

GALOIS THEORY AND INTEGRAL MODELS OF Λ -RINGS

JAMES BORGER, BART DE SMIT

ABSTRACT. We show that any Λ -ring, in the sense of Riemann–Roch theory, which is finite étale over the rational numbers and has an integral model as a Λ -ring is contained in a product of cyclotomic fields. In fact, we show that the category of them is described in a Galois-theoretic way in terms of the monoid of pro-finite integers under multiplication and the cyclotomic character. We also study the maximality of these integral models and give a more precise, integral version of the result above. These results reveal an interesting relation between Λ -rings and class field theory.

INTRODUCTION

According to the most common definition, a Λ -ring structure on a commutative ring R is a sequence of set maps $\lambda_1, \lambda_2, \dots$ from R to itself that satisfy certain complex implicitly stated axioms. This notion was introduced by Grothendieck [4], under the name special λ -ring, to give an abstract setting for studying the structure on Grothendieck groups inherited from exterior power operations; and as far as we are aware, with just one exception [2], Λ -rings have been studied in the literature for this purpose only.

However, it seems that the study of abstract Λ -rings—those having no apparent relation to K -theory—will have something to say about number theory. One example of such a relationship is the likely existence of strong arithmetic restrictions on the complexity of finitely generated rings that admit a Λ -ring structure. The primary purpose of this paper is to investigate this issue in the zero-dimensional case. Precisely, what finite étale Λ -rings over \mathbf{Q} are of the form $\mathbf{Q} \otimes A$, where A is a Λ -ring that is finite flat over \mathbf{Z} ?

We will consider Λ -actions only on rings whose underlying abelian group is torsion-free, and giving a Λ -action on such a ring R is the same as giving commuting ring endomorphisms $\psi_p: R \rightarrow R$, one for each prime p , lifting the Frobenius map modulo p —that is, such that $\psi_p(x) - x^p \in pR$ for all $x \in R$. (The equivalence of this with Grothendieck’s original definition is proved in Wilkerson [7].) An example that will be important here is $\mathbf{Z}[\mu_r] = \mathbf{Z}[z]/(z^r - 1)$, where r is a positive integer and ψ_p sends z to z^p . A morphism of torsion-free Λ -rings is the same as a ring map f that satisfies $f \circ \psi_p = \psi_p \circ f$ for all primes p .

Note that if R is a \mathbf{Q} -algebra, the congruence conditions in the definition above disappear. Also, Galois theory as interpreted by Grothendieck gives an anti-equivalence between the category of finite étale \mathbf{Q} -algebras and the category of finite discrete sets equipped with a continuous action of the absolute Galois group $G_{\mathbf{Q}}$ with respect to a fixed algebraic closure $\bar{\mathbf{Q}}$. Combining these two remarks, we see that the category of Λ -rings that are finite étale over \mathbf{Q} is nothing more than

the category of finite discrete sets equipped with a continuous action of the monoid $G_{\mathbf{Q}} \times \mathbf{N}'$, where \mathbf{N}' is the monoid $\{1, 2, \dots\}$ under multiplication with the discrete topology. This is because \mathbf{N}' is freely generated as a commutative monoid by the prime numbers.

It is not always true, however, that such a Λ -ring K has an integral Λ -model, by which we mean a sub- Λ -ring A , finite over \mathbf{Z} , such that $\mathbf{Q} \otimes A = K$. In order to formulate exactly when this happens, we write $\hat{\mathbf{Z}}^\circ$ for set of profinite integers viewed as a topological monoid under multiplication, and we consider the continuous monoid map

$$G_{\mathbf{Q}} \times \mathbf{N}' \longrightarrow \hat{\mathbf{Z}}^\circ$$

given by the cyclotomic character $G_{\mathbf{Q}} \rightarrow \hat{\mathbf{Z}}^* \subset \hat{\mathbf{Z}}^\circ$ on the first factor and the natural inclusion on the second. Note that this map has a dense image. Now let K be a finite étale algebra over \mathbf{Q} , and let S be the set of ring maps from K to $\bar{\mathbf{Q}}$. Suppose K is endowed with a Λ -ring structure, so that we have an induced monoid map

$$G_{\mathbf{Q}} \times \mathbf{N}' \longrightarrow \text{Map}(S, S),$$

where $\text{Map}(S, S)$ is the monoid of set maps from S to itself. With the discrete topology on $\text{Map}(S, S)$ this map is continuous.

