

Definition 7 (Number ring)**.** A *number ring* is a subring of a number field K where a number field is a finite field extension of $\mathbb{Q}$. A *firm number ring* is a number ring which is also a firm ring.

Definition 8 (Integral)**.** Let A, B and C be commutative rings such that $A \subset C$ and $B \subset C$ are subrings of C. Then an element $b \in B$ is *integral* (over A) when there exists a monic polynomial $f \in A[X]$ with $f(b) = 0$. When every element $b \in B$ is integral over A, we say that B is integral over A.

Lemma 3.5. *Let R be a number ring and K its field of fractions. Then if $x, y \in K$ are integral over R, so are xy, $x + y$ and $x - y$.*

Proof. We refer to proposition 3.17 in [5] for the sum and product. We have -1 is integral over R as $x + 1$ is a monic polynomial with coefficients in R. Then with the product we find that $-y$ is integral over R for y integral over R. Hence we get that $x - y$ is integral over R. ■

For every number ring R with field of fractions K we have that R is integral over R. Hence the previous lemma tells us that the set of all elements $x \in K$ which are integral over R is a subring of K which contains R. This subring is called the *integral closure* and we denote the integral closure of R with $\tilde{R}$.

Definition 9 (Dedekind domain)**.** A number ring R that is not a number field is called a *Dedekind domain* if for every prime ideal $\mathfrak{p}$ of R, the local ring $R_{\mathfrak{p}}$ is a discrete valuation ring.

Theorem 3.6. *Let R be a number ring with field of fractions K, and $\mathcal{O}_K$ the ring of integers of K. Then the following statements hold:*

(a) $\mathcal{O}_K = \{x \in K : f_{\mathbb{Q}}^x \in \mathbb{Z}[X]\}$;

(b) the integral closure of R equals $\tilde{R} = R\mathcal{O}_K$;

(c) R is Dedekind if and only if it contains $\mathcal{O}_K$.

Proof. We refer to theorem 3.20 in [5]. ■

Lemma 3.7. *Every number ring R is of finite index in its integral closure $\tilde{R}$.*

Proof. We refer to theorem 4.9 in [5]. ■

Proposition 3.8. *Let R and R' be number rings with field of fractions K. Then the following statements hold:*

(a) $\tilde{R}$ is commensurable with R;

(b) R and R' are commensurable if and only if $\tilde{R} = \tilde{R}'$.

Proof. For (a), let R be a number ring. Then with lemma 3.7 it follows that R is of finite index in $\tilde{R}$. So alongside with $R \cap \tilde{R} = R$ we conclude that $(\tilde{R} : R \cap \tilde{R})$ is finite and $(R : R \cap \tilde{R}) = 1$. Thus indeed we have that R and $\tilde{R}$ are commensurable.

For (b), suppose that $\tilde{R} = \tilde{R}'$. Due to (a) we have that R and $\tilde{R}$ are commensurable. Similarly, we have that R' and $\tilde{R}'$ are commensurable. Hence it follows with proposition 3.3 that R and R' are commensurable.

Suppose that R and R' are commensurable. Then there exists an $n \in \mathbb{Z}_{>0}$ such that $(R' : R \cap R') = n$. Furthermore, there exist $b_i \in R'$ such that

$$R' = \bigcup_{i=1}^{n} (b_i + (R \cap R')).$$

Let $x \in R'$, then $1, x, x^2, \ldots, x^n$ cannot all be contained in different cosets. Hence there exist $k, l \in \mathbb{Z}_{>0}$ such that $k < l$ and $x^k \equiv x^l \bmod (R \cap R')$. Thus there exists an $r \in R \cap R'$ such that $x^l - x^k - r = 0$. Therefore, $x \in R'$ is integral over R. Hence R' is integral over R. This gives that $R' \subset \tilde{R}$ and $\tilde{R}' \subset \tilde{\tilde{R}} = \tilde{R}$. Thus $\tilde{R}' \subset \tilde{R}$, and interchanging R and R' gives that $\tilde{R} \subset \tilde{R}'$. Therefore, we obtain that $\tilde{R} = \tilde{R}'$. ■

