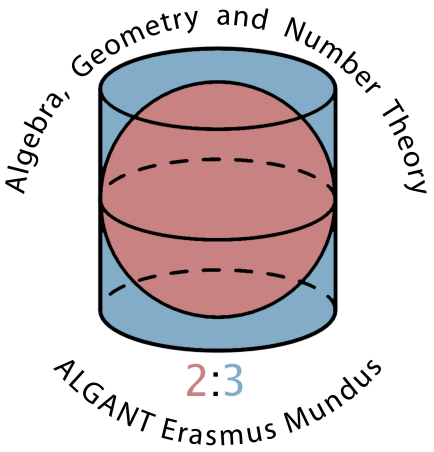
Super-multiplicativity of ideal norms in number fields

Marseglia, S.

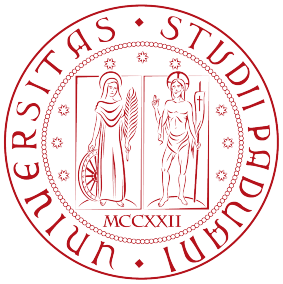


Universiteit Leiden
Mathematisch Instituut

Master Thesis

Super-multiplicativity of ideal norms in number fields

Academic year 2012-2013



Candidate:
Stefano Marseglia

Advisor:
Prof. Bart de Smit

Contents

Introduction

When we are studying a number ring R, that is a subring of a number field K, it can be useful to understand "how big" its ideals are compared to the whole ring. The main tool for this purpose is the norm map:

$$\begin{aligned} N : \mathcal{I}(R) &\longrightarrow \mathbb{Z}_{>0} \\ I &\longmapsto \#R/I \end{aligned}$$

where $\mathcal{I}(R)$ is the set of non-zero ideals of R. It is well known that this map is multiplicative if R is the *maximal order*, or *ring of integers* of the number field. This means that for every pair of ideals $I, J \subseteq R$ we have:

$$N(I)N(J) = N(IJ).$$

For an arbitrary number ring in general this equality fails. For example, if we consider the quadratic order $\mathbb{Z}[2i]$ and the ideal $I = (2, 2i)$, then we have that $N(I) = 2$ and $N(I^2) = 8$, so we have the inequality $N(I^2) > N(I)^2$.

In the first chapter we will recall some theorems and useful techniques of commutative algebra and algebraic number theory that will help us to understand the behaviour of the ideal norm.

In chapter 2 we will see that the inequality of the previous example is not a coincidence. More precisely we will prove that in any quadratic order, for every pair of ideals I, J we have that $N(IJ) \geq N(I)N(J)$. We will call the norm of a number ring *super-multiplicative* if this inequality holds for every pair of ideals. A natural question is if the ideal norm is always super-multiplicative. The answer is negative, and in the end of the second chapter we will exhibit an example which tells us that in a quartic order we cannot prove an analogous theorem.

In a quadratic order every ideal can be generated by 2 elements and in a quartic order by 4 elements, so we are led to wonder if the behaviour of the norm is related to the number of generators and what happens in a cubic order, or more generally in a number ring in which every ideal can be generated by 3 elements.

The rest of this work aims to prove the following:

Main Theorem. *Let R be a number ring. Then the following statements are equivalent:*

1. *every ideal of R can be generated by 3 elements;*
2. *for every ring extension $R \subseteq R' \subseteq \tilde{R}$, where $\tilde{R}$ is the normalization of R, we have that the norm is super-multiplicative.*

In chapter 3 we will prove the that 1 implies 2. It turns out that this proof holds in a more general setting: if I, J are two ideals in a commutative 1-dimensional noetherian domain R, such that IJ can be generated by 3 elements and the norm $N(IJ)$ is finite then we have $N(IJ) \geq N(I)N(J)$.

In chapter 4 we will prove the other implication. We will first deal with local number rings, bounding the number of generators of any ideal. Then we will give a sufficient condition on the behaviour of the ideal norm to prove that this bound is ≤ 3. Finally we will apply this result to the non-local case to complete the proof.

1 Preliminaries

A field K is called *number field* if it is a finite extension of $\mathbb{Q}$. We will say that R is a *number ring* if it is a subring of a number field. A number ring for which the additive group is finitely generated is called *order* in its field of fractions. As every number ring has no non-zero additive torsion element, every order is in fact free as an abelian group of rank $[Q(R) : \mathbb{Q}]$, where $Q(R)$ is the fractions field of R. Number rings satisfy some very interesting properties and we will recall some of them in the following proposition. The proofs can be found in chapter 2 of [PSHNR12].

Proposition 1.1. *Let R be a number ring. Then*

1. *every non-zero R-ideal has finite index;*
2. *R is noetherian;*
3. *if R is not a field then it has Krull dimension 1, that is every non-zero prime ideal is maximal.*

In a domain R with field of fractions K, a *fractional ideal* I is a non-zero R-submodule of K such that $xI \subseteq R$ for some $x \in K^*$. Multiplying by a suitable element of R, we can assume that the element x in the definition is in R. Observe that an R-ideal is just a fractional ideal I with $I \subseteq R$.
The norm of an R-ideal I is defined to be the index of I in R as an additive subgroup

$$N(R) = \#(R/I) = [R : I],$$

which is a finite or cardinal number. We can extend the definition of the index to arbitrary fractional ideals I, J taking:

$$[I : J] = \frac{[I : I \cap J]}{[J : I \cap J]}.$$

It is an easy consequence that we have $[I : J] = [I : H]/[J : H]$ for every fractional ideal H. Now let R be an order and let I be a non-zero ideal of R. For every $x \in K^*$ we have that multiplication by x induces a linear transformation M_x for which we have that

$$|\det(M_x)| = [R : xR] = [I : xI].$$

As a consequence we have that $[R : xI] = N(xR)[R : I]$, which implies that $N(IJ) = N(I)N(J)$ if I or J is principal.

As in this work we aim to study the relation between the norm of an ideal and the number of generators, we will use the following result, which is known as Nakayama's lemma. See [AM69, 2.8, pag. 22] for the proof.

Lemma 1.2. *Let R be a local ring, $\mathfrak{m}$ its maximal ideal, $k = R/\mathfrak{m}$ the residue field. Let M be a finitely generated R-module. Let x_i $(1 \leq i \leq n)$ be elements of M whose images in $M/\mathfrak{m}M$ form a basis of this vector space over k. Then the $x_1, \cdots, x_n$ generate M.*

Let R be a commutative ring with unity and let S be a *multiplicatively closed* subset of R, i.e. a set containing the unity 1 which is closed under multiplication. Then we have the *ring of fractions* $S^{-1}R = \{r/s : r \in R, s \in S\}$, and more generally for every R-module M we can consider $S^{-1}M = \{m/s : m \in M, s \in S\}$. In particular if we choose $S = R \setminus \mathfrak{p}$, where $\mathfrak{p}$ is a prime ideal of R, then $S^{-1}R$ is denoted $R_{\mathfrak{p}}$ and it is called the *localization* of R at $\mathfrak{p}$. The ring $R_{\mathfrak{p}}$ is a local ring with unique maximal ideal $\mathfrak{p}R_{\mathfrak{p}}$. Localizing and more generally formation of fractions commutes with finite sums, finite intersections and quotients. More precisely:

Proposition 1.3. *Let S be a multiplicatively closed subset of a commutative ring R. If N and P are submodules of an R-module M, then*

1. *$S^{-1}(N + P) = S^{-1}(N) + S^{-1}(P)$;*
2. *$S^{-1}(N \cap P) = S^{-1}(N) \cap S^{-1}(P)$;*
3. *the $S^{-1}R$-modules $S^{-1}(M/N)$ and $(S^{-1}M)/(S^{-1}N)$ are isomorphic.*

The proof can be found in [AM69, 3.4, pag. 39]. A natural question is when we obtain the same ring of fractions with different multiplicatively closed subsets. The following proposition gives a nice criterion:

Proposition 1.4. *Let S, T be two multiplicatively closed subsets of a commutative ring R, such that $S \subseteq T$. Let $\phi : S^{-1}R \longrightarrow T^{-1}R$ be the homomorphism that maps $a/s \in S^{-1}R$ to $a/s \in T^{-1}R$. Then ϕ is bijective if and only if for every $t \in T$ there exists $x \in R$ such that $xt \in S$.*

Proof. Assume that ϕ is a bijection. It is surjective and then for every $t \in T$ there exist $a \in R$ and $s \in S$ such that $\phi(a/s) = 1/t$, which means that there exists $y \in T$ such that $(at - s)y = 0$. Moreover ϕ is injective which implies that exists $r \in S$ such that $r(at - s) = 0$, hence $atr = sr \in S$. For the other implication, assume that for every $t \in T$ there exists $x \in R$ with $tx \in S$. If $a/s \in S^{-1}R$ is mapped to 0 in $T^{-1}R$, then there exists $t \in T$ such that $(a - 0s)t = at = 0$. Now using our hypothesis we have that $a(tx) = 0$, for some $x \in R$, and $tx \in S$ so $a/s = 0$ in $S^{-1}R$. So ϕ is injective. For the surjectivity, let b/t be any element in $T^{-1}R$. Then we have that $(bx)/(tx) \in S^{-1}R$ is a preimage of it. □

Another very useful tool for studying modules is the concept of *length*. More precisely let M be an R-module. A *composition series* for M is a finite chain

$$0 = M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n = M,$$

where every factor of the series M_i/M_{i-1} is *simple*, i.e. it is non-zero and it has no proper sub-modules. The length of the series is n. We will use also the Jordan-Hölder theorem, whose proof can be found in [EIS95, 2.13, pag. 72].