0.1. Theorem. *The Λ -ring K has an integral Λ -model if and only if the action of $G_{\mathbf{Q}} \times \mathbf{N}'$ on S factors (necessarily uniquely) through $\hat{\mathbf{Z}}^\circ$; in more precise terms, if and only if there is a continuous monoid map $\hat{\mathbf{Z}}^\circ \rightarrow \text{Map}(S, S)$ so that the diagram*

$$\begin{array}{ccc} G_{\mathbf{Q}} \times \mathbf{N}' & \longrightarrow & \hat{\mathbf{Z}}^\circ \\ & \searrow & \downarrow \\ & & \text{Map}(S, S) \end{array}$$

commutes.

It follows that the category of such Λ -rings is anti-equivalent to the category of finite discrete sets with a continuous action of $\hat{\mathbf{Z}}^\circ$ and that every such Λ -ring is contained in a product of cyclotomic fields. It also suggests there is an interesting theory of a Λ -algebraic fundamental monoid, analogous to that of the usual algebraic fundamental group, but we will leave this for a later date.

Another consequence is that the elements $-1, 0 \in \hat{\mathbf{Z}}^\circ$ give an involution ψ_{-1} (complex conjugation) and a idempotent endomorphism ψ_0 on any K with an integral Λ -model. In K -theory, the dual and rank also give such operators, but here they come automatically from the Λ -ring structure. Also observe that any element of the subset $0S \subseteq S$ is Galois invariant and hence corresponds to a direct factor \mathbf{Q} of the algebra K . Therefore K cannot be a field unless $K = \mathbf{Q}$.

In the first section, we give some basic facts and also show the sufficiency of the condition in the theorem above. In the second section, we show the necessity. The proof combines a simple application of the Kronecker–Weber theorem and the Chebotarev density theorem with some elementary but slightly intricate work on actions of the monoid $\hat{\mathbf{Z}}^\circ$.

The third section gives a proof of the following theorem:

0.2. Theorem. *The Λ -ring $\mathbf{Z}[\mu_r]$ is the maximal integral Λ -model of $\mathbf{Q} \otimes \mathbf{Z}[\mu_r]$.*

Of course, the non- Λ version of this statement is false—the usual maximal order of $\mathbf{Q} \otimes \mathbf{Z}[\mu_r]$ is a product of rings of integers in cyclotomic fields and strictly contains $\mathbf{Z}[\mu_r]$, if $r > 1$.

A direct consequence of these theorems is:

0.3. Corollary. *Every Λ -ring that has finite rank as an abelian group and has no non-zero nilpotent elements is a sub- Λ -ring of a Λ -ring of the form $\mathbf{Z}[\mu_r]^n$.*

We do not need to require that the ring be torsion-free because any torsion element in a Λ -ring is nilpotent, as explained to us by F. Clauwens. For completeness' sake, we have included his argument in 3.6. Of course, it uses the definition of Λ -ring that is correct even in the presence of non-zero torsion, rather than the naive extension of the definition above.

Finally, many of the questions answered in this paper have analogues over general number fields. There one would use Frobenius lifts modulo prime ideals of the ring of integers, and then general class field theory and the class group come in, as well as the theory of complex multiplication in particular cases. Because these analogues of Λ -rings are not objects of prior interest, we have not included anything about them here. But it is clear that finite-rank Λ -rings, in this generalized sense or the original, are fundamentally objects of class field theory and that they offer a slightly different perspective on the subject. It would be interesting to explore this further.

1. BASICS

The category of Λ -rings has all limits and colimits, and they agree, as rings, with those taken in the category of rings. (E.g. [1]) We will only need to take tensor products, intersections, and images of morphisms, and it is quite easy to show their existence on the subcategory of torsion-free Λ -rings using the equivalent definition given in the introduction. For any ring R , let $R[\mu_r]$ denote $R[z]/(z^r - 1)$. Because $R[\mu_r] = R \otimes \mathbf{Z}[z]/(z^r - 1)$, the ring $R[\mu_r]$ is naturally a Λ -ring if R is.

