LAMBDA ACTIONS OF RINGS OF INTEGERS

JAMES BORGER, BART DE SMIT

Abstract. Let \( O \) be the ring of integers of a number field \( K \). For an \( O \)-algebra \( R \) which is torsion free as an \( O \)-module we define what we mean by a \( \Lambda_O \)-ring structure on \( R \). We can determine whether a finite étale \( K \)-algebra \( E \) with \( \Lambda_O \)-ring structure has an integral model in terms of a Deligne-Ribet monoid of \( K \). This a commutative monoid whose invertible elements form a ray class group.

1. Introduction

Let \( O \) be a Dedekind domain with quotient field \( K \). Denote the set of maximal ideals of \( O \) by \( \mathcal{M} \). We assume that \( k(p) = O/p \) is a finite field for each \( p \in \mathcal{M} \).

Let \( E \) be a torsion-free commutative \( O \)-algebra. Then for each \( p \in \mathcal{M} \) the algebra \( E/pE = E \otimes_O k(p) \) over \( k(p) \) has a natural \( k(p) \)-algebra endomorphism \( F_p : x \mapsto x^{#k(p)} \), which is called the Frobenius endomorphism. By a Frobenius lift of \( E \) at \( p \) we mean an \( O \)-algebra endomorphism \( \psi_p \) such that \( \psi_p \otimes k(p) = F_p \). We define a \( \Lambda_O \)-structure on \( E \) to be a map \( \mathcal{M} \to \text{End}_{O_{\text{alg}}}(E) \), denoted \( p \mapsto \psi_p \), such that

1. \( \psi_p \) is a Frobenius lift at \( p \) for each \( p \in \mathcal{M} \).
2. \( \psi_p \psi_q = \psi_q \psi_p \) for all \( p, q \in \mathcal{M} \).

By a \( \Lambda_O \)-ring we mean a torsion-free \( O \)-algebra with \( \Lambda_O \)-structure.

If \( O \) is local then the commutation condition (2) is vacuous. For all \( p \in \mathcal{M} \) for which \( E \otimes k(p) = 0 \) the lifting condition (1) is vacuous. In particular, if \( E \) is an algebra over \( K \), then any commuting collection of \( K \)-automorphisms of \( E \) indexed by the maximal ideals of \( O \) is a \( \Lambda_O \)-structure on \( E \).

A \( \Lambda_\mathbb{Z} \)-structure on a ring without \( \mathbb{Z} \)-torsion is the same as a \( \lambda \)-ring structure [2]. For instance, for any abelian group \( A \) we have a natural \( \Lambda_\mathbb{Z} \)-structure on the group ring \( \mathbb{Z}[A] \) given by \( \psi_p(a) = a^p \) for \( a \in A \) and \( p \) a prime number.

If \( O \) is the ring of integers of a number field \( K \), and \( E \) is the ring of integers of a subfield \( L \) of the strict Hilbert class field of \( K \), then \( E \) has a unique \( \Lambda_O \)-structure: \( \psi_p \) is the Artin symbol of \( p \) in the field extension \( K \subset L \).

This preprint is a preliminary version dating from 2006. We are making it available in this form because some people would like to cite it now. The final version should be available before long.
In an earlier paper [1], we showed that a $\Lambda_\mathbb{Z}$-ring that is reduced and finite flat over $\mathbb{Z}$ is a $\Lambda_\mathbb{Z}$-subring of $\mathbb{Z}[C]^n$ for some finite cyclic group $C$ and positive integer $n$. The proof uses the explicit description of ray class fields over $\mathbb{Q}$ as cyclotomic fields. Over a number field class field theory is less explicit, and the generalizations we present in the present paper are by consequence less explicit. However, we can still give a very similar criterion for a $\Lambda_\mathcal{O}$-structure on a finite étale $K$-algebra $E$ to come from an $\Lambda_\mathcal{O}$-subring which is finite flat as an $\mathcal{O}$-module see Theorem 1.2 below. Such a $\Lambda_\mathcal{O}$-subring is called an integral $\Lambda_\mathcal{O}$-model of the $\Lambda_\mathcal{O}$-ring $E$.