Theorem 1.5. *Let R be a ring, M an R- module. M has a finite composition series iff M is Artinian and Noetherian. If M has a finite composition series $0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n = M$ of length n, then*

- *Every chain of submodules of M has length $\leq n$, and can be refined to a composition series.*
- *The sum of the localization maps $M \to M_{\mathfrak{p}}$, for $\mathfrak{p}$ a prime ideal, gives an isomorphism of R-modules*

$$M \simeq \bigoplus_{\mathfrak{m}} M_{\mathfrak{m}},$$

  where the sum is taken over all maximal ideals $\mathfrak{m}$ such that some $M_i/M_{i+1} \simeq R/\mathfrak{m}$. The number of M_i/M_{i+1} isomorphic to $R/\mathfrak{m}$ is the length of $M_{\mathfrak{m}}$ as a module over $R_{\mathfrak{m}}$ and is thus independent of the composition series.
- *We have $M = M_{\mathfrak{m}}$ iff M is annihilated by some power of $\mathfrak{m}$.*

The next proposition gives us a sufficient condition for the finiteness of the length. The proof is a consequence of theorems [AM69, 6.8, pag. 77] and [AM69, 8.5, pag. 90]

Proposition 1.6. *Let R be a commutative ring. Then R has finite length if and only if it is noetherian and zero-dimensional.*

Recall that a commutative ring has Krull dimension 0 if every prime ideal is maximal.

Remark 1.7. *Let R be a commutative ring and I an ideal such that R/I has finite length as an R-module. Consider a composition series, which exists by theorem 1.5*

$$M_0 = \frac{R}{I} \supset M_1 \supset M_2 \supset \cdots \supset M_l = 0.$$

Every factor is simple, so it must be of the form

$$\frac{M_i}{M_{i+1}} \simeq \frac{R}{\mathfrak{m}_i},$$

where $\mathfrak{m}_i$ is a maximal ideal of R. Now, fix a maximal ideal $\mathfrak{m}$. Then we have

$$\#\{i \ : \ \mathfrak{m}_i = \mathfrak{m}\} = l\left(\frac{R_\mathfrak{m}}{I_\mathfrak{m}}\right)$$

as an $R_\mathfrak{m}$-module, because all the factors $R/\mathfrak{m}_i$ disappear if we localize R at $\mathfrak{m} \neq \mathfrak{m}_i$. Hence we get that $l(R/I) = \sum_\mathfrak{m} l(R_\mathfrak{m}/I_\mathfrak{m})$ and

$$N(I) = \#(R/I) = \prod_{\mathfrak{m}\subset R} \#(R/\mathfrak{m})^{l(R_\mathfrak{m}/I_\mathfrak{m})}.$$

So if I is a fractional R-ideal containing R, as the index $[R : I] = 1/[I : R]$, then we can define $l(R/I) = -l(I/R)$.

Now let R be a commutative domain, $\mathfrak{m}$ a maximal ideal. Let J be an ideal of the localization $R_\mathfrak{m}$ such that the $R_\mathfrak{m}$-module $R_\mathfrak{m}/J$ has finite length. Observe that $(J\cap R)_\mathfrak{m} = J$. So we have an injective map $R/(J\cap R) \to R_\mathfrak{m}/J$. Then we get that $R/(J \cap R)$ is annihilated by a power of the maximal ideal $\mathfrak{m}$. Hence by 1.5 we have that the previous map is actually an isomorphism of R-modules and we have

$$l_R\left(\frac{R}{J \cap R}\right) = l_{R_\mathfrak{m}}\left(\frac{R_\mathfrak{m}}{J}\right)$$

where l_R and $l_{R_\mathfrak{m}}$ denote the length as R-module and as $R_\mathfrak{m}$-module respectively.

We will say that a fractional R-ideal I is *invertible* if there exists a fractional ideal J such that $IJ = R$. If I is an R-ideal then, from the definition, it is invertible if there exists another R-ideal J such that IJ is principal. There is a nice criterion to determine whether a fractional ideal is invertible or not. The proof can be found in [MATS95, 11.3, pag. 80].

Theorem 1.8. *Let R be a domain and I a fractional R-ideal. Then I is invertible if and only if the following two conditions hold:*

(1) I is finitely generated;

(2) the localization $I_\mathfrak{m}$ at each maximal ideal $\mathfrak{m}$ of R is a principal fractional $R_\mathfrak{m}$-ideal.

Definition 1.9. *Let R be a commutative ring. We will say that the ideal norm on R is super-multiplicative if for every pair of R-ideals I, J such that $N(IJ)$ is finite we have*

$$N(IJ) \geq N(I)N(J).$$

For brevity we will say that R is super-multiplicative.

Observe that being super-multiplicative is a local property for commutative domains. More precisely:

Lemma 1.10. *Let R be a commutative domain, then R is super-multiplicative if and only if for every maximal ideal $\mathfrak{m}$ we have that $R_{\mathfrak{m}}$ is super-multiplicative.*

Proof. Assume that R is super-multiplicative and let I, J be $R_{\mathfrak{m}}$-ideals with IJ of finite index in $R_{\mathfrak{m}}$. Then we have

$$\begin{aligned}
[R_{\mathfrak{m}} : IJ] &= \#(R/\mathfrak{m})^{l_{R_{\mathfrak{m}}}(R_{\mathfrak{m}}/(IJ))} = \#(R/\mathfrak{m})^{l_R(R/IJ\cap R)} = [R : IJ \cap R] \\
[R_{\mathfrak{m}} : I] &= \#(R/\mathfrak{m})^{l_{R_{\mathfrak{m}}}(R_{\mathfrak{m}}/I)} = \#(R/\mathfrak{m})^{l_R(R/I\cap R)} = [R : I \cap R] \\
[R_{\mathfrak{m}} : J] &= \#(R/\mathfrak{m})^{l_{R_{\mathfrak{m}}}(R_{\mathfrak{m}}/J)} = \#(R/\mathfrak{m})^{l_R(R/J\cap R)} = [R : J \cap R].
\end{aligned}$$

Observe that $(I \cap R)(J \cap R)$ and $(IJ \cap R)$ are equal locally at every maximal ideal, so they are equal also globally. Hence we get that $[R_{\mathfrak{m}} : IJ] \geq [R_{\mathfrak{m}} : I][R_{\mathfrak{m}} : J]$. In the other direction if we have that $R_{\mathfrak{m}}$ is super-multiplicative for every $\mathfrak{m}$, then taking the product of the local norms lead us to have the required inequality also in the global ring. □

Proposition 1.11. *Let R be a number ring, I an invertible R-ideal. Then for every R-ideal J we have*

$$N(I)N(J) = N(IJ).$$

Proof. The localization $I_{\mathfrak{p}}$ at every prime $\mathfrak{p}$ is principal by 1.8, so we have that $[R_{\mathfrak{p}} : J_{\mathfrak{p}}][R_{\mathfrak{p}} : I_{\mathfrak{p}}] = [R_{\mathfrak{p}} : (IJ)_{\mathfrak{p}}]$ for every $\mathfrak{p}$, hence

$$N(IJ) = \prod_{\mathfrak{p}} \#\left(\frac{R_{\mathfrak{p}}}{(IJ)_{\mathfrak{p}}}\right) = \prod_{\mathfrak{p}} \#\left(\frac{R_{\mathfrak{p}}}{I_{\mathfrak{p}}}\right) \prod_{\mathfrak{p}} \#\left(\frac{R_{\mathfrak{p}}}{J_{\mathfrak{p}}}\right) = N(I)N(J).$$

□

Proposition 1.12. *Let R be a noetherian local domain of dimension one, $\mathfrak{m}$ its maximal ideal, $k = R/\mathfrak{m}$ its residue field. Then the following are equivalent:*

1. *R is integrally closed;*

2. *$\mathfrak{m}$ is a principal ideal;*

3. *$\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 1$;*

4. *every non-zero ideal is a power of $\mathfrak{m}$.*

A noetherian local domain of dimension one satisfying one of these conditions is called *discrete valuation ring*, briefly DVR. The proof can be found in [AM69, 9.2, pag. 94]. Then we have a criterion for invertibility for prime ideals of a number ring.

Theorem 1.13. *Let $\mathfrak{p}$ be a prime ideal of a number ring R. Then the following are equivalent:*

(1) $\mathfrak{p}$ is an invertible R-ideal;

(2) $R_\mathfrak{p}$ is a discrete valuation ring.

Proof. See [PSHNR12, 2.17, pag. 22]. □

If these conditions hold for every non-zero prime ideal of a number ring then it is called *Dedekind domain*. In chapter 9 of [AM69] there are several characterizations of Dedekind domains.

Proposition 1.14. *Let R be a noetherian domain of dimension one. Then the following are equivalent:*

(1) R is integrally closed;

(2) $R_\mathfrak{p}$ is a discrete valuation ring, for every maximal ideal $\mathfrak{p}$;

(3) every non-zero fractional ideal is invertible.

In particular, in a Dedekind domain we have that the set of fractional ideals is a multiplicative group. The integral closure of a number ring R, usually denoted $\tilde{R}$, is a Dedekind domain. More precisely we have:

Theorem 1.15. *Let R be a number ring that is Dedekind and let $\mathcal{I}(R)$ be the group of fractional ideals. Then there is an isomorphism*

$$\mathcal{I}(R) \xrightarrow{\sim} \bigoplus_{\mathfrak{p}} \mathbb{Z}$$

that sends $I \mapsto (\mathrm{ord}_\mathfrak{p}(I))_\mathfrak{p}$, where $\mathrm{ord}_\mathfrak{p}(I) = l_{R_\mathfrak{p}}(R_\mathfrak{p}/I_\mathfrak{p})$ and every $I \in \mathcal{I}(R)$ factors uniquely as a product $I = \prod_\mathfrak{p} \mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(I)}$.