Given a Λ -ring R , it will be convenient to call a Λ -ring K equipped with a map $R \rightarrow K$ of Λ -rings an $R\Lambda$ -ring. (Compare [1, 1.13].) When we say K is flat, or étale, or so on, we mean as R -algebras in the usual sense. We call a sub- Λ -ring of a $\mathbf{Q}\Lambda$ -ring a Λ -order if it is finite over \mathbf{Z} . We do not require that it have full rank.

1.1. Proposition. *Let K be a finite étale $\mathbf{Q}\Lambda$ -ring. Then K has a Λ -order that contains all others.*

We call this Λ -order the maximal Λ -order of K .

Proof. Because any Λ -order A is contained in the usual maximal order of K , which is finite over \mathbf{Z} , it is enough to show that any two such subrings A and B are contained in a third. But $A \otimes B$ is a Λ -ring that is finite over \mathbf{Z} , and therefore its image in the Λ -ring K is a Λ -ring that is finite over \mathbf{Z} . \square

1.2. Proposition. *Let $K \subseteq L$ be an inclusion of finite étale $\mathbf{Q}\Lambda$ -rings. Let $A \subseteq K$ and $B \subseteq L$ be their maximal Λ -orders. Then $A = K \cap B$.*

Proof. The intersection $K \cap B$ is on the one hand a sub- Λ -ring of K and, on the other, finite over \mathbf{Z} . It is maximal among such rings because of the maximality of B . \square

We can now prove the sufficiency of the conditions of theorem 0.1.

1.3. Proposition. *Let r be a positive integer, let S be a finite $\mathbf{Z}/r\mathbf{Z}^\circ$ -set, and let K be the corresponding finite étale $\mathbf{Q}\Lambda$ -ring. Then K has an integral Λ -model.*

Proof. Take a set T (such as S) admitting a surjection $\coprod_T \mathbf{Z}/r\mathbf{Z}^\circ \rightarrow S$ of $\mathbf{Z}/r\mathbf{Z}^\circ$ -sets, the left side denoting the free $\mathbf{Z}/r\mathbf{Z}^\circ$ -set generated by T . Let L be the corresponding finite étale $\mathbf{Q}\Lambda$ -ring. Then K is naturally a sub- Λ -ring of L . On the other hand L is $\mathbf{Q}[\mu_r]^T$ and so has a Λ -model $\mathbf{Z}[\mu_r]^T$. The intersection of this with K is then both a Λ -ring and an order of full rank in K . \square

2. NECESSARY CONDITIONS

Let K be a finite étale $\mathbf{Q}\Lambda$ -ring admitting an integral Λ -model A , and let $S = \text{Hom}(K, \mathbf{Q})$ be the corresponding $G_{\mathbf{Q}} \times \mathbf{N}'$ -set.

The purpose of this section is to show that there is an integer $r > 0$ such that this action factors through the map $G_{\mathbf{Q}} \times \mathbf{N}' \rightarrow \mathbf{Z}/r\mathbf{Z}^\circ$, where $\mathbf{Z}/r\mathbf{Z}^\circ$ denotes the monoid of integers modulo r under multiplication, given by the cyclotomic character on the first factor and reduction modulo r on the second.

As usual, we say a prime number p is unramified in A if A/pA has no non-zero nilpotent elements. A prime is ramified in A if and only if it divides the discriminant of A . Therefore the set of primes that ramify in A is finite and contains the set of primes that ramify in the usual maximal order of K .

2.1. Proposition. *The endomorphism ψ_p of A is an automorphism if and only if p is unramified in A . In this case, ψ_p is the unique lift of the Frobenius endomorphism of A/pA .*

Proof. If ψ_p is an automorphism, then the Frobenius endomorphism $x \mapsto x^p$ of A/pA is an automorphism, and so p is unramified.