Let $I$ be the monoid of non-zero ideals of $\mathcal{O}$, with ideal multiplication as the monoid operation. It is the free commutative monoid on $\mathcal{M}$. Let $K^{\text{sep}}$ be a separable closure of $K$, and let $G_K$ be the Galois group of $K^{\text{sep}}$ over $K$. It is a profinite group. By a $G_K$-set $X$ we mean a finite discrete set with a continuous $G_K$-action. By Grothendieck’s formulation of Galois theory, a finite étale $K$-algebra $E$ is determined by the $G_K$-set $S$ consisting of all $K$-algebra homomorphisms $E \rightarrow K^{\text{sep}}$. Giving a $\Lambda_\mathcal{O}$-structure on $E$ then translates to giving a monoid map $I/\mathcal{O} \rightarrow \text{Map}_{G_K}(S, S)$. By giving $I$ the discrete topology, we see that the category of $\Lambda_\mathcal{O}$-rings whose underlying $\mathcal{O}$-algebra is a finite étale $K$-algebra, is anti-equivalent to the category of finite discrete sets with a continuous action of the monoid $I/\mathcal{O} \times G_K$.

Let us first suppose that $\mathcal{O}$ is complete discrete valuation ring with maximal ideal $\mathfrak{p}$. Then $I(\mathcal{O})$ is isomorphic as a monoid to the monoid of non-negative integers with addition. Let $I_K \subset G_K$ be the inertia subgroup. Then $I_K$ is normal in $G_K$ and $G_K/I_K$ is the absolute Galois group of $k(\mathfrak{p})$, which contains the Frobenius element $F \in G_K/I_K$ given by $x \mapsto x^{\#F(\mathfrak{p})}$. Thus, $F$ acts on any $G_K$-set on which $I_K$ acts trivially.

**Theorem 1.1.** Suppose $\mathcal{O}$ is complete discrete valuation ring with maximal ideal $\mathfrak{p}$. Let $E$ be a finite étale $K$-algebra with $\Lambda_\mathcal{O}$-structure, and let $S$ be the set of $K$-algebra maps from $E$ to $K^{\text{sep}}$. Then $K$ has an integral $\Lambda_\mathcal{O}$-model if and only if the action of $I(\mathcal{O}) \times G_K$ on $S$ satisfies the two conditions

\begin{enumerate}
  \item the group $I_K$ acts trivially on $S_{\text{unr}} = \bigcap_{\mathfrak{a} \in I(\mathcal{O})} \mathfrak{a}S$;
  \item $\mathfrak{p} \in I(\mathcal{O})$ and $F \in G_K/I_K$ act in the same way on $S_{\text{unr}}$.
\end{enumerate}

See Section 2 for the proof.

Next, let us assume that $\mathcal{O}$ is the ring of integers in a number field.

In order to phrase our global result we first recall the definition of the Deligne-Ribet monoid. A cycle of $K$ is a formal product $\mathfrak{f} = \prod \mathfrak{p}^{n_\mathfrak{p}}$, where the product ranges over all primes of $K$, both finite and infinite, all $n_\mathfrak{p}$ are non-negative integers, only finitely many of which are non-zero, and we have $n_\mathfrak{p} \in \{0, 1\}$ for real primes $\mathfrak{p}$, and $n_\mathfrak{p} = 0$ for complex primes.
if and only if there is a cycle $f$. Theorem 1.2. Suppose $O$ of $K$ is a finite field. Then the inertia group $I$ is a complete discrete valuation ring with maximal ideal $p$. We write $k = k(p)$. Let $A$ be a reduced finite flat $O$-algebra.

Let us suppose first that $A$ is unramified over $O$, i.e., that $k \otimes_O A$ is étale over $k$. Then $k \otimes_O A$ is a product of finite fields. Since $A$ is complete in its $p$-adic topology, idempotents of $A/pA$ lift to $A$, so that $A$ is a finite product of rings of integers in finite unramified extensions of $K$. Write

$$S = \text{Hom}_{O\text{-alg}}(A, K^{\text{sep}}) = \text{Hom}_{K\text{-alg}}(A \otimes_O K, K^{\text{sep}}).$$

Then the inertia group $I_K \subset G_K$ acts trivially on $S$. Every finite unramified field extension $L$ of $K$ is Galois with an abelian Galois group, and its rings of integers has a unique Frobenius lift, which is

$$I = \prod_{p < \infty} \mathbb{B}^{\omega_p},$$

which can be viewed as an element of $I(O)$. We write $\text{ord}_p(f) = n_p$.

For a cycle $f$ we say that two non-zero $O$-ideals $a$ and $b$ are $f$-equivalent if $xa = b$ for some $x \in K^*$ with $x > 0$ at all real places $p$ with $\text{ord}_p(f) > 0$, and $\text{ord}_p(x - 1) + \text{ord}_p(a) \geq \text{ord}_p(f)$ at all finite places $p$. One can check that this is an equivalence relation, and that the multiplication of ideals is well-defined on the quotient set. Thus, the quotient set is a monoid, the Deligne-Ribet-monoid, and we denote it by $\text{DR}(f)$.