Lemma 3.9. *Let R be a number ring. Then for every $f \in \mathrm{End}(R^+)$ there exists a unique $\bar{f} \in \mathrm{End}(\mathbb{Q} \cdot R^+)$ such that $\bar{f}_{|_{R^+}} = f$, and this $\bar{f}$ is $\mathbb{Q}$-linear. Furthermore, the map $\mathrm{End}(R^+) \to \mathrm{End}_{\mathbb{Q}}(\mathbb{Q} \cdot R^+)$ given by $f \mapsto \bar{f}$ is an injective ring homomorphism.*

Proof. Suppose that $x \in \mathbb{Q} \cdot R^+$. Then $x = \sum_{i=1}^{k} q_i r_i$, where $q_i \in \mathbb{Q}$ and $r_i \in R^+$. For every $q_i \in \mathbb{Q}$ there exists $a_i, b_i \in \mathbb{Z}$ such that $q_i = \frac{a_i}{b_i}$ we can choose $b_i \in \mathbb{Z}_{>0}$. Then $x = \sum_{i=1}^{k} \frac{a_i r_i}{b_i}$ and hence we can write

$$x = \frac{\sum_{i=1}^{k} a_i r_i \left(\prod_{1 \le j \le k, j \ne i}^{k} b_i\right)}{\prod_{i=1}^{k} b_i}.$$

Since all the $b_i \in \mathbb{Z}_{>0}$ and $\sum_{i=1}^{k} a_i r_i \left(\prod_{1 \le j \le k, j \ne i}^{k} b_i\right) \in R^+$ as $\mathbb{Z}$ is a subgroup of R, we see that we can write every $x \in \mathbb{Q} \cdot R^+$ in the form $\frac{y}{n}$ for some $y \in R^+$ and $n \in \mathbb{Z}_{>0}$.

Let us define $\bar{f}(\frac{y}{n}) := \frac{f(y)}{n}$. We will now show that $\bar{f}$ is well-defined. Let $z \in R^+$ and $m \in \mathbb{Z}_{>0}$ such that $\frac{y}{n} = \frac{z}{m}$. Then my and nz are the same element of R^+. This gives that $f(my) = f(nz)$ and because f is $\mathbb{Z}$-linear we get that $mf(y) = nf(z)$. Hence we find that $\frac{f(y)}{n} = \frac{f(z)}{m}$. Clearly, we have that $\bar{f}_{|_{R^+}} = f$ since $\bar{f}(\frac{r}{1}) = f(r)$ for all $r \in R$. We have that $\bar{f}$ is $\mathbb{Z}$-linear as f is $\mathbb{Z}$-linear and $\bar{f}(\frac{y}{n}) = \frac{f(y)}{n}$ and hence an element of $\mathbb{Q} \cdot R^+$. Let $w \in R^+$ and $l \in \mathbb{Z}_{>0}$. Then

$$\begin{aligned} \bar{f}\left(\tfrac{y}{n} + \tfrac{w}{l}\right) &= \bar{f}\left(\tfrac{ly+nw}{nl}\right) \\ &= \tfrac{f(ly+nw)}{nl} \\ &= \tfrac{f(y)}{n} + \tfrac{f(w)}{l} \\ &= \bar{f}(\tfrac{y}{n}) + \bar{f}(\tfrac{w}{l}). \end{aligned}$$

Hence $\bar{f}$ is additive and therefore we find that $\bar{f}$ is indeed an element of $\mathrm{End}(\mathbb{Q} \cdot R^+)$ such that $\bar{f}_{|_{R^+}} = f$.

Let $q \in \mathbb{Q}$ and $r \in R^+$. Then there exist $a, b \in \mathbb{Z}$ such that $q = \frac{a}{b}$. Considering $\bar{f}$ is $\mathbb{Z}$-linear, we have that $b\bar{f}(qr) = \bar{f}(ar)$ and $bq\bar{f}(r) = a\bar{f}(r)$. Again, $\bar{f}$ is $\mathbb{Z}$-linear so we obtain that $b\bar{f}(qr) = bq\bar{f}(r)$. Hence, multiplying with $\frac{1}{b}$ gives that $\bar{f}(qr) = q\bar{f}(r)$. Thus we find that $\bar{f}$ is indeed $\mathbb{Q}$-linear. Let $q \cdot \mathbb{Q}$ and $r \in R^+$, then $\bar{f}(qr^+) = q\bar{f}(r) = qf(r)$. Hence $\bar{f}$ is uniquely determined by the image of R^+.