Suppose instead that p is unramified. Then A/pA is a finite product of finite fields, and so the Frobenius endomorphism of A/pA is an automorphism of finite order. The category of finite étale \mathbf{Z}_p -algebras is equivalent to the category of finite étale \mathbf{F}_p -algebras, by way of the functor $\mathbf{F}_p \otimes_{\mathbf{Z}_p} -$. (See [3, IV (18.3.3)], say). Thus the endomorphism $1 \otimes \psi_p$ of $\mathbf{Z}_p \otimes A$ is the unique Frobenius lift and it is an automorphism of finite order. It follows that $\psi_p: A \rightarrow A$ is the unique Frobenius lift to A , and is also an automorphism. \square

2.2. Proposition. *There is a positive integer c , divisible only by primes that ramify in A , such that the action of $G_{\mathbf{Q}}$ on S factors through the cyclotomic character $G_{\mathbf{Q}} \rightarrow \mathbf{Z}/c\mathbf{Z}^*$. If p is unramified in A , then $p \in \mathbf{N}'$ and $(p \bmod c) \in \mathbf{Z}/c\mathbf{Z}^*$ act in the same way on S .*

Proof. Define the number field N to be the invariant field of the kernel of the map $G_{\mathbf{Q}} \rightarrow \text{Map}(S, S)$. Write $\bar{G} = \text{Gal}(N/\mathbf{Q})$ and let \mathcal{O}_N be the ring of integers of N .

Take any element $g \in \bar{G}$. By Chebotarev's theorem [6, V.6] there is an unramified prime \mathfrak{p} of N lying over a prime number p such that $g(x) \equiv x^p \pmod{\mathfrak{p}}$ for all $x \in \mathcal{O}_N$, i.e., g is the Frobenius element of \mathfrak{p} in the extension $\mathbf{Q} \subset N$. Since Chebotarev's theorem provides infinitely many such \mathfrak{p} , we may also assume that A is unramified at p .

We now claim that for all $s \in S = \text{Hom}(A, \mathcal{O}_N)$ the maps $s \circ \psi_p$ and $g \circ s$ from A to \mathcal{O}_N are equal. Since A is unramified at p , the map $\text{Hom}(A, \mathcal{O}_N) \rightarrow \text{Hom}(A, \mathcal{O}_N/\mathfrak{p})$ is injective, so it suffices to show that their compositions with the map $\mathcal{O}_N \rightarrow \mathcal{O}_N/\mathfrak{p}$

are equal. But this follows from 2.1 and our choice of \mathfrak{p} . Thus, $g \in \bar{G}$ and $p \in \mathbf{N}'$ act in the same way on S .

It follows that the image of $G_{\mathbf{Q}}$ in $\text{Map}(S, S)$ is contained in the image of \mathbf{N}' , so \bar{G} is abelian. By the Kronecker-Weber theorem [6, III.3.8], N is contained in a cyclotomic field $\mathbf{Q}(\mu_c)$, where c is divisible only by primes that ramify in N . Since N is the common Galois closure of the components of $A \otimes \mathbf{Q}$, such primes are ramified in A as well. The last statement follows from the fact that for any prime number $p \nmid c$ the element $(p \bmod c) \in \mathbf{Z}/c\mathbf{Z}^*$ corresponds to the Frobenius element of any prime over p in the extension $\mathbf{Q} \subset \mathbf{Q}(\mu_c)$. \square

It follows that our map of topological monoids $G_{\mathbf{Q}} \times \mathbf{N}' \rightarrow \text{Map}(S, S)$ factors through $\hat{\mathbf{Z}}^* \times \mathbf{N}'$. We will show that it factors further through $\hat{\mathbf{Z}}^\circ$ with the following criterion.