Proof. See [PSHNR12, 2.18, pag. 23]. □

Corollary 1.16. *Let R be a number ring. Then R is Dedekind if and only if for every maximal ideal $\mathfrak{p}$ we have $N(\mathfrak{p}^2) = N(\mathfrak{p})N(\mathfrak{p})$.*

Proof. If R is Dedekind then every prime ideal $\mathfrak{p}$ is invertible, hence we have $N(\mathfrak{p}^2) = N(\mathfrak{p})N(\mathfrak{p})$ by 1.11. On the other hand, as $(R/\mathfrak{p}^2)/(\mathfrak{p}/\mathfrak{p}^2) \simeq R/\mathfrak{p}$ then the equality of the norms implies that $\mathfrak{p}/\mathfrak{p}^2$ is 1-dimensional over $R/\mathfrak{p}$. As this holds for every prime then R is Dedekind. □

Proposition 1.17. *Let R be a semilocal commutative domain, i.e. a domain with a finite number of maximal ideals. Then, a fractional ideal over R is invertible if and only if it is principal and non-zero. In particular, a semilocal Dedekind domain, like the normalization of any local number ring, is a principal ideal domain.*

Proof. Observe that if $x \in R$ is non-zero, then the ideal (x) has inverse (x^{-1}). So only the converse needs to be proved. Suppose that I is an invertible R-ideal, with inverse J, i.e. $IJ = R$. Let $\mathfrak{m}_1, \cdots, \mathfrak{m}_l$ be the maximal ideals of R. As $IJ \nsubseteq \mathfrak{m}_k$ for every k, there exist $a_k \in I, b_k \in J$ such that $a_k b_k \in R \setminus \mathfrak{m}_k$. By maximality $\mathfrak{m}_j \nsubseteq \mathfrak{m}_k$, whenever $j \neq k$. Then there exists $\lambda_{jk} \in \mathfrak{m}_j \setminus \mathfrak{m}_k$. Calling $\lambda_k = \prod_{j \neq k} \lambda_{jk}$, we obtain $\lambda_k \in \mathfrak{m}_j$ for all $j \neq k$ and, as $\mathfrak{m}_k$ is prime, $\lambda_k \notin \mathfrak{m}_k$. Then, writing

$$a = \lambda_1 a_1 + \cdots + \lambda_n a_n \in I, \quad b = \lambda_1 b_1 + \cdots + \lambda_n b_n \in J$$

we can expand the product to get

$$ab = \sum_{i,j} \lambda_i \lambda_j a_i b_j. \tag{1}$$

However, $a_i b_j \in IJ = R$ so $\lambda_i \lambda_j a_i b_j$ is in $\mathfrak{m}_k$ whenever either i or j is not equal to k. On the other hand, $\lambda_k \lambda_k a_k b_k \notin \mathfrak{m}_k$ and, consequently, there is exactly one term on the right hand side of (1) which is not in $\mathfrak{m}_k$, so $ab \notin \mathfrak{m}_k$.

We have shown that ab is not in any maximal ideal of R, and must therefore be a unit. So a is non-zero and,

$$(a) \subseteq I = abI \subseteq aJI = aR = (a)$$

as required. □

It is very interesting to understand the behaviour of prime ideals when we are extending a number field to a bigger one. More precisely let K be a number field with ring of integers R and let $L = K(\alpha)$ be an algebraic

extension with ring of integers S. Denote by $p(X) \in R[X]$ the minimal polynomial of α over the field K. The following theorem from [NEU95, 8.3, pag. 47] gives us a very useful tool to describe the ramification of a prime ideal $\mathfrak{p}$ of R when extended to S. Recall that the conductor of a number ring T with normalization $\tilde{T}$ is given by

$$\mathfrak{f}_T = \left\{ x \in \tilde{T} \ : \ x\tilde{T} \subset T \right\}$$

and has the property that a prime ideal $\mathfrak{p}$ of T divides $\mathfrak{f}_T$ if and only if it is not invertible.

Theorem 1.18. *Let $\mathfrak{p}$ be a prime ideal of R which is relatively prime to the conductor $\mathfrak{f}$ of $R[\alpha]$, and let*

$$\overline{p}(X) = \overline{p}_1(X)^{e_1} \cdots \overline{p}_r(X)^{e_r}$$

be the factorization of the polynomial $\overline{p}(X) = p(X) \bmod \mathfrak{p}$ into irreducibles $\overline{p}_i(X) \equiv p_i(X) \bmod \mathfrak{p}$ over the residue class field $R/\mathfrak{p}$, with all $p_i(X) \in R[X]$ monic. Then

$$\mathfrak{P}_i = \mathfrak{p}R + p_i(\alpha)R \quad i = 1, \cdots, r$$

are the different prime ideals of S above $\mathfrak{p}$. The inertia degree f_i of $\mathfrak{P}_i$, that is the degree of the extension $(S/\mathfrak{P}_i)/(R/\mathfrak{p})$, is the degree of $p_i(X)$, and one has

$$\mathfrak{p}S = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}.$$

A very useful tool when we are dealing with extensions of fields is the tensor product. It can be defined via the following universal property, as in [AM69, 2.12, pag. 24].

Proposition 1.19. *Let M, N be R-modules. Then there exists a pair (T, g) consisting of an R-module T and an R-bilinear mapping $g : M \times N \to T$, with the following property: given any R-module P and any R-bilinear mapping $f : M \times N \to P$, there exists a unique R-linear mapping $f' : T \to P$ such that $f = f' \circ g$ (in other words, every bilinear function on $M \times N$ factors through T). Moreover, if (T, g) and (T', g') are two pairs with this property, then there exists a unique isomorphism $j : T \to T'$ such that $j \circ g = g'$.*

This unique up to (a unique) isomorphism module T is called *tensor product* over R of M and N and it is denoted $M \otimes_R N$. It can be proved that the tensor product is right exact, which means that if we have an exact sequence of R-modules

$$M \longrightarrow N \longrightarrow P \longrightarrow 0,$$

and let S be any R-module, then

$$M \otimes_R S \longrightarrow N \otimes_R S \longrightarrow P \otimes_R S \longrightarrow 0$$

is exact. There are several canonical isomorphisms:

Proposition 1.20. *Let M, N, P be R-modules. Then there exist natural isomorphisms*

1. $M \otimes N \simeq N \otimes M$
2. $(M \otimes N) \otimes P \simeq M \otimes (N \otimes P) \simeq M \otimes N \otimes P$
3. $(M \oplus N) \otimes P \simeq (M \oplus P) \otimes (N \oplus P)$
4. $R \otimes M \simeq M$

Let R, S be rings, let M be an R-module, P a S-module and N an (R, S)-bimodule. Then $M \otimes_R N$ is naturally a S-module, $N \otimes_S P$ an R-module, and we have

$$(M \otimes_R N) \otimes_S P \simeq M \otimes_R (N \otimes_S P)$$

Proof. See [AM69, 2.14,2.15 pag. 26-27]. □

A nice application of the tensor product is a generalization of the Chinese Reminder theorem.

Theorem 1.21. *Let R be a commutative ring and let $\mathfrak{a}_1, \cdots, \mathfrak{a}_l$ be R-ideals such that $\mathfrak{a}_i + \mathfrak{a}_j = R$ for every $i \neq j$. Let M be an R-module. Then*

$$\frac{M}{\mathfrak{a}_1 \cdots \mathfrak{a}_l M} \simeq \frac{M}{\mathfrak{a}_1 M} \times \cdots \frac{M}{\mathfrak{a}_l M}$$

Proof. The Chinese Remainder Theorem says that we have

$$\frac{R}{\mathfrak{a}_1 \cdots \mathfrak{a}_l} \simeq \frac{R}{\mathfrak{a}_1} \times \cdots \times \frac{R}{\mathfrak{a}_l}.$$

Using the canonical isomorphism $R/I \otimes_R M \simeq M/IM$ for every R-ideal I, we obtain the desired isomorphism. □

When we are extending rings it is very useful to know if a maximal ideal remains maximal. If the extension is integral, this situation can be described very precisely. In fact:

Proposition 1.22. *Let $R \subset S$ be rings, S integral over R; let $\mathfrak{q}$ be a prime ideal of S and let $\mathfrak{p} = \mathfrak{q} \cap R$. Then $\mathfrak{q}$ is maximal if and only if $\mathfrak{p}$ is maximal.*

Proof. See [AM69, 5.8 pag. 61]. □

2 Quadratic and quartic case

Lemma 2.1. *Let R be an order in a quadratic field K. Let I be an R-ideal and let R_I be its multiplier ring, i.e. $R_I = \{x \in K : \ xI \subseteq I\}$. Then I is an invertible ideal of R_I.*

Proof. I is an ideal of an order in a quadratic number field, so in particular it is a free $\mathbb{Z}$-module of rank 2 and so it is finitely generated. To show that it is invertible as R_I-ideal, by theorem 1.8 it suffices to show that every localization at a maximal ideal $\mathfrak{p}$ of R_I is invertible or, equivalently, principal. Assume that it is not, i.e. there exists a maximal ideal $\mathfrak{p}$ such that $I_\mathfrak{p}$ is not invertible. Observe that if $\mathfrak{p}$ is above the rational prime number p, then we cannot have $pR_I = \mathfrak{p}$, because by 1.13 it would be invertible, hence $R_{I\mathfrak{p}}$ would be a PID and so also $I_\mathfrak{p}$ would be invertible.
We know that $[R_I : pR_I] = p^2$ and $pR_I \subsetneq \mathfrak{p}$. In other words we have

$$pR_I \overset{p}{\subsetneq} \mathfrak{p} \overset{p}{\subsetneq} R_I.$$

Now observe that also $[I : pI] = p^2$ as it is a free $\mathbb{Z}$-module of rank 2. Now look at the dimension of $I_\mathfrak{p}/(\mathfrak{p}I)_\mathfrak{p}$ over $R_{I\mathfrak{p}}/\mathfrak{p}R_{I\mathfrak{p}} \simeq \mathbb{F}_p$. It cannot be more than 2, because I can be generated by 2 elements over R_I, then the same holds for $I_\mathfrak{p}$ over $R_{I\mathfrak{p}}$ and hence $I_\mathfrak{p}/(\mathfrak{p}I)_\mathfrak{p}$ can be generated by 2 elements over $R_{I\mathfrak{p}}/\mathfrak{p}R_{I\mathfrak{p}}$. So in particular we have two possibilities:

$$\#\frac{I_\mathfrak{p}}{(\mathfrak{p}I)_\mathfrak{p}} = \begin{cases} p \\ p^2 \end{cases}$$