Clearly, $\bar{\text{id}}_R = \text{id}_{\mathbb{Q}\cdot R^+}$ as $\bar{\text{id}}_R(qr) = q\bar{\text{id}}_R(r) = qr$. Furthermore, we have that $\overline{f+g} = \bar{f} + \bar{g}$ and $\overline{f \circ g} = \bar{f} \circ \bar{g}$ as both sides coincide on R^+. Since we have proved that for every $f \in \text{End}(R^+)$ there exists a unique $\mathbb{Q}$-linear $\bar{f} \in \text{End}(\mathbb{Q} \cdot R^+)$, we note that the map $\text{End}(R^+) \to \text{End}_{\mathbb{Q}}(\mathbb{Q} \cdot R^+)$ given by $f \mapsto \bar{f}$ is an injective ring homomorphism. ■

Due to the inclusion stated in lemma 3.9 we can view $\text{End}(R^+)$ as a subring of $\text{End}_{\mathbb{Q}}(\mathbb{Q} \cdot R^+)$.

Lemma 3.10. *Let R be a number ring. Then R is firm if and only if $\text{End}(R^+)$ is commutative; if and only if $\mathbb{Q} \cdot \text{End}(R^+)$ is commutative.*

Proof. The statement R is firm if and only if $\text{End}(R^+)$ is commutative is stated and proved in theorem 2.3. Hence it is sufficient to prove that $\text{End}(R^+)$ is commutative if and only if $\mathbb{Q} \cdot \text{End}(R^+)$ is commutative. We embed $\mathbb{Q}$ into $\text{End}_{\mathbb{Q}}(\mathbb{Q} \cdot R^+)$ by sending every $q \in \mathbb{Q}$ to the endomorphism $x \mapsto qx$. Hence the elements of $\mathbb{Q}$ under the embedding commute with all the elements of $\text{End}_{\mathbb{Q}}(\mathbb{Q} \cdot R^+)$. Thus if $\text{End}(R^+)$ is commutative we get that $\mathbb{Q} \cdot \text{End}(R^+)$ is commutative. When $\text{End}(R^+)$ is not commutative then so is $\mathbb{Q} \cdot \text{End}(R^+)$. Therefore, we find that $\text{End}(R^+)$ is commutative if and only if $\mathbb{Q} \cdot \text{End}(R^+)$ is commutative. ■

Lemma 3.11. *Let R be a number ring. Then*

$$\mathbb{Q} \cdot \text{End}(R^+) = \left\{ f \in \text{End}_{\mathbb{Q}}(\mathbb{Q} \cdot R^+) : \exists n \in \mathbb{Z}_{>0} : f(R^+) \subset \tfrac{1}{n} R^+ \right\}.$$

Proof. Suppose that $h \in \mathbb{Q} \cdot \text{End}(R^+)$, then there exists $g \in \text{End}(R^+)$ such that $h = \frac{m}{n} g$. However, $mg \in \text{End}(R^+)$, so it follows that $h \in \left\{ f \in \text{End}_{\mathbb{Q}}(\mathbb{Q} \cdot R^+) : \exists n \in \mathbb{Z}_{>0} : f(R^+) \subset \frac{1}{n} R^+ \right\}$.