2.3. Proposition. *A continuous action of $\hat{\mathbf{Z}}^* \times \mathbf{N}'$ on a finite discrete set T factors through a continuous action of $\hat{\mathbf{Z}}^\circ$ if and only if*

- (i) *all but finitely many primes $p \in \mathbf{N}'$ act as automorphisms on T , and*
- (ii) *for all $d \in \mathbf{N}'$ there exists an integer c_d such that the action of $\hat{\mathbf{Z}}^*$ on dT factors through $\mathbf{Z}/c_d\mathbf{Z}^*$ and for each $n \in \mathbf{N}'$ with $ndT = dT$ we have*
 - *n is relatively prime to c_d , and*
 - *the elements $(n \bmod c_d) \in \mathbf{Z}/c_d\mathbf{Z}^*$ and $n \in \mathbf{N}'$ act on dT in the same way.*

Proof. To show the necessity of (i) and (ii), assume that the action of $\hat{\mathbf{Z}}^* \times \mathbf{N}'$ factors through $\mathbf{Z}/r\mathbf{Z}^\circ$ for some integer $r > 0$. Then all primes not dividing r , when viewed as elements of \mathbf{N}' , act as automorphisms on T . This establishes (i).

To show (ii), take any $d \in \mathbf{N}'$ and let c_d be the smallest positive integer c for which the $\hat{\mathbf{Z}}^*$ -action on dT factors through $\mathbf{Z}/c\mathbf{Z}^*$. Note that c_d divides all c with this property. Now suppose that p is a prime with $pdT = dT$. Write $r = p^n e$, with $p \nmid e$. Then for any $x, y \in \mathbf{Z}/r\mathbf{Z}^\circ$ with $x \equiv y \pmod{e}$ and $s \in T$, we have

$$p^n(xs) = (p^n x)s = (p^n y)s = p^n(ys).$$

Since p acts as a bijection on dT this implies that x and y act in the same way on dT , so the action of $\hat{\mathbf{Z}}^\circ$ on dT factors through $\mathbf{Z}/e\mathbf{Z}^\circ$. In particular, $c_d \mid e$, so $p \nmid c_d$, and the elements $p \in \mathbf{N}'$ and $(p \bmod e) \in \mathbf{Z}/e\mathbf{Z}^*$ and $(p \bmod c_d) \in \mathbf{Z}/c_d\mathbf{Z}^*$ all act in the same way on dT . Since \mathbf{N}' is generated by the primes, part (ii) follows.

For the converse, suppose (i) and (ii) hold. For every prime number p , let a_p be the smallest integer $a \geq 0$ such that $p^a T = p^{a+1} T$. By (i) we have $a_p = 0$ for all but finitely many p , so $r_0 = \prod_p p^{a_p}$ is an integer. Note that for any $n \in \mathbf{N}'$ we have $nT = \text{gcd}(n, r_0)T$.

Now let r be any integer divisible by dc_d for every $d \mid r_0$. We will show that the action of $\hat{\mathbf{Z}}^* \times \mathbf{N}'$ on T factors through $\mathbf{Z}/r\mathbf{Z}^\circ$. To do this, we will show directly that any two elements $(a_1, d_1), (a_2, d_2) \in \hat{\mathbf{Z}}^* \times \mathbf{N}'$ satisfying $a_1 d_1 \equiv a_2 d_2 \pmod{r}$ act in the same way on T .

Since $r_0 \mid r$ the congruence implies that d_1 and d_2 have the same greatest common divisor d with r_0 , so we have $d_1 T = dT = d_2 T$. For $i = 1, 2$ we define $d'_i \in \mathbf{N}'$ by $d_i = dd'_i$ and deduce that $d'_i(dT) = dT$. Using (ii) one sees that d'_i is coprime to c_d , and that the action of d'_i on dT is that of $(d'_i \bmod c_d) \in \mathbf{Z}/c_d\mathbf{Z}^*$. By the defining property of r we have $dc_d \mid r$, so $a_1 d'_1 d \equiv a_2 d'_2 d \pmod{dc_d}$, which implies $a_1 d'_1 \equiv a_2 d'_2 \pmod{c_d}$. It follows that (a_1, d'_1) and (a_2, d'_2) are mapped to the same

element of $\mathbf{Z}/c_d\mathbf{Z}^\circ$, which in fact lies in $\mathbf{Z}/c_d\mathbf{Z}^*$. Thus, (a_1, d'_1) and (a_2, d'_2) act identically on dT , and composing with $(1, d)$ we see that (a_1, d_1) and (a_2, d_2) act in the same way on T . \square