If it is equal to p then the group is cyclic and by 1.2 we have that $I_\mathfrak{p}$ is principal $R_\mathfrak{p}$-ideal and hence invertible. Contradiction. Observe that also the converse holds: if $I_\mathfrak{p}$ is principal, then the dimension of $I_\mathfrak{p}/(\mathfrak{p}I)_\mathfrak{p}$ is 1 and hence it has p elements. If the dimension is 2, then we also have that $\#I/\mathfrak{p}I = p^2$ (it cannot have fewer elements) and so we have that

$$\underbrace{pI \subset \overbrace{\mathfrak{p}I \subset I}^{p^2}}_{p^2},$$

which implies $pI = \mathfrak{p}I$, so by the definition of multiplier ring $p^{-1}\mathfrak{p} \subseteq R_I$, hence $pR_I = \mathfrak{p}$ by the maximality of $\mathfrak{p}$. Contradiction.
So I is an invertible R_I-ideal. □

Lemma 2.2. *Let R be an order in a quadratic number field K and consider the localizations at a prime number $p \in \mathbb{Z}$, namely $\tilde{R}_{(p)} = \tilde{R} \otimes \mathbb{Z}_{(p)}$ and $R_{(p)} = R \otimes \mathbb{Z}_{(p)}$. Then we have that $\tilde{R}_{(p)}/R_{(p)} \simeq \mathbb{Z}/p^n\mathbb{Z}$ for some $n \in \mathbb{Z}_{\geq 0}$.*

Proof. As both R and $\tilde{R}$ are orders in a quadratic number field, we have that they are free $\mathbb{Z}$-modules of rank 2, i.e. there exist $\alpha \in R$ and $\beta \in \tilde{R}$ such that $R = \mathbb{Z} \oplus \alpha\mathbb{Z}$ and $\tilde{R} = \mathbb{Z} \oplus \beta\mathbb{Z}$. Then observe that:

$$\frac{\tilde{R}}{R} = \frac{\mathbb{Z} \oplus \beta\mathbb{Z}}{\mathbb{Z} \oplus \alpha\mathbb{Z}} \simeq \frac{\beta\mathbb{Z}}{(\mathbb{Z} \oplus \alpha\mathbb{Z}) \cap \beta\mathbb{Z}},$$

so it is cyclic with generator $\overline{\beta}$. Hence

$$\frac{\tilde{R}_{(p)}}{R_{(p)}} \simeq \frac{\beta\mathbb{Z}_{(p)}}{(\mathbb{Z}_{(p)} \oplus \alpha\mathbb{Z}_{(p)}) \cap \beta\mathbb{Z}_{(p)}} = \left\langle \frac{\overline{\beta}}{1} \right\rangle.$$

So we need to prove that the order of the generator is a p-power.
Let $m = \mathrm{ord}(\overline{\beta}) = p^a \cdot t$, with $(p, t) = 1$. As

$$p^a \cdot \left(\frac{\overline{\beta}}{1}\right) = p^a \cdot \left(\overline{\beta} \cdot \frac{t}{t}\right) = \overline{0},$$

we obtain that $\mathrm{ord}(\overline{\beta}/1)$ divides p^a and so it is a p-power. □

Theorem 2.3. *The ideal norm in any quadratic order is super-multiplicative.*

Proof. Let R be a quadratic order and I, J two ideals of R. We want to show that

$$\frac{[R : IJ]}{[R : I][R : J]} \geq 1.$$

Now if we look at our inequality locally at p we consider:

$$\frac{[R_{(p)} : I_{(p)}J_{(p)}]}{[R_{(p)} : I_{(p)}][R_{(p)} : J_{(p)}]}. \qquad (*)$$

By lemma 2.1 we have that I and J are invertible in their multiplier rings. So their localizations at (p) are principal by 1.17, because the rings $R_{I(p)}$ and $R_{J(p)}$ are semilocal. Say that we have $I_{(p)} = xR_{I(p)}$ and $J_{(p)} = yR_{J(p)}$. Moreover observe that $R_{I(p)}$ and $R_{J(p)}$ are both $R_{(p)}$-fractional ideals. So we have that

$$\begin{aligned}
[R_{(p)} : I_{(p)}] &= [R_{(p)} : R_{I(p)}][R_{(p)} : xR_{(p)}] \\
[R_{(p)} : J_{(p)}] &= [R_{(p)} : R_{J(p)}][R_{(p)} : yR_{(p)}] \\
[R_{(p)} : I_{(p)}J_{(p)}] &= [R_{(p)} : xR_{I(p)}yR_{J(p)}] = \\
&= [R_{(p)} : R_{I(p)}R_{J(p)}][R_{(p)} : xR_{(p)}][R_{(p)} : yR_{(p)}]
\end{aligned}$$

If we substitute these equalities in (*) we get:

$$\frac{[R_{(p)} : R_{I(p)}R_{J(p)}]}{[R_{(p)} : R_{I(p)}][R_{(p)} : R_{J(p)}]} = \frac{[R_{I(p)} : R_{(p)}][R_{J(p)} : R_{(p)}]}{[R_{I(p)}R_{J(p)} : R_{(p)}]}.$$

As $\tilde{R}_{(p)}/R_{(p)}$ is a cyclic p-group by 2.2, the lattice of its subgroups is totally ordered w.r.t. the inclusion relation. Then as $R \subseteq R_I, R_J \subseteq \tilde{R}$, where R_I and R_J are the two multiplier rings of I and J, we have that $R_{I(p)} \subseteq R_{J(p)}$ or viceversa. Assume that $R_{I(p)} \subseteq R_{J(p)}$ (otherwise swap I and J) then $R_{I(p)}R_{J(p)} = R_{J(p)}$. So we have:

$$\frac{[R_{I(p)} : R_{(p)}][R_{J(p)} : R_{(p)}]}{[R_{I(p)}R_{J(p)} : R_{(p)}]} = \frac{[R_{I(p)} : R_{(p)}][R_{J(p)} : R_{(p)}]}{[R_{J(p)} : R_{(p)}]} = [R_{I(p)} : R_{(p)}] \geq 1.$$

As this inequality holds for the localization at every rational prime p, then it holds also for the original quotient, because from 1.5 we have that for every R-ideal I, R/I is a $\mathbb{Z}$-module of finite length and we have:

$$\frac{R}{I} \simeq \bigoplus_p \left(\frac{R}{I}\right)_{(p)} \simeq \frac{R_{(p)}}{I_{(p)}}.$$

So, looking at the norms:

$$N(IJ) = \prod_p \left(\#\frac{R_{(p)}}{(IJ)_{(p)}}\right) \geq \prod_p \left(\#\frac{R_{(p)}}{I_{(p)}}\right) \prod_p \left(\#\frac{R_{(p)}}{J_{(p)}}\right) = N(I)N(J).$$

□

As we have understood the quadratic case, then we will move to extensions of $\mathbb{Q}$ of higher degree. The next example shows that we cannot prove an analogous theorem for the quartic case.

Example 2.4. *Consider the field $\mathbb{Q}(\alpha)$, where α is the root of an irreducible polynomial in $\mathbb{Z}[X]$ of degree 4. Take the order $R = \mathbb{Z}[\alpha]$ and define $S = \mathbb{Z} + pR \subset R$, where p is a rational prime number. Observe that also S is an order. Consider the S-fractional ideals $I = S \cdot 1 + S\alpha$ and $J = S \cdot 1 + S\alpha^2$, which have $\mathbb{Z}$-basis $1, \alpha, p\alpha^2, p\alpha^3$ and $1, p\alpha, \alpha^2, p\alpha^3$, respectively. So in particular they have index*

$$[I : S] = [J : S] = p,$$

hence $N(I) = N(J) = p^{-1}$, where we consider the norm w.r.t. S. Their product is $IJ = R$, which contains S with index p^3, so we have the inequality:

$$p^{-2} = N(I)N(J) > N(IJ) = p^{-3}.$$

So if we define $I' = pI, J' = pJ$ *and* $R' = pR$ *then* $N(I') = N(J') = p^3$ *and* $N(R') = p$. *Hence*

$$p^6 = N(I')N(J') > N(I'J') = N(p^2R) = p^5.$$

Moreover as $IR = R$ *then*

$$p^{-4} = N(I)N(R) < N(R) = p^{-3},$$

or equivalently

$$p^4 = N(R')N(I') < N(I'R') = N(p^2R) = p^5$$

and so we have both the inequalities.

3 Main theorem: first implication

In the previous section we have seen that in a quadratic order we always have that the norm is super-multiplicative. Observe that in a quadratic order every ideal can be generated by 2 elements. Moreover we have seen that in a quartic order, where every ideal can be generated by 4 elements, we cannot state something analogous about the ideal norm. So the natural question is what happens if we deal with ideals generated by 3 elements.