Now suppose that $h \in \left\{ f \in \text{End}_{\mathbb{Q}}(\mathbb{Q} \cdot R^+) : \exists n \in \mathbb{Z}_{>0} : f(R^+) \subset \frac{1}{n} R^+ \right\}$ then it holds that $h(R^+) \subset \frac{1}{m} R^+$ for a $m \in \mathbb{Z}_{>0}$. Then it holds that $m \cdot h(R^+) \subset R^+$ and therefore $m \cdot h \in \text{End}(R^+)$, which again implies that $f \in \mathbb{Q} \cdot \text{End}(R^+)$. ■

Theorem 3.12. *Let K be a number field and let R and R' be subrings of K such that R and R' are commensurable. Then R is firm if and only if R' is firm.*

Proof. Let R and R' be subrings of the number field K and let R and R' be commensurable. Then there exists an $m \in \mathbb{Z}_{>0}$ such that $R \subset \frac{1}{m} R'$ and $R' \subset \frac{1}{m} R$. Hence we have that $\mathbb{Q} \cdot R \subset \mathbb{Q} \cdot R'$ and $\mathbb{Q} \cdot R' \subset \mathbb{Q} \cdot R$. Therefore, we find that $\mathbb{Q} \cdot R = \mathbb{Q} \cdot R'$.

Using $\mathbb{Q} \cdot R = \mathbb{Q} \cdot R'$, we will show that $\mathbb{Q} \cdot \text{End}(R^+) = \mathbb{Q} \cdot \text{End}(R'^+)$, then by lemma 3.10 it will follow that R is firm if and only if R' is firm.

Let $f \in \mathbb{Q} \cdot \text{End}(R^+)$, then $f \in \text{End}_{\mathbb{Q}}(\mathbb{Q} \cdot R^+)$ such that there exists an $n \in \mathbb{Z}_{>0}$ with $f(R^+) \subset \frac{1}{n} R^+$. Then from $\mathbb{Q} \cdot R^+ = \mathbb{Q} \cdot R'^+$ it follows that $f \in \text{End}_{\mathbb{Q}}(\mathbb{Q} \cdot R'^+)$. Lemma 3.11 lets us write $f(R'^+)$ as there exists an $m \in \mathbb{Z}_{>0}$ such that $R \subset \frac{1}{m} R'$ and $R' \subset \frac{1}{m} R$. Hence we find that $f(R'^+) \subset \frac{1}{m^2 n} R'^+$. Thus it follows that $f \in \mathbb{Q} \cdot \text{End}(R'^+)$. Proving $f \in \mathbb{Q} \cdot \text{End}(R'^+)$ implies $f \in \mathbb{Q} \cdot \text{End}(R^+)$ goes analogous. This gives $\mathbb{Q} \cdot \text{End}(R^+) = \mathbb{Q} \cdot \text{End}(R'^+)$. Lastly, applying lemma 3.10 we find that R is firm if and only if R' is firm. ■

Corollary 3.12.1. *Let R be a number ring, then R is firm if and only if $\tilde{R}$ is firm.*

Proof. This follows directly from theorem 3.12 and proposition 3.8. ∎

3.3 Firm number rings of quadratic extensions

Lemma 3.13. *Let K be a finite field extension of $\mathbb{Q}$, and $R \subset K$ a subring. Suppose $I \subset R$ is an ideal with $I \neq (0)$. Then $\#(R/I) < \infty$.*

Proof. Let $\alpha \in I$ such that $\alpha \neq 0$; such an α exists as $I \neq (0)$. Then there exists $n \in \mathbb{Z}_{>0}$ and $a_0, \ldots, a_n \in \mathbb{Q}$ such that not all $a_i = 0$ and

$$\sum_{i=0}^{n} a_i \alpha^i = 0.$$

Without loss of generality, we can assume that $a_0 \neq 0$ and that $a_i \in \mathbb{Z}$. Therefore we obtain that

$$a_0 = -\sum_{i=1}^{n} a_i \alpha^i \in \alpha \cdot \mathbb{Z}[\alpha] \subset I.$$

Hence $I \cap \mathbb{Z} \neq (0)$ and because $a_0 \in I$ we obtain that $a_0 R \subset I$. With Proposition 3.2 we get that $\#(R/a_0R) \leq |a_0|^{[K:\mathbb{Q}]}$ and thus using $a_0 R \subset I$, we find that $\#(R/I) \leq |a_0|^{[K:\mathbb{Q}]} < \infty$. ∎

Lemma 3.14. *Let R be a number ring. If there exists a prime p such that*

$$\#(R/pR) = p,$$

then the ring R is firm.