In order to finish the proof of theorem 0.1 one checks the conditions of 2.3 for $T = S$. Condition (i) follows from 2.1 and the fact that A is ramified at only finitely many primes. For condition (ii), suppose $d \in \mathbf{N}'$ is given and consider the sub- Λ -ring $\psi_d(A)$ of A which corresponds to the $G_{\mathbf{Q}} \times \mathbf{N}'$ -set dS of S . Proposition 2.2 applied to $\psi_d(A)$ now provides an integer c_d so that the $G_{\mathbf{Q}}$ -action on dS factors through $\mathbf{Z}/c_d\mathbf{Z}^*$. Any $n \in \mathbf{N}'$ with $ndS = dS$ is a product of primes that are unramified in $\psi_d(A)$ by 2.1, and so 2.2 tells us that $(n \bmod c_d) \in \mathbf{Z}/c_d\mathbf{Z}^*$ and that this element acts on dS in the same way as n . This gives condition (ii).

3. EXPLICIT MAXIMAL Λ -ORDERS

Given a prime number p , there is a notion of Λ_p -action on a ring R , and as before, this has a simple description if R has no p -torsion: a ring endomorphism ψ_p of R that lifts the Frobenius endomorphism, that is, such that $\psi_p(x) - x^p \in pR$ for all $x \in R$. Also as before, a sub- Λ_p -ring A of a $\mathbf{Q}_p\Lambda_p$ -ring K is called a Λ_p -order if it is finite over \mathbf{Z}_p . It is said to be maximal if it contains every other Λ_p -order in K .

We have two natural ways of making Λ_p -orders. First, for any abelian group V the group ring $\mathbf{Z}_p[V]$ is a Λ_p -ring when we set $\psi_p(r) = r$ for $r \in \mathbf{Z}_p$ and $\psi_p(v) = v^p$ for $v \in V$. Secondly, if A is the ring of integers of a finite unramified extension K of \mathbf{Q}_p , then A has a unique Λ_p -ring structure, where ψ_p is the Frobenius map (cf. 2.1). By extending ψ_p to K we see that A is the maximal Λ_p -order of K . Taking tensor products of these two building blocks we see that for any integer q the ring $A[\mu_q] = A[z]/(z^q - 1)$ is a Λ_p -order in $K[\mu_q]$.

3.1. Lemma. *If q is a power of p , then $A[\mu_q]$ is the maximal Λ_p -order of $K[\mu_q]$.*

Proof. By induction, it is enough to assume $A[\mu_q]$ is maximal and then prove $A[\mu_{pq}]$ is.

Let k denote the residue field of A , and let ζ denote a primitive pq -th root of unity in some extension of K . Then we have $K[z]/(z^{pq} - 1) = K(\zeta) \times K[y]/(y^q - 1)$, the element z corresponding to (ζ, y) . In these terms, the Λ_p -action is given by $\psi_p(b, f(y)) = (f^*(\zeta^p), f^*(y^p))$, where $f^*(y)$ denotes polynomial obtained by applying the Frobenius map ψ_p coefficient-wise to $f(y)$.

Now consider the following diagram of rings:

$$\begin{array}{ccc} A[z]/(z^{pq} - 1) & \xrightarrow{z \mapsto y} & A[y]/(y^q - 1) \\ \downarrow z \mapsto \zeta & & \downarrow y \mapsto y \\ A[\zeta] & \xrightarrow{\zeta \mapsto y} & k[y]/(y^q - 1), \end{array}$$

where $A[\zeta]$ denotes the ring of integers in $K(\zeta)$. As noted for example in Kervaire–Murthy [5], this is a pull-back diagram. This is just an instance of the easy fact that for ideals I and J in any ring R , we have

$$R/(I \cap J) = R/I \times_{R/(I+J)} R/J.$$

In our case, take $R = A[z]$, $I = (z^q - 1)$, and $J = (1 + z^q + \dots + z^{q(p-1)})$.