Definition 3.1. *Let R be a commutative ring. We define*

$$g(R) = \sup_{\substack{I \subset R \\ ideal}} \Big(\inf_{\substack{S \subset I \\ I = \langle S \rangle}} \#S \Big).$$

Remark 3.2. *Let R be a commutative domain. Observe that $g(R)$ is also the bound for the cardinality of a minimal set of generators for every fractional ideal I. In fact, by the definition of fractional ideal, there exists a non-zero element x in the fraction field of R such that $xI \subseteq R$. So xI is an R-ideal and hence can be generated by $g(R)$ elements, so I can be generated by the same elements divided by x.*

Remark 3.3. *Let $R \subset R'$ be an extension of commutative domains such that the abelian group R'/R has finite exponent, say n. Then we have that $g(R') \leq g(R)$. In fact if J is an R'-ideal, then $nJ \subseteq R$ can be generated by $g(R)$ elements. So J can be generated by the same elements divided by n.*

Remark 3.4. *Let R be a number ring inside a number field K. We have $g(R) \leq [K : \mathbb{Q}]$ and this bound is sharp, in the sense that we can find an order R' in K such that $g(R') = [K : \mathbb{Q}]$. Let $\mathcal{O}_K$ be the maximal order of K. Let I be any R-ideal. As R is noetherian, I can be generated by a finite set of elements, say $x_1, \cdots, x_d$. We can find an integer $n \geq 1$ such that $nx_1, \cdots, nx_d \in \mathcal{O}_K$. Then observe that $I' = nI \cap (\mathcal{O}_K \cap R)$ is an ideal of $\mathcal{O}_K \cap R$, so it is generated over $\mathbb{Z}$ by at most $[K : \mathbb{Q}]$ elements, say $\alpha_1, \cdots, \alpha_{[K:\mathbb{Q}]}$. As $I'R = nI$, we have that $\alpha_1/n, \cdots, \alpha_{[K:\mathbb{Q}]}/n$ generate I over R. Hence $g(R) \leq [K : \mathbb{Q}]$. To prove the second part, let α be an algebraic integer such that $K = \mathbb{Q}(\alpha)$. Consider $R' = \mathbb{Z} + p\mathbb{Z}[\alpha]$ where p is a rational prime number. Then $\mathfrak{m} = p\mathbb{Z}[\alpha]$ is a maximal ideal of R' and $\dim_{\mathbb{F}_p} \mathfrak{m}/\mathfrak{m}^2 = [K : \mathbb{Q}]$, so $g(R') = [K : \mathbb{Q}]$.*

We have a nice description of the behaviour of $g(R)$ for a number ring R when we localize at a prime ideal.

Lemma 3.5. *Let R be a number ring, with normalization $\tilde{R}$. Let I be an R-ideal. For every integer $d \geq 2$ the following are equivalent:*

1. *the R-ideal I can be generated by d elements;*

2. *for every prime ideal $\mathfrak{p}$ of R, the $R_\mathfrak{p}$-ideal $I_\mathfrak{p}$ can be generated by d elements.*

Proof. Observe that 1 implies 2 is a consequence of the fact that $(I_\mathfrak{p} \cap R)_\mathfrak{p} = I_\mathfrak{p}$. For the other direction, assume that $I_\mathfrak{p}$ is d-generated, for every $\mathfrak{p}$. Observe that we can choose the local generators to be in I, just multiplying by the common denominator, which is a unit in $R_\mathfrak{p}$. Now, as $\tilde{R}/R$ is a finite R-module, it has finite length. Consider a composition series

$$\tilde{R}/R = M_0 \supset M_1 \supset \cdots \supset M_l = 0.$$

All the factors M_i/M_{i+1} for $i = 0, \cdots, l-1$ are simple, hence of the form $R/\mathfrak{p}_i$, for a maximal R-ideal $\mathfrak{p}_i$. Observe that if we localize at a maximal ideal $\mathfrak{p} \neq \mathfrak{p}_i$, for $i = 0, \cdots, l-1$, all the factors disappear, and hence we have that $\tilde{R}_\mathfrak{p} = R_\mathfrak{p}$. Hence $R_\mathfrak{p}$ is a principal ideal domain and then $I_\mathfrak{p}$ is also principal. As the factors of the composition series are a finite number this situation occurs for almost all maximal ideals of R. Hence $I/\mathfrak{p}I \simeq I_\mathfrak{p}/\mathfrak{p}I_\mathfrak{p}$ is a 1-dimensional $R/\mathfrak{p}$-vector space for almost all maximal ideals. Then consider the finite set $S = \left\{\mathfrak{p} : \dim_{(R/\mathfrak{p})} I/\mathfrak{p}I \neq 1\right\}$. By the Chinese Remainder Theorem 1.21 we can pick an element $x_1 \in I$ such that $x_1 \notin \mathfrak{p}I$ for every $\mathfrak{p} \in S$. Then consider $T = \{\mathfrak{p} : I \supsetneq \mathfrak{p}I + (x_1)\}$, it is also finite because the ideals I and (x_1) are locally equal for almost all prime ideals of R. Then we can build a set of global generators in the following way: with the Chinese Remainder Theorem take $x_2 \in I \setminus (\mathfrak{p}I + (x_1))$ for every $\mathfrak{p} \in T$, $x_3 \in I \setminus (\mathfrak{p}I + (x_1, x_2))$ for every $\mathfrak{p} \in T$ such that I is not equal to $\mathfrak{p}I + (x_1, x_2)$, and so on until x_d. Then observe that $x_1, x_2, \cdots, x_d$ is a set of generators for I, because it is so locally at every prime: if $\mathfrak{p} \in S$ then $I_\mathfrak{p} = (x_1, x_2, \cdots, x_d)$ by construction, if $\mathfrak{p} \in T \setminus S$ then $I_\mathfrak{p} = (x_2)$ and if $\mathfrak{p} \notin T$ then $I_\mathfrak{p} = (x_1)$. Now observe that $I = \bigcap_\mathfrak{p} I_\mathfrak{p}$ and so $x_1, x_2, \cdots, x_d$ generates the ideal I over R. □

Corollary 3.6. *Let R be a number ring. If $g(R_\mathfrak{p}) > 1$ for some prime R-ideal then*

$$g(R) = \sup_\mathfrak{p} g(R_\mathfrak{p}).$$

Remark 3.7. *Let R be a number ring such that $g(R_\mathfrak{p}) = 1$ for every prime ideal, then R is a Dedekind domain because every ideal I has principal localizations, hence I is invertible. Similarly as in the proof of the previous lemma, we can show that $g(R) \leq 2$.*

Now that we have introduced some notation, we can start proving the first implication of the main theorem.

Lemma 3.8. *Let U, V, W be vector spaces over a field k, with W of dimension ≥ 2. Let $\varphi : U \otimes V \twoheadrightarrow W$ be a surjective linear map. Then there exists an element $u \in U$ such that $\dim_k \varphi(u \otimes V) \geq 2$, or there exists an element $v \in V$ such that $\dim_k \varphi(U \otimes v) \geq 2$.*

Proof. By contradiction, assume that $\varphi(u \otimes V)$ and $\varphi(U \otimes v)$ have dimension ≤ 1, for every choice of $u \in U$ and $v \in V$. Observe that $\{\varphi(u \otimes v) : u \in U, v \in V\}$ is a set of generators of the image of φ, hence of W as φ is surjective. As W has dimension ≥ 2 then among these generators there are 2 which are linearly independent, say $w_1 = \varphi(u_1 \otimes v_1)$ and $w_2 = \varphi(u_2 \otimes v_2)$. Observe

$$\varphi(u_1 \otimes v_2) \in \varphi(u_1 \otimes V) \cap \varphi(U \otimes v_2) = kw_1 \cap kw_2 = 0.$$

Then we have that $\varphi(u_1 \otimes v_2) = 0$. Similarly we obtain also $\varphi(u_2 \otimes v_1) = 0$. But then we have that both $\varphi((u_1 + u_2) \otimes v_1) = w_1$ and $\varphi((u_1 + u_2) \otimes v_2) = w_2$ are in $\varphi((u_1 + u_2) \otimes V)$. So it contains two linearly independent vectors and then it must have dimension ≥ 2. Contradiction. □

Theorem 3.9. *Let R be a commutative domain and $I, J \subset R$ two non-zero ideals, such that IJ can be generated by 3 elements. Let $\mathfrak{m} \subset R$ be a maximal ideal. Then there exists a non-zero $x \in I_\mathfrak{m}$ such that $(IJ)_\mathfrak{m}/xJ_\mathfrak{m}$ is cyclic as $R_\mathfrak{m}$-module, or there exists a non-zero $x \in J_\mathfrak{m}$ such that $(IJ)_\mathfrak{m}/xI_\mathfrak{m}$ is cyclic as $R_\mathfrak{m}$-module. Moreover there exists a generator of this cyclic module which is of the form $\overline{ij}$ with $i \in I_\mathfrak{m}, j \in J_\mathfrak{m}$.*

Proof. Observe that since $IJ/\mathfrak{m}IJ$ is a k-vector space of dimension ≤ 3, also the localization $W = (IJ)_\mathfrak{m}/\mathfrak{m}(IJ)_\mathfrak{m}$ has dimension non-zero and ≤ 3. First, if W is a k-vector space of dimension 1 then by 1.2 we have that $(IJ)_\mathfrak{m}$ is a cyclic $R_\mathfrak{m}$-ideal and then there exists $x \in I_\mathfrak{m}$ such that $(IJ)_\mathfrak{m}/xJ_\mathfrak{m}$ is cyclic. If the dimension of W is ≥ 2, then consider the product map:

$$\begin{aligned} \varphi : \frac{I_\mathfrak{m}}{\mathfrak{m}I_\mathfrak{m}} \otimes \frac{J_\mathfrak{m}}{\mathfrak{m}J_\mathfrak{m}} &\longrightarrow W \\ \overline{i} \otimes \overline{j} &\longmapsto \overline{ij} \end{aligned}$$