Proof. By theorem 2.10 it is suffices to show that

$$I := \bigcap_{k=1}^{\infty} p^k R = (0).$$

For every $n \in \mathbb{Z}_{>0}$ we know that $I \subset p^n R$. Now since $\#(R/p^n R) = \#(R/pR)^n = p^n$ due to corollary 3.1.1 and the fact that $\#(R/p^n R) \leq \#(R/I)$ for every $n \in \mathbb{Z}_{>0}$ we get that $p^n \leq \#(R/I)$ for every $n \in \mathbb{Z}_{>0}$. Hence with lemma 3.13 we get that $I = (0)$. ∎

For example, the ring $R = \mathbb{Z}[\frac{1}{2+i}]$ is a firm number ring, which is a subring of $\mathbb{Q}(i)$. The minimum polynomial of $2 + i$ over $\mathbb{Q}$ is given by

$$f_{\mathbb{Q}}^{2+i} = X^2 - 4X + 5$$

from this we deduce that $i = 2 - \frac{5}{2+i}$ and therefore we obtain that $\mathbb{Z}[i] \subset R$. To show that R is firm, we will use lemma 3.14. The ring homomorphism $\mathbb{Z}[X]/(5X^2 - 4X + 1) \to \mathbb{Z}[\frac{1}{2+i}]$ defined by $X \mapsto \frac{1}{2+i}$ and $n \mapsto n$ for every $n \in \mathbb{Z}$ is injective and surjective. Hence it induces a ring isomorphism $\mathbb{Z}[X]/(5, 5X^2 - 4X + 1) \to \mathbb{Z}[\frac{1}{2+i}]/(5)$. Since $\mathbb{Z}[X]/(5, 5X^2 - 4X + 1) = \mathbb{Z}[X]/(5, X + 1)$, we have that $\mathbb{Z}[X]/(5, 5X^2 - 4X + 1) \cong \mathbb{Z}/5\mathbb{Z}$. Thus we find that $\dim_{\mathbb{F}_5}(R/5R) = 1$. Therefore, we get that R is firm.

Lemma 3.15. *Let K be a quadratic extension of $\mathbb{Q}$, and let R be a subring of K such that $R \not\subset \mathbb{Q}$. Let $\mathbb{Z}_{(p)}$ denote the subring $\{\frac{a}{b} \in \mathbb{Q} | a, b \in \mathbb{Z}, b \notin p\mathbb{Z}\}$ of $\mathbb{Q}$. Then for all primes p such that $\dim_{\mathbb{F}_p}(R/pR) = 2$ we have that R is integral over $\mathbb{Z}_{(p)}$.*

Proof. Let p be a prime such that $\dim_{\mathbb{F}_p}(R/pR) = 2$. Then $R/pR = \mathbb{F}_p \cdot \bar{1} \oplus \mathbb{F}_p \cdot \bar{\alpha}$ for all α with $\alpha \notin \mathbb{Z} + pR$. Since $\alpha \in R \setminus (\mathbb{Z} + pR)$ and R is a subring of K we have that there exist $u, v, w \in \mathbb{Z}$ such that $\text{ggd}(u, v, w) = 1$ and

$$u \cdot \alpha^2 + v \cdot \alpha + w = 0.$$

Then it holds that

$$\bar{u} \cdot \bar{\alpha}^2 + \bar{v} \cdot \bar{\alpha} + \bar{w} \cdot 1 = 0$$

as well, and therefore $\bar{u} \neq 0$ as $\bar{\alpha}$ and $\bar{1}$ form a $\mathbb{F}_p$-basis for R/pR. As $\bar{u} \neq 0$ we obtain that $p \nmid u$. Hence we have that

$$\alpha^2 + \tfrac{v}{u} \cdot \alpha + \tfrac{w}{u} = 0$$

with $\frac{v}{u}, \frac{w}{u} \in \mathbb{Z}_{(p)}$. Thus we have for every $\alpha \in R \setminus (\mathbb{Z} + pR)$ that α is integral over $\mathbb{Z}_{(p)}$. We have that $\alpha \notin \mathbb{Z} + pR$ if and only if $\bar{\alpha} \notin \mathbb{F}_p$. As $\dim_{\mathbb{F}_p}(R/pR) = 2$ there exists an $\bar{\alpha} \notin \mathbb{F}_p \cdot \bar{1}$.