It is not hard to see that the ray class group $\text{Cl}(f)$ is the group of invertible elements of $\text{DR}(f)$. Also, $\text{DR}(1)$ is a group: it is the class group of $O$. More generally, for each ideal $d$ dividing $f$ finitely we can consider the map $i_d : \text{Cl}(f/d) \to \text{DR}(f)$ that sends the class of an ideal $a$ to the class of $a \cdot d$. These maps give rise to a bijection

$$i = \prod i_d : \prod_{a \mid f} \text{Cl}(f/a) \cong \text{DR}(f).$$

**Theorem 1.2.** Suppose $O$ is the ring of integers of a number field $K$. Let $E$ be a finite étale $K$-algebra with $\Lambda_O$-structure, and let $S$ be the set of $K$-algebra maps from $E$ to $K^{\text{sep}}$. Then $K$ has an integral $\Lambda_O$-model if and only if there is a cycle $f$ of $K$ so that the action of $G_{K^{\text{sep}}} \times I(O)$ on $S$ factors (necessarily uniquely) through the map

$$G_K \times I(O) \to \text{DR}(f),$$

which is the product of the Artin symbol $G_K \to \text{Cl}(f) \subset \text{DR}(f)$ on the first coordinate, and the quotient map $I(O) \to \text{DR}(f)$ on the second.

It follows that the category of such $A$-rings is anti-equivalent to the category of finite discrete sets with a continuous action by the profinite monoid $\lim \text{DR}(f)$, where the limit is taken over all cycles $f$ with respect to the canonical maps $\text{DR}(f) \to \text{DR}(f')$ when $f' | f$. When $K = \mathbb{Q}$ this limit is the multiplicative monoid of profinite integers.

2. **The local case**

Suppose that $O$ is a complete discrete valuation ring with maximal ideal $p$. We write $k = k(p)$. Let $A$ be a reduced finite flat $O$-algebra.

Let us suppose first that $A$ is unramified over $O$, i.e., that $k \otimes_O A$ is étale over $k$. Then $k \otimes_O A$ is a product of finite fields. Since $A$ is complete in its $p$-adic topology, idempotents of $A/pA$ lift to $A$, so that $A$ is a finite product of rings of integers in finite unramified extensions of $K$. Write

$$S = \text{Hom}_{O\text{-alg}}(A, K^{\text{sep}}) = \text{Hom}_{K\text{-alg}}(A \otimes_O K, K^{\text{sep}}).$$

Then the inertia group $I_K \subset G_K$ acts trivially on $S$. Every finite unramified field extension $L$ of $K$ is Galois with an abelian Galois group, and its rings of integers has a unique Frobenius lift, which is
homomorphisms $f$ and $s$ set of all and it splits the inclusion $S$. Since $S$ is a quotient $\Lambda_E$-ring of $E$ on $S$ and that $A$ is a sub-$\Lambda_O$-ring of $E$ with Frobenius lift $f_0$ at $p$. We will show that the $\Lambda_O$-ring surjection $E 	o E_0$ splits.

Note that now $p^k S = S_0$ for sufficiently large $k$, so $p$ act as a bijection on $S_0$. Thus, $f_0$ is an automorphism of $E_0$. For $s \in S_i$ we have $p^i s \in S_0$ and $p$ acts invertibly on $S_0$, so we can define a map $S \to S_0$ by sending $s \in S_i$ to $p^{-i}(p^i s)$.

Now suppose that the $\Lambda_O$-ring $E$ has an integral model, i.e., that $E$ has an $O$-sub algebra $A$ which satisfies

1. $A$ is finite flat over $O$;
2. $\psi_p(A) \subset A$;
3. $\psi_p \otimes O k$ is the Frobenius $x \mapsto x^k$ on $A \otimes k$.

The image $A_0$ of $A$ in the quotient ring $E_0$ of $E$ is a sub-$\Lambda_O$-ring of $E_0$ which is reduced and finitely generated as an $O$-module and $O$-torsion free. Thus, $E_0$ has an integral $\Lambda_O$-model. Since $f_0$ is an automorphism of $E_0$ the rings $A_0$ and its subring $f(A_0)$ have the same discriminant.
Thus, \( f_0(A_0) = A_0 \) and \( f_0 \) is an automorphism of \( A_0 \). This implies that the map \( x \mapsto x^{\#k} \) on \( A_0 \otimes \mathcal{O} k \) is an automorphism, so that \( A_0 \) is unramified over \( \mathcal{O} \). Conditions (1) and (2) of Theorem 1.1 now follow by Proposition 2.1.