It is a surjective linear map of k-vector spaces and the image has dimension ≥ 2. Then by 3.8 (swapping I and J if necessary) there exists $x \in I_\mathfrak{m}$ such that $\varphi(x \otimes (J_\mathfrak{m}/\mathfrak{m}J_\mathfrak{m}))$ has dimension ≥ 2. So the quotient space

$$\frac{W}{\varphi(x \otimes (J_\mathfrak{m}/\mathfrak{m}J_\mathfrak{m}))} \simeq \frac{(IJ)_\mathfrak{m}}{xJ_\mathfrak{m} + \mathfrak{m}(IJ)_\mathfrak{m}}$$

has dimension ≤ 1. Moreover, it is not difficult to see that it is isomorphic to $S/\mathfrak{m}S$, where $S = (IJ)_\mathfrak{m}/xJ_\mathfrak{m}$. So by 1.2 we have that S is a cyclic $R_\mathfrak{m}$-module.
We can be more precise saying that every generator is of the form $\sum_{t\in T} \overline{i_t j_t}$, where T is a finite set of indices, $i_t \in I_\mathfrak{m}$ and $j_t \in J_\mathfrak{m}$. So in particular $\left\{\overline{i_t j_t}\right\}_{t\in T}$ is a finite set of generators for S. As the k-vector space $S/\mathfrak{m}S$ is 1-dimensional, among the projections $\overline{i_t j_t}$ there exists one $\overline{i_{t_0} j_{t_0}}$ which is a basis. Hence, again by 1.2, $i_{t_0} j_{t_0}$ is a generator of S. □

Corollary 3.10. *Using the same notation as in theorem 3.9, the morphism of $R_\mathfrak{m}$-modules "multiplication by j"*

$$\frac{I_\mathfrak{m}}{xR_\mathfrak{m}} \xrightarrow{\cdot j} \frac{(IJ)_\mathfrak{m}}{xJ_\mathfrak{m}}$$

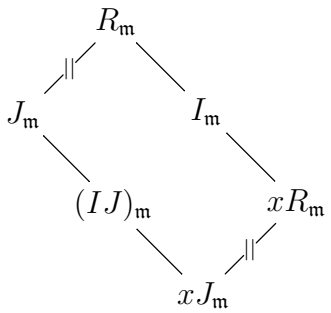
is surjective.

Proof. This follows from the fact that $(IJ)_\mathfrak{m}/xJ_\mathfrak{m}$ is generated by one element exactly of the form ij, with $i \in I_\mathfrak{m}$. □

Theorem 3.11. *Let R be a commutative noetherian 1-dimensional domain. Let I, J be two non-zero ideals such that IJ can be generated by 3 elements. Then we have that*

$$l\left(\frac{R_\mathfrak{m}}{I_\mathfrak{m}}\right) + l\left(\frac{R_\mathfrak{m}}{J_\mathfrak{m}}\right) \leq l\left(\frac{R_\mathfrak{m}}{(IJ)_\mathfrak{m}}\right)$$

Proof. Swapping I and J if necessary, let $x \in I_\mathfrak{m}$ be as in the statement of theorem 3.9, so in particular it is non-zero. Consider the ring $R_\mathfrak{m}/xJ_\mathfrak{m}$. It has finite length by proposition 1.6 because it is noetherian and zero-dimensional. Consider the two chains of ideals of $R_\mathfrak{m}$:



These two chains define two series for $R_\mathfrak{m}/xJ_\mathfrak{m}$, and they can be refined in composition series, which will have the same length and same factors (up to the order) by theorem 1.5. Observe that the multiplication by x is an

isomorphism of $R_\mathfrak{m}$ onto $xR_\mathfrak{m}$ and of $J_\mathfrak{m}$ onto $xJ_\mathfrak{m}$, so it induces a R-module isomorphism also on the quotients. Hence we have $l(R_\mathfrak{m}/J_\mathfrak{m}) = l(xR_\mathfrak{m}/xJ_\mathfrak{m})$ and as the diagram of inclusions is commutative we have also $l(R_\mathfrak{m}/xR_\mathfrak{m}) = l(J_\mathfrak{m}/xJ_\mathfrak{m})$. Moreover, as $I_\mathfrak{m}/xR_\mathfrak{m}$ is mapped onto $(IJ)_\mathfrak{m}/xJ_\mathfrak{m}$ by 3.10, for every factor of the composition series between $R_\mathfrak{m}$ and $I_\mathfrak{m}$ there exists a corresponding factor between $J_\mathfrak{m}$ and $(IJ)_\mathfrak{m}$. So we have

$$l\left(\frac{R_\mathfrak{m}}{I_\mathfrak{m}}\right) \leq l\left(\frac{J_\mathfrak{m}}{(IJ)_\mathfrak{m}}\right).$$

To get our thesis is sufficient to add on both sides $l(R_\mathfrak{m}/J_\mathfrak{m})$. □

Observe that this last result allows us to prove the first implication of the main theorem:

Corollary 3.12. *Let R be a number ring such that $g(R) \leq 3$, then R is super-multiplicative.*

Proof. Remember that a number ring is a 1-dimensional noetherian domain. As every ideal can be generated by 3 elements, for every pair of non-zero ideals from 3.11 we get

$$\#(R/\mathfrak{m})^{l(R_\mathfrak{m}/(IJ)_\mathfrak{m})} \geq \#(R/\mathfrak{m})^{l(R_\mathfrak{m}/I_\mathfrak{m})+l(R_\mathfrak{m}/J_\mathfrak{m})},$$

for every maximal R-ideal $\mathfrak{m}$. Hence by remark 1.10 we get

$$N(IJ) \geq N(I)N(J).$$

□

4 Main theorem: second implication

In the next lemmas and theorems we will exhibit a bound for $g(R)$ for a local number ring R depending on the extension of its maximal ideal in the normalization $\tilde{R}$.

Lemma 4.1. *Let V be a finite dimensional vector space over a finite field k such that*

$$V = V_1 \cup \cdots \cup V_n,$$

where each V_i is a subspace strictly contained in V. Then $n > \#k$.

Proof. As $V_i \subsetneq V$, then it has codimension ≥ 1, which implies that $\#V_i \leq (\#k)^{\dim_k V - 1}$. As $\overline{0} \in V_1 \cap \cdots \cap V_n$, then

$$\#k^{\dim_k V} = \#V = \#(V_1 \cup \cdots \cup V_n) \leq$$
$$\leq \left(\sum_{i=1}^{n} \#V_i \right) - (n-1) < \sum_{i=1}^{n} \#V_i \leq n \#k^{\dim_k V - 1}.$$

Then dividing by $\#k^{\dim_k V - 1}$ we get $n > \#k$. □

Lemma 4.2. *Let R be a local number ring with maximal ideal $\mathfrak{m}$ and residue field k. Let $\tilde{R}$ be its normalization. Let l be number of distinct maximal ideals of the finite ring $\tilde{R}/\mathfrak{m}\tilde{R}$. If $l \leq \#k$ then there exists $x \in I$ such that $I\tilde{R} = x\tilde{R}$.*

Proof. If $I = 0$ then take $x = 0$. So assume that I is non-zero. The maximal ideals of $\tilde{R}/\mathfrak{m}\tilde{R}$ correspond bijectively to the maximal $\tilde{R}$-ideals above $\mathfrak{m}$. Denote them $\mathfrak{m}_1, \cdots, \mathfrak{m}_l$. Consider the R-modules $W = I/\mathfrak{m}I$ and $I\tilde{R}/\mathfrak{m}_i I\tilde{R}$. As $\mathfrak{m} \subseteq \mathfrak{m}_i$ for every i, they are annihilated by $\mathfrak{m}$ and hence they are k-vector spaces. For every i, consider the map

$$\varphi_i : W \longrightarrow \frac{I\tilde{R}}{\mathfrak{m}_i I\tilde{R}}$$

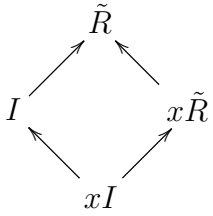
that sends $\overline{x} \in W$ to the vector $\overline{x} \in I\tilde{R}/\mathfrak{m}_i I\tilde{R}$ and let W_i be the kernel of φ_i, which is a subspace of W. The set I is a set of generators as $\tilde{R}$-module for $I\tilde{R}$, hence for $I\tilde{R}/\mathfrak{m}_i I\tilde{R}$, then φ_i is not the zero map, i.e. for every i, W_i is not the whole W. By lemma 4.1 we get that $W_1 \cup \cdots \cup W_l \subsetneq W$ and so there exists $x \in I$ whose projection in W is not in W_i, for every i. Observe that this condition means that $\mathrm{ord}_{\mathfrak{m}_i}(x) \leq \mathrm{ord}_{\mathfrak{m}_i}(I\tilde{R})$ for every i. Moreover $x \in I \subset I\tilde{R}$, so $\mathrm{ord}_{\mathfrak{m}_i}(x) \geq \mathrm{ord}_{\mathfrak{m}_i}(I\tilde{R})$ for every i. Then we have that $\mathrm{ord}_{\mathfrak{m}_i}(x) = \mathrm{ord}_{\mathfrak{m}_i}(I\tilde{R})$ for every i, which is equivalent by 1.15 to have $x\tilde{R} = I\tilde{R}$.

□

Lemma 4.3. *Let R be a local number ring with maximal ideal $\mathfrak{m}$ and residue field k. Let $\tilde{R}$ be its normalization. Let l be number of distinct maximal ideals of the finite ring $\tilde{R}/\mathfrak{m}\tilde{R}$. If $l \leq \#k$ then for every R-ideal I we have that*

$$\dim_k \frac{I}{\mathfrak{m}I} \leq \dim_k \frac{\tilde{R}}{\mathfrak{m}\tilde{R}}.$$

Proof. The maximal ideals of $\tilde{R}/\mathfrak{m}\tilde{R}$ correspond bijectively to the maximal $\tilde{R}$-ideals above $\mathfrak{m}$. Denote them $\mathfrak{m}_1, \cdots, \mathfrak{m}_l$. Observe that by lemma 4.2 we know that $\mathfrak{m}\tilde{R} = x\tilde{R}$ for some $x \in \mathfrak{m}$. Multiplication by x induces a R-module isomorphism $\tilde{R} \simeq x\tilde{R}$ and so we get also an isomorphism on the quotient $\tilde{R}/I \simeq (x\tilde{R})/(xI)$. As the following diagram of inclusions is commutative



we have also $\#(I/xI) = \#(\tilde{R}/x\tilde{R})$. Then

$$[\tilde{R} : \mathfrak{m}\tilde{R}] = [\tilde{R} : x\tilde{R}] = [I : xI] = [I : \mathfrak{m}I][\mathfrak{m}I : xI].$$

So we get that $\#(I/\mathfrak{m}I)$ divides $\#(\tilde{R}/\mathfrak{m}\tilde{R})$, and as $I/\mathfrak{m}I$ and $\tilde{R}/\mathfrak{m}\tilde{R}$ are both k-vector spaces we get our statement on their k-dimensions. □

Now we would like to be able to drop the hypothesis on the residue field. The construction described in the next theorem lets us enlarge the residue field without losing information on the number of generators of any ideal.