Now suppose R is a Λ_p -order in $K[\mu_{pq}]$. Then the image of R in $K[y]/(y^q - 1)$ is contained, by induction, in $A[y]/(y^q - 1)$. Therefore R is contained in $A[\zeta] \times A[y]/(y^q - 1)$; we will view elements of R as elements of this product without further comment. Because the diagram above is a pull-back diagram, we need only show that the two maps $R \rightrightarrows k[y]/(y^q - 1)$ given by mapping to the two factors and then projecting to $k[y]/(y^q - 1)$ agree.

Let v denote the valuation on $A[\zeta]$ normalized so that $v(p) = 1$. Let $a \leq 1/(p-1)$ be the largest number such that

$$(3.1.1) \quad \text{for all } (b, f(y)) \in R \text{ we have } v(b - f(\zeta)) \geq a.$$

Note that the expression $f(\zeta)$ makes sense only modulo $\zeta_p - 1$, and so the condition above is meaningless if $a > v(\zeta_p - 1) = 1/(p-1)$.

Let $(b, f(y))$ be an element of R . Then because R is a Λ_p -ring, there is an element $(c, g(y)) \in pR$ such that

$$(c, g(y)) = (b, f(y))^p - \psi_p(b, f(y)) = (b^p - f^*(\zeta^p), f(y)^p - f^*(y^p)).$$

On the other hand, because of our assumption on a , we have

$$1 + a \leq v(c - g(\zeta)) = v((b^p - f^*(\zeta^p)) - (f(\zeta)^p - f^*(\zeta^p))) = v(b^p - f(\zeta)^p).$$

But because the integral polynomial $p(X - Y)$ divides $(X - Y)^p - (X^p - Y^p)$, we have

$$v((b - f(\zeta))^p - (b^p - f(\zeta)^p)) \geq 1 + a$$

and hence $v(b - f(\zeta)) \geq (1 + a)/p$. That is, $(1 + a)/p$ satisfies (3.1.1).

But then $a = 1/(p-1)$ because otherwise this would violate the maximality of a . In other words, for any element $(b, f(y)) \in R$, the element $\zeta_p - 1$ divides $b - f(\zeta)$. This is just another way of saying b and $f(y)$ have the same image in $A[\zeta]/(\zeta_p - 1) = k[y]/(y^q - 1)$, and hence the element $(b, f(y))$ lies in the fiber product, which we showed above is $A[\mu_{pq}]$. \square

3.2. Remark. It is not true that $\mathbf{Z}_p[V]$ is maximal for every finite abelian group V . For example, if $V = \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$ and $x = \frac{1}{p} \sum_{\sigma \in V} \sigma$, then $\psi_p(x) = p$ and $x^2 = px$. Therefore, the subring $\mathbf{Z}_p[V][x]$ of $\mathbf{Q}_p[V]$ is a sub- Λ_p -ring which is finite over \mathbf{Z}_p . The global analogue also holds: $\mathbf{Z}[V]$ is not the maximal integral Λ -model for $\mathbf{Q}[V]$. This follows from the local statement.

3.3. Proposition. *Let K be a finite étale $\mathbf{Q}\Lambda$ -ring, and let R be a Λ -order. If $\mathbf{Z}_p \otimes R$ is a maximal Λ_p -order in $\mathbf{Q}_p \otimes R$ for all primes p , then R is maximal.*

Proof. Let S be the maximal Λ -order in $\mathbf{Q} \otimes R$. Because $\mathbf{Z}_p \otimes R$ is the maximal Λ_p -order in $\mathbf{Q}_p \otimes R$, the inclusion $\mathbf{Z}_p \otimes R \subseteq \mathbf{Z}_p \otimes S$ is an equality. Therefore R and S have the same rank, and p does not divide the index of R in S . \square