For the converse, suppose that conditions (1) and (2) hold. We will produce an integral \( \Lambda_{\mathcal{O}} \)-model of \( E = E_0 \times \cdots \times E_n \). Let \( R_i \) be the integral closure of \( \mathcal{O} \) in \( E_i \). Since \( I_K \) acts trivially on \( S_0 \) the ring \( R_0 \) has a unique \( \Lambda_{\mathcal{O}} \)-structure by Proposition 2.1. Now suppose that

\[
A = i(R_0) \oplus (0 \times a_1 \times \cdots \times a_n)
\]

with \( a_i \) an ideal in \( R_i \). Then the condition \( \psi_p(a) - a^{\#k(p)} \in pA \) for all \( a \in A \) is equivalent to \( a_i^{\#k(p)} \subset p a_i \) and \( f_i(a_{i-1}) \subset p a_i \). This holds, for instance if \( a_i = p^i R_i \), in which case \( A \) is an integral \( \Lambda_{\mathcal{O}} \)-model of \( E \). \( \Box \)

The integral model that is supplied by the proof is not always optimal. For instance, for the \( \Lambda_{\mathcal{O}} \)-ring \( \mathbb{Z}[C_4] \) we get a strict subring. However for the \( \Lambda_{\mathcal{O}} \)-ring \( \mathbb{Z}[V_4] \) the proof provides a \( \Lambda_{\mathcal{O}} \)-subring of \( \mathbb{Q}[V_4] \) which is strictly larger than \( \mathbb{Z}[V_4] \).

3. **Global arguments**

Now assume that \( K \) is a global field with ring of integers \( \mathcal{O} \). Let \( E \) be a finite étale \( K \)-algebra with a \( \Lambda_{\mathcal{O}} \)-structure. Writing \( S = \text{Hom}_K(E, K^{\text{sep}}) \) we thus get an action of \( I(\mathcal{O}) \times G_K \) on \( S \).

For each maximal ideal \( p \) of \( \mathcal{O} \) we consider the completion \( \mathcal{O}_p \), and its quotient field \( K_p \). Then we obtain an \( \Lambda_{\mathcal{O}_p} \)-structure on the finite étale \( K_p \)-algebra \( E_p = E \otimes K K_p \). If \( A \) is an integral \( \Lambda_{\mathcal{O}} \)-model of \( E \), then \( A \otimes \mathcal{O} \mathcal{O}_p \) is an integral \( \Lambda_{\mathcal{O}_p} \)-model of \( E_p \).

Fixing an embedding \( K^{\text{sep}} \to K^{\text{sep}} \) for each \( p \) we can view \( G_p \) as a subgroup of \( G_K \). The finite étale \( K_p \)-algebra \( E_p \) then corresponds to the \( G_p \)-set that one gets by restricting the action of \( G_K \) on \( S \) to \( G_p \).

Let us assume that an integral \( \Lambda_{\mathcal{O}} \)-model \( A \) of \( E \) exists. Let \( \bar{G} \) be the image of \( G_K \) in \( \text{Map}(S, S) \). Chebotarev’s theorem now implies the following: for each \( g \in \bar{G} \) there is a maximal ideal \( p = p_g \) of \( \mathcal{O} \) so that

1. the image of \( I_p \) is trivial in \( \bar{G} \);
2. the image of \( F_p \in G_p/I_p \) in \( \bar{G} \) is \( g \);
3. \( A \) is unramified at \( p \).

By Proposition 2.1, the action of \( g \) on \( S \) is the same as the action of \( p_g \) on \( S \). Since the \( p_g \) commute with eachother, it follows that \( \bar{G} \) is abelian.

It remains to show that the \( I(\mathcal{O}) \times G_K \)-action on \( S \) factors through the Deligne-Ribet monoid of some cycle \( f \).

By class field theory, any continuous action of \( G_K \) on a finite discrete set \( T \), whose image is abelian, factors, by the Artin map, through the ray class group \( \text{Cl}(c(T)) \) for a minimal cycle \( c(T) \) of \( K \), which we call the conductor of \( T \).
Define \( r \in I(\mathcal{O}) \) by setting

\[
\text{ord}_p(r) = \inf \{ i \geq 0 : p^{i+1}S = p^iS \}
\]

for all maximal ideals \( p \) of \( \mathcal{O} \). This is well defined because \( pS = S \) whenever \( p \) is unramified in \( A \) by Proposition unramified.