Suppose that $\beta \in \mathbb{Z} + pR$ then $\alpha + \beta \notin \mathbb{Z} + pR$ and hence integral over $\mathbb{Z}_{(p)}$. Since $\alpha + \beta$ is integral over $\mathbb{Z}_{(p)}$, we have that $\beta = (\alpha + \beta) - \alpha$ is integral over $\mathbb{Z}_{(p)}$ using lemma 3.5. ■

Lemma 3.16. *Let K be a quadratic extension of $\mathbb{Q}$, and let R be a subring of K such that $R \not\subset \mathbb{Q}$. Suppose that for all primes p we have that $\dim_{\mathbb{F}_p}(R/pR) \in \{0, 2\}$. Then R is integral over $R \cap \mathbb{Q}$.*

Proof. Let us denote with A the ring $R \cap \mathbb{Q}$. We have that A is a Principal Ideal Domain (PID) and that every non-zero prime ideal of A is of the form pA for p a prime number and $\dim_{\mathbb{F}_p}(R/pR) = 2$. For prime numbers p with $\dim_{\mathbb{F}_p}(R/pR) = 0$ we have that $R = pR$ and thus that $\frac{1}{p} \in R$ and hence that $\frac{1}{p} \in A$. Suppose that for all p we have $\dim_{\mathbb{F}_p}(R/pR) = 0$. Then $\mathbb{Q} \subset A$ and it follows that R is integral over A as K is algebraic over $\mathbb{Q}$. So now we can assume there is at least one prime number p such that $\dim_{\mathbb{F}_p}(R/pR) = 2$. Now let $\alpha \in R$ and let

$$\text{den}_A(\alpha) := \left\{ d \in A : \exists n \in \mathbb{Z}_{>0} : d\alpha^n \in \sum_{i=0}^{n-1} A \cdot \alpha^i \right\}$$

then $\text{den}_A(\alpha)$ is an A-ideal, because $d \in \text{den}_A(\alpha)$ implies that for every $r \in A$ we have

$$r(d\alpha^n) \in r\left(\sum_{i=0}^{n-1} A \cdot \alpha^i\right) = \sum_{i=0}^{n-1} rA \cdot \alpha^i = \sum_{i=0}^{n-1} A \cdot \alpha^i.$$

It is also closed under addition. Namely let $d, h \in \text{den}_A(\alpha)$, then

$$d\alpha^n \in \sum_{i=0}^{n-1} A \cdot \alpha^i, \quad h\alpha^k \in \sum_{i=0}^{k-1} A \cdot \alpha^i.$$

Without loss of generality, we suppose that $n \geq k$, then we can write

$$h\alpha^n \in \sum_{i=n-k}^{n-1} A \cdot \alpha^i \subset \sum_{i=0}^{n-1} A \cdot \alpha^i$$

hence we deduce that $d + h \in \mathrm{den}_A(\alpha)$. With lemma 3.15 we know that for every $\alpha \in R$ and for every prime number p such that $\dim_{\mathbb{F}_p}(R/pR) = 2$ that α is integral over $\mathbb{Z}_{(p)}$. So there exists a monic polynomial $f \in \mathbb{Z}_{(p)}[X]$ with $f(\alpha) = 0$ for every such prime number. Clearly there exists a $d \in \mathbb{Z} \setminus p\mathbb{Z}$ such that $d \cdot f \in \mathbb{Z}[X]$ and hence $d \in \mathrm{den}_A(\alpha)$. Since every $\mathrm{den}_A(\alpha)$ is an A-ideal and A is a PID we have that there exists an $\omega \in A$ such that $\omega A = \mathrm{den}_A(\alpha)$. Suppose that $\omega A \subset pA$, then one has that

$$k\mathbb{Z} = \omega A \cap \mathbb{Z} \subseteq pA \cap \mathbb{Z} = p\mathbb{Z}$$

for a certain $k \in \mathbb{Z}$. Now as there exists $d \in \mathrm{den}_A(\alpha)$ such that $d \in \mathbb{Z} \setminus p\mathbb{Z}$ with the fact that $p \mid k$ we get that p should divide d, which gives a contradiction. Hence, for every prime number p with $\dim_{\mathbb{F}_p}(R/pR) = 2$ we get that $\omega A \not\subset pA$, so the ideal is ωA is not contained in any non-zero prime ideal and thus $\omega \in A^*$.