Theorem 4.4. *Let R be a local number ring with maximal ideal $\mathfrak{m}$, residue field k and normalization $\tilde{R}$. Then for every R-ideal I we have that*

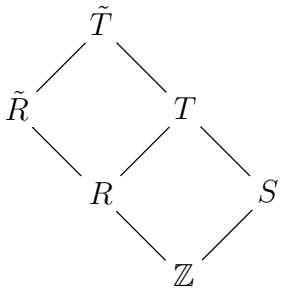
$$\dim_k \frac{I}{\mathfrak{m}I} \leq \dim_k \frac{\tilde{R}}{\mathfrak{m}\tilde{R}}.$$

Proof. We want to be able to apply the lemma 4.2. Let $\mathfrak{m}_1, \cdots, \mathfrak{m}_l$ be the maximal ideals of $\tilde{R}$, which are above $\mathfrak{m}$. Choose $\overline{f}(x)$ a monic irreducible polynomial in $\mathbb{F}_p[X]$ of degree d coprime with $[(\tilde{R}/\mathfrak{m}_i) : \mathbb{F}_p]$ for every $i = 1, \cdots, l$ and such that $(\#k)^d \geq l$. Observe that such d is also coprime with $[k : \mathbb{F}_p]$ because each $\tilde{R}/\mathfrak{m}_i$ is an extension of k. Let $f(X)$ be a monic lift in $\mathbb{Z}[X]$, which is also irreducible and of the same degree. Let α be a zero of $f(X)$ and consider $\mathbb{Q}(\alpha)$. It is a number field of degree d over $\mathbb{Q}$ and let S

be the order $\mathbb{Z}[X]/(f)$. We know that as $\overline{f}(X)$ is irreducible modulo p, then by theorem 1.18, the prime ideal p is inert, i.e. pS is a prime ideal of S, and the quotient S/pS is isomorphic to $\mathbb{F}_{p^d}$. Now let's define $T = R \otimes_{\mathbb{Z}} S$ and observe that

$$T \simeq \frac{R[X]}{(f)}$$

by propositions 1.19 and 1.20. Now let $\tilde{T}$ be its normalization. In other words we are in the following situation:



Now I claim that T is a local domain, with unique maximal ideal $\mathfrak{m} \otimes_{\mathbb{Z}} S = \mathfrak{M}$.

First of all observe that $k \otimes_{\mathbb{F}_p} (S/pS)$ is a field: it is clearly a ring, so consider the projection

$$k \otimes_{\mathbb{F}_p} (S/pS) \twoheadrightarrow \frac{k \otimes_{\mathbb{F}_p} (S/pS)}{\mathfrak{R}},$$

where $\mathfrak{R}$ is a maximal ideal. The image F is a field extension of $\mathbb{F}_p$. As both k and S/pS can be embedded in F then the degree $[F : \mathbb{F}_p]$ is divisible by $[k : \mathbb{F}_p]d$, which is exactly the dimension of $k \otimes_{\mathbb{F}_p} (S/pS)$ as $\mathbb{F}_p$-vector space. So the projection is also injective, $\mathfrak{R}$ is the zero ideal and $k \otimes_{\mathbb{F}_p} (S/pS)$ is a field.

Now observe that $T/\mathfrak{M}$ is a $\mathbb{F}_p$-vector space, because it is a $\mathbb{Z}$-module annihilated by $p\mathbb{Z}$. Observe that

$$k \otimes_{\mathbb{F}_p} \frac{S}{pS} \simeq \frac{R \otimes_{\mathbb{Z}} S}{(\mathfrak{m} \otimes_{\mathbb{Z}} S) + (R \otimes_{\mathbb{Z}} pS)} \simeq \frac{T}{\mathfrak{M}}.$$

So $T/\mathfrak{M}$ is a field and $\mathfrak{M}$ is a maximal ideal. I claim that $\mathfrak{M}$ is the unique maximal ideal. Let $\mathfrak{N}$ be any maximal ideal of T and recall that we have that $T \simeq R[X]/(f)$. So T is a finitely generated R-module and hence T is integral over R. Then by 1.22 $\mathfrak{N} \cap R$ must be the maximal ideal $\mathfrak{m}$. So $\mathfrak{N}$ contains the T-ideal generated by $\mathfrak{m}$, which is $\mathfrak{M}$, and by maximality they are equal. So T is local.

Now observe that also $\tilde{R}/\mathfrak{m}_i$ and S/pS have coprime degree over $\mathbb{F}_p$ and that $\tilde{R} \otimes_{\mathbb{Z}} S = \tilde{R}[X]/(f)$ is integral over $\tilde{R}$. So by the same argument as before we can deduce that there exists an isomorphism of fields

$$\frac{\tilde{R}}{\mathfrak{m}_i} \otimes_{\mathbb{F}_p} \frac{S}{pS} \simeq \frac{\tilde{R} \otimes_{\mathbb{Z}} S}{\mathfrak{m}_i \otimes_{\mathbb{Z}} S},$$

and that the maximal ideals of $\tilde{R} \otimes_{\mathbb{Z}} S$ are exactly the $\mathfrak{m}_i \otimes_{\mathbb{Z}} S = \mathfrak{M}_i$, with $i = 1, \cdots, l$.

The ring $\tilde{R}$ is integrally closed, so because of 1.12 and 1.14 we have that $\mathfrak{m}_i$ is invertible in a semilocal ring. So by 1.17 it is a principal ideal. Then also $\mathfrak{M}_i$ is principal, hence invertible, and we have that $\tilde{R} \otimes_{\mathbb{Z}} S$ is integrally closed, hence it is equal to $\tilde{T}$.
Observe that $T/\mathfrak{M}$ has $(\#k)^d$ elements, which is bigger than l. Then we can apply lemma 4.3 and we get that

$$\dim_{(T/\mathfrak{M})} \frac{I \otimes_{\mathbb{Z}} S}{\mathfrak{M}(I \otimes_{\mathbb{Z}} S)} \leq \dim_{(T/\mathfrak{M})} \frac{\tilde{T}}{\mathfrak{M}\tilde{T}}.$$

Now observe that $I \otimes_{\mathbb{Z}} S = I \otimes_R T$ and using the canonical isomorphisms of the tensor product we get

$$\frac{I \otimes_R T}{\mathfrak{M}(I \otimes_R T)} \simeq (I \otimes_R T) \otimes_T \frac{T}{\mathfrak{M}} \simeq I \otimes_R \frac{T}{\mathfrak{M}} \simeq I \otimes_R k \otimes_k \frac{T}{\mathfrak{M}} \simeq \frac{I}{\mathfrak{m}I} \otimes_k \frac{T}{\mathfrak{M}}.$$

So

$$\dim_{(T/\mathfrak{M})} \frac{I \otimes_{\mathbb{Z}} S}{\mathfrak{M}(I \otimes_{\mathbb{Z}} S)} = \dim_{(T/\mathfrak{M})} \left(\frac{I}{\mathfrak{m}I} \otimes_k \frac{T}{\mathfrak{M}} \right) = \dim_k \frac{I}{\mathfrak{m}I}.$$

Similarly we have that

$$\frac{\tilde{T}}{\mathfrak{M}\tilde{T}} \simeq \tilde{T} \otimes_T \frac{T}{\mathfrak{M}} \simeq (\tilde{R} \otimes_R T) \otimes_T \frac{T}{\mathfrak{M}} \simeq \tilde{R} \otimes_R \frac{T}{\mathfrak{M}} \simeq \tilde{R} \otimes_R k \otimes_k \frac{T}{\mathfrak{M}} \simeq \frac{\tilde{R}}{\mathfrak{m}\tilde{R}} \otimes_k \frac{T}{\mathfrak{M}}.$$

So also

$$\dim_{(T/\mathfrak{M})} \frac{\tilde{T}}{\mathfrak{M}\tilde{T}} = \dim_k \frac{\tilde{R}}{\mathfrak{m}\tilde{R}}.$$

Then we can conclude that

$$\dim_k \frac{I}{\mathfrak{m}I} \leq \dim_k \frac{\tilde{R}}{\mathfrak{m}\tilde{R}}$$

□

Corollary 4.5. *Let R be a local number ring with maximal ideal $\mathfrak{m}$, residue field k and normalization $\tilde{R}$. Then $g(R) = \dim_k(\tilde{R}/\mathfrak{m}\tilde{R})$.*

Proof. Let $r = \dim_k(\tilde{R}/\mathfrak{m}\tilde{R})$ and let I be any R-ideal. By the previous lemma 4.3 we obtain that $\dim_k(I/\mathfrak{m}I) \leq r$. As every number ring is noetherian, we have that I is finitely generated and hence we can apply Nakayama's lemma 1.2 to get that I is generated by at most r elements. Hence $g(R) \leq r$. Moreover observe that $\tilde{R}$ is a fractional R-ideal and by 1.2 we know that it is generated by exactly r elements, so $g(R) = r$. □

The next lemma and proposition will give us a sufficient condition on the ideal norm which guarantees $\dim_k(\tilde{R}/\mathfrak{m}\tilde{R}) \leq 3$.