3.4. Theorem. *Let $r \geq 1$ be an integer. Then $\mathbf{Z}[\mu_r]$ is the maximal Λ -order in $\mathbf{Q}[\mu_r]$.*

Proof. By 3.3, it suffices to show that for every prime p , the Λ_p -order $\mathbf{Z}_p[\mu_r]$ is maximal. Write $r = qn$, where q is the largest power of p dividing r . Then $\mathbf{Z}_p[\mu_r] = \mathbf{Z}_p[\mu_n][\mu_q] = \prod_A A[\mu_q]$, where A runs over the irreducible factors of $\mathbf{Z}_p[\mu_n]$, all of which are unramified extensions of \mathbf{Z}_p . By 3.1, each factor $A[\mu_q]$ is a maximal Λ_p -order, and therefore so is their product. \square

3.5. Remark. Using 0.3 and 1.2, we can also describe the maximal Λ -order in general as follows. Let S be a finite $\mathbf{Z}/r\mathbf{Z}^\circ$ -set, let $\zeta_r \in \bar{\mathbf{Q}}$ denote a primitive r -th root of unity, and let $K = \text{Hom}_{\mathbf{Z}/r\mathbf{Z}^*}(S, \mathbf{Q}(\zeta_r))$ denote the corresponding finite étale Λ -ring over \mathbf{Q} . Consider the isomorphism

$$\mathbf{Q}[\mu_r] \rightarrow \prod_{d|r} \mathbf{Q}(\zeta_r^d)$$

given by $z \mapsto (\dots, \zeta_r^d, \dots)_{d|r}$. Then the maximal Λ -order in K is the set of elements $f \in K$ such that for all $s \in S$, the element

$$(\dots, f(ds), \dots)_{d|r} \in \prod_{d|r} \mathbf{Q}(\zeta_r^d) \cong \mathbf{Q}[\mu_r]$$

lies in $\mathbf{Z}[\mu_r]$.

3.6. We conclude with a fact about torsion in Λ -rings, which was brought to our attention by Clauwens. We therefore assume the reader is familiar with the basics of the theory of Λ -rings outside the torsion-free setting. (E.g., see [4], [7], or [1].)

Proposition. *Every torsion element in a Λ -ring is nilpotent.*

Proof. For any element x of a Λ -ring R , write

$$\lambda(x) = 1 + t\lambda_1(x) + t^2\lambda_2(x) + \dots \in 1 + tR[[t]].$$

Then we have $\lambda(x+y) = \lambda(x)\lambda(y)$ for all $x, y \in R$. Let r be an element of R such that $p^n r = 0$ for some prime p and integer $n \geq 0$. Since any torsion element of R is the sum of such elements, it suffices to show r is nilpotent. We have

$$1 = \lambda(p^n r) = \lambda(r)^{p^n} = (1 + rt + \dots)^{p^n},$$

which is congruent to $1 + r^{p^n} t^{p^n} + \dots$ modulo p . Therefore $r^{p^n} = ps$, for some $s \in R$, and hence we have

$$r^{1+np^n} = rp^n s^n = 0.$$

□

In fact, a similar proof shows that any torsion element of p -power order in a Λ_p -ring is nilpotent.

Corollary 0.3 then follows from this proposition and theorems 0.1 and 0.2.

REFERENCES

- [1] James Borger and Ben Wieland. Plethystic algebra. *Adv. Math.*, 194(2):246–283, 2005.
- [2] F. J. B. J. Clauwens. Commuting polynomials and λ -ring structures on $\mathbf{Z}[x]$. *J. Pure Appl. Algebra*, 95(3):261–269, 1994.
- [3] A. Grothendieck. Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas IV. *Inst. Hautes Études Sci. Publ. Math.*, (32):361, 1967.
- [4] Alexander Grothendieck. La théorie des classes de Chern. *Bull. Soc. Math. France*, 86:137–154, 1958.
- [5] Michel A. Kervaire and M. Pavaman Murthy. On the projective class group of cyclic groups of prime power order. *Comment. Math. Helv.*, 52(3):415–452, 1977.
- [6] Jürgen Neukirch. *Class field theory*, volume 280 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, Berlin, 1986.
- [7] Clarence Wilkerson. Lambda-rings, binomial domains, and vector bundles over $\mathbf{CP}(\infty)$. *Comm. Algebra*, 10(3):311–328, 1982.

E-mail address: borger@maths.anu.edu.au, desmit@math.leidenuniv.nl