Therefore we have that $\mathrm{den}_A(\alpha) = A$, so for every $\alpha \in R$ we have that there exists an $n \in \mathbb{Z}_{>0}$ such that

$$\alpha^n \in \sum_{i=0}^{n-1} A \cdot \alpha^i$$

and hence every α is integral over A. ■

Lemma 3.17. *Let F be a free R-module, and M an R-submodule with R a* PID*. Then M is free and its rank is less than or equal to the rank of F.*

Proof. We refer to theorem 7.1 in [3]; part one. ■

Lemma 3.18. *Let A be a* PID*, and L be a finite separable extension of its quotient field of degree n. Let B be the integral closure of A in L. Then B is a free module of rank n over A.*

Proof. We refer to theorem 1 in [4]; part one; chapter 2 integral closure. ■

Theorem 3.19. *Let K be a quadratic field extension of $\mathbb{Q}$, and let R be a subring of K such that $R \not\subset \mathbb{Q}$. Then R is either*

(a) firm; and moreover, there exists a prime number p such that $\dim_{\mathbb{F}_p}(R/pR) = 1$,

(b) or R is not firm; and moreover, for all prime numbers p we have that $\dim_{\mathbb{F}_p}(R/pR) \in \{0, 2\}$, and R^+ is a free $(R \cap \mathbb{Q})$-module of rank 2.

Proof. Let K be quadratic extension of $\mathbb{Q}$, and let R be a subring of K such that $R \not\subset \mathbb{Q}$. If there exists a prime p such that $\dim_{\mathbb{F}_p}(R/pR) = 1$, we obtain with lemma 3.14 that R is a firm number ring.

Suppose that there does not exist a prime p such that $\dim_{\mathbb{F}_p}(R/pR) = 1$, so the dimension is either 0 or 2. With lemma 3.16 we have that R is integral over $R \cap \mathbb{Q}$. Let $\tilde{R}$ be the integral closure of R in K, where K is a field extension of $Q(R \cap \mathbb{Q}) = \mathbb{Q}$ of degree 2. Then with lemma 3.18 we find that $\tilde{R}$ is a free $R \cap \mathbb{Q}$-module of rank 2. Because $R \cap \mathbb{Q}$ is a PID and R is a $R \cap \mathbb{Q}$-submodule of $\tilde{R}$ it follows that R is a free $R \cap \mathbb{Q}$-module of rank less than or equal to 2 with lemma 3.17. Now as $R \not\subset \mathbb{Q}$ it cannot be of rank 0 or 1; it has to be of rank 2. Thus R^+ is a free $(R \cap \mathbb{Q})$-module of rank 2, hence

$$M(2, R \cap \mathbb{Q}) \subset \mathrm{End}(R^+).$$

Hence R is not a firm ring by theorem 2.3. ■

4 References

[1] Martin Brandenburg. [online, accessed at 9 June 2023, https://math.stackexchange.com/questions/638582/rings-that-are-isomorphic-to-the-endomorphism-ring-of-their-additive-group].

[2] Fernando Q. Gouvêa. *p-adic Numbers*. Second. 0172-5939. Springer Berlin, Heidelberg, 2012. ISBN: 978-3-642-59058-0.

[3] S. Lang. *Algebra*. Graduate Texts in Mathematics. Springer New York, 2005. ISBN: 9780387953854. URL: https://books.google.nl/books?id=Fge-BwqhqIYC.

[4] S. Lang. *Algebraic Number Theory*. Graduate Texts in Mathematics. Springer, 1994. ISBN: 9780387942254. URL: https://books.google.nl/books?id=u5eGtA0YalgC.

[5] P. Stevenhagen. "Number Rings". [online, accessed at 3 June 2023, https://websites.math.leidenuniv.nl/algebra/ant.pdf].