Lemma 4.6 (H. Lenstra)**.** *Let k be a field and A a k-algebra with $\dim_k A \geq 4$. Then exactly one of the following holds:*

(i) there exist $x, y \in A$ such that $\dim_k(k1 + kx + ky + kxy) \geq 4$;

(ii) there exists a k-vector space V with $A = k \oplus V$ and $V \cdot V = 0$;

(iii) there exists a k-vector space V with $A \simeq \begin{pmatrix} k & V \\ 0 & k \end{pmatrix}$, that is $A = ke \oplus kf \oplus V$, with $V \cdot V = eV = Vf = 0, e^2 = e, f^2 = f, ef = fe = 0, e + f = 1$.

Proof. Suppose that *(i)* does not hold, which means that for every $x, y \in A$ such that $x \notin k$ and $y \notin k + kx$ we have that $xy \in k1 + kx + ky$. First we claim that for every $x \in A$ we have $x^2 \in k + kx$. Pick $y \notin k + kx$. We have $xy \in k1 + kx + ky$ and $x(y + x) \in k1 + kx + k(y + x) = k1 + kx + ky$; hence $x^2 \in k1+kx+ky$. We can use the same argument for $z \notin k1+kx+ky \supset k+kx$ (which exists because the dimension of A over k is ≥ 4) and we get that $x^2 \in k1 + kx + kz$. So $x^2 \in k1 + kx + ky \cap k1 + kx + kz = k + kx$. From these considerations we get that every subspace $W \subset A$ containing 1 is also a ring (i.e. it is closed under multiplication).
Observe that each $x \in A$ acts by multiplication on the left on $A/(k + kx)$ and each vector is an eigenvector. This means that there is one eigenvalue and hence the action of x is just a multiplication by a scalar. This means that there exists a unique k-linear morphism $\lambda : A \longrightarrow k$, such that $xy \equiv \lambda(x)y \bmod (k + kx)$ for every $y \in A$. We can use the same argument for the action of y on $A/(k + ky)$ and the action of xy on $A/(k + kx + ky)$, which has dimension > 0, by hypothesis. As all the actions are scalar on $A/(k + kx + ky)$ we get that $\lambda(x)\lambda(y) = \lambda(xy)$. As this works for every $x, y \in A$ then $\lambda : A \to k$ is a k-algebra morphism. We can use the same argument for the multiplication on the right, to get that there is a unique ring homomorphism $\mu : A \to k$ such that for every $x, z \in A$ we have $zx \equiv \mu(x)z \bmod (k + kx)$. Then we get that $A = k + \ker\lambda = k + \ker\mu$, which also implies that the dimension over k of the kernels is ≥ 3.

Now we want to prove that $\ker\lambda \cdot \ker\mu = 0$. For $x \in \ker\lambda$ and $y \in \ker\mu$ we have $xA \subset k + kx$ and $Ay \subset k + ky$. Observe that $xy \in xA \cap Ay$. If $k + kx \neq k + ky$ then $xA \cap Ay \subseteq k$ and as both λ and μ are the identity on k then $xy = \lambda(xy) = \lambda(x)\lambda(y) = 0$. If otherwise $k + kx = k + ky$, pick $z \in \ker\mu \setminus (k + kx)$, which is possible because $\dim_k \ker\mu \geq 3$. Then observe that $k + kx \cap k + kz = k$, so $xz \in xA \cap Az \subseteq k$. As μ is the identity on k, we have $xz = \mu(xz) = \mu(x)\mu(z) = 0$. Similarly $x(y + z) \in xA \cap A(y + z) \subset k + kx \cap k + k(y + z) = k + kx \cap k + kz = k$, so also $x(y + z) = \mu(x(y + z)) = \mu(x)(\mu(y) + \mu(z)) = 0$. Hence we get that $xy = 0$. Now we have to distinguish two cases. If $\ker\mu = \ker\lambda$ then, as λ and μ agree on k, they coincide on the whole A. So we are in case *(ii)* with $V = \ker\mu = \ker\lambda$. If $\ker\mu \neq \ker\lambda$, then call $V = \ker\mu \cap \ker\lambda$ which has exactly codimension 2: as the kernels are different it must be strictly bigger than 1 and it is strictly smaller than 3 because $\ker\mu, \ker\lambda$ have codimension 1. So the projections of $1, \ker\lambda, \ker\mu$ are 3 distinct lines in A/V. Hence: $\ker\lambda = k \cdot e + V$ where we choose e with $\mu(e) = 1$ (it can be done as $\ker\lambda$ maps surjectively onto k), $\ker\mu = k \cdot f + V$ where $f = 1 - e$. Observe that $ef = e(1 - e) = (1 - f)f = 0$, because $e \in \ker\lambda$ and $f \in \ker\mu$. Then we obtain $e^2 = e, f^2 = f, fe = 0$. Also $eV = Vf = 0$. From this conditions we get that $A = ke \oplus kf \oplus V$, because $\ker\lambda = ke \oplus V$ has codimension 1 and $f \notin \ker\lambda$. Then

$$A \longrightarrow \begin{bmatrix} k & V \\ 0 & k \end{bmatrix}$$
$$ae + bf + v \longmapsto \begin{pmatrix} b & v \\ 0 & a \end{pmatrix}$$

is a well defined morphism and clearly it is bijective. So we are in case *(iii)*. To conclude, observe that if *(ii)* holds then A is a commutative algebra and in case *(iii)* A is not. If A has *(ii)* then it has not *(i)*, because the subspace $k1 + kx + ky$ is a ring and so $\dim_k(k1 + kx + ky + kxy) \leq 3$. If A has *(iii)* then it cannot have *(i)*, because if $x = \begin{pmatrix} a & u \\ 0 & b \end{pmatrix}$ and $y = \begin{pmatrix} c & v \\ 0 & d \end{pmatrix}$ then we have $(x - a)(y - d) = 0$ and so $xy \in k + kx + ky$. □

Lemma 4.7. *Let R be a local number ring, with maximal ideal $\mathfrak{m}$ and residue field k. Assume that $R' = \mathfrak{m}\tilde{R} + R$ is super-multiplicative, where $\tilde{R}$ is the normalization of R. Then*

$$\dim_k \frac{\tilde{R}}{\mathfrak{m}\tilde{R}} \leq 3.$$

Proof. We define $A = \tilde{R}/\mathfrak{m}\tilde{R}$. Observe that it is an R-module annihilated by the maximal ideal $\mathfrak{m}$, so it is a finite dimensional k-algebra. Assume by

contradiction that $\dim_k A \geq 4$, so we are in one of three cases of lemma 4.6. Observe that as $\tilde{R}$ is commutative, then A is the same, so we cannot be in case *(iii)*. Assume that we are in case *(ii)*, so $A = k \oplus V$, with V a k-vector space such that $V^2 = 0$. Consider the projection $\tilde{R} \twoheadrightarrow A$. Let $\tilde{\mathfrak{m}}$ be the pre-image of V. Observe that $k = A/V \simeq \tilde{R}/\tilde{\mathfrak{m}}$, so $\tilde{\mathfrak{m}}$ is a maximal ideal of $\tilde{R}$. The ring $\tilde{R}$ is integrally closed so by propositions 1.12 and 1.14 we have that $\tilde{\mathfrak{m}}/\tilde{\mathfrak{m}}^2$ is 1-dimensional. So also its image V/V^2 is 1-dimensional and as $V^2 = 0$, then V is 1-dimensional and hence A has dimension 2 over k. Contradiction. So we are in case *(i)*. Then there exist x, y such that $\dim_k(1 + x + y + xy) \geq 4$. Consider the R'-fractional ideals $I = (1, x, \mathfrak{m}\tilde{R})$ and $J = (1, y, \mathfrak{m}\tilde{R})$. Observe that $\tilde{R}/R' \simeq A/k$ and inside it we have I/R' and J/R' which are generated by the images of x and y, respectively, so they are 1-dimensional. The image of the product IJ/R' is generated by the projections of x, y and xy. So it has dimension 3. So we have that the length as R'-module are

$$l\left(\frac{R'}{IJ}\right) = -3, \qquad l\left(\frac{R'}{I}\right) + l\left(\frac{R'}{J}\right) = -2.$$

But this contradicts the fact that R' is super-multiplicative. So we have that $\dim_k A \leq 3$.

□

Now to conclude the second implication of the main theorem stated in the introduction, we need to return to the non-local case.

Corollary 4.8. *Let R be a number ring. Assume that for every maximal R-ideal $\mathfrak{m}$, the number ring $R' = \mathfrak{m}\tilde{R} + R$ is super-multiplicative. Then $g(R) \leq 3$.*

Proof. Observe that by lemma 1.10 we have $R'_{\mathfrak{m}}$ is super-multiplicative for every maximal ideal. Then by lemma 4.7 the hypothesis of lemma 4.5 are all satisfied and we get that every $R_{\mathfrak{m}}$-ideal is generated by 3 elements, for every $\mathfrak{m}$. Then by 3.5 we have that every R-ideal is generated by 3 elements. □

To conclude consider what we proved: let R be a number ring, $R \subset R' \subset \tilde{R}$, then

$$\begin{array}{ccc} g(R) \leq 3 & \Longrightarrow & g(R') \leq 3 \\ \Downarrow & \swarrow & \Downarrow \\ R \text{ super-mult.} & & R' \text{ super-mult.} \end{array}$$

So to conclude that the properties are all equivalent we need the last implication, i.e. if R is super-multiplicative then every R' is super-multiplicative. But unfortunately we don't know if it holds or if there is a counterexample.

References

[PSHNR12] Stevenhagen, Peter (September 24,2012), *Number Rings*, Universiteit Leiden, `http://websites.math.leidenuniv.nl/algebra/ant.pdf`

[AM69] Atiyah, M.F. and Macdonald I.G. (1969), *Introduction to Commutative Algebra*, Addison-Wesley.

[EIS95] Eisenbud, D. (1995), *Commutative Algebra with a view towards algebraic geometry*, Springer-Verlag.

[MATS95] Matsumura H. (1989), *Commutative ring theory*, Cambridge University Press.

[NEU95] Neukirch J. (1999), *Algebraic Number Theory*, Springer.