We now define the cycle \( \mathfrak{f} \) by

\[
\mathfrak{f} = \text{lcm}_{\mathfrak{p} \mid \mathfrak{f}} \mathfrak{d} \cdot c(\mathfrak{d}S).
\]

Note first that \( c(S) \mid \mathfrak{f} \), so the \( G_K \)-action on \( S \) factors through the Artin map \( G_K \rightarrow \text{Cl}(\mathfrak{f}) \).

Next, we claim that for \( a \in I(\mathcal{O}) \) coprime to \( \mathfrak{f} \) the action of \( a \) on \( S \) is equal that of its class \([a] \) in \( \text{Cl}(\mathfrak{f}) \). It suffices to prove this for \( a = p \) prime. Then one notes that \( r \mid f \) so \( p \nmid r \) so \( p \) acts as a bijection on \( S \).

By our local result, \( A \) is unramified at \( p \) and \( p \) acts as \( F_p \in G_p/I_p \) on \( S \). By the definition of the Artin symbol, the action of \([p] \in \text{Cl}(\mathfrak{f})\) is the same. This shows the claim.

Now suppose that \( \mathfrak{d} \in I(\mathcal{O}) \) with \( \mathfrak{d} \mid \mathfrak{f} \). Let us write \( I_\mathfrak{d} \) for the submonoid of \( I(\mathcal{O}) \) consisting of all \( a \in I(\mathcal{O}) \) that are coprime to \( f/\mathfrak{d} \).

We now claim that \( I_\mathfrak{d} \) acts by bijections on \( \mathfrak{d}S \), by the definition of \( f \) is quotient of \( \text{Cl}(f/\mathfrak{d}) \). and that the action factors through \( \text{Cl}(f/\mathfrak{d}) \). To see this, let \( a = \text{gcd}(\mathfrak{d}, r) \) and write \( \mathfrak{d} = ab \). By definition of \( r \) all prime divisors of \( b \) act bijectively on \( \mathfrak{d}S \), so \( c(aS) = c(\mathfrak{d}S) \) is coprime to \( b \).

By definition of \( f \) we have \( c(aS) \mid f/ga \), and it follows that \( c(aS) \mid f/\mathfrak{d} \).

Thus, \( G_K \)-action on \( \mathfrak{d}S \) factors through \( \text{Cl}(f/\mathfrak{d}) \) and the claim holds.

Since multiplication by any divisor \( \mathfrak{d} \in I(\mathcal{O}) \) of \( f \) gives a bijection \( \text{Cl}(f/\mathfrak{d}) \rightarrow [\mathfrak{d}]DR(f)* \) this shows that the action of \( \{ a \in I(\mathcal{O}) : \gcd(a, f) = \mathfrak{d} \} \) on \( S \) factors through \( [\mathfrak{d}]DR(f)* \). Taking the union over all \( \mathfrak{d} \) we see that the \( I(\mathcal{O}) \)-actions factors through \( DR(f) \).

For the converse, assume that the \( G_K \times I(\mathcal{O}) \)-action on \( S \) factors through \( DR(f) \) for some cycle \( f \).

We first show the existence, for each \( p \in \mathcal{M} \) of an integral \( \Lambda_{\mathcal{O}_p} \)-model for the \( \Lambda_{\mathcal{O}_p} \)-ring \( E \otimes_K K_p \). For \( p \nmid f \) this follows from the definition of the Artin map and Proposition 2.1. So assume \( p \nmid f \), and write \( f = p^{n}f' \) with \( p \nmid f' \). Then \([p^{k}] \in [p^{n}]\text{Cl}(f') \subset DR(f) \) for all \( k \geq n \). This implies that the action of \( p \) on \( \bigcap_i p^{i}S = p^{n}S \) is given by the Artin symbol of \([p] \in \text{Cl}(f') \), which by Theorem 1.1 guarantees existence of an integral \( \Lambda_{\mathcal{O}_p} \)-model.

Now let \( R \) be the integral closure of \( \mathcal{O} \) in \( E \). Then \( R \) is finite flat over \( \mathcal{O} \) and \( E = R \otimes_{\mathcal{O}} K \). For all \( p \nmid f \) we are in the unramified case, and our integral \( \Lambda_{\mathcal{O}_p} \)-module is equal to \( R \otimes_{\mathcal{O}} \mathcal{O}_p \). It follows that the intersection \( A \) over all \( p \) of our integral \( \Lambda_{\mathcal{O}_p} \)-module gives a sub-\( \mathcal{O} \)-algebra of \( R \), which is of finite index, and which is closed under all \( \psi_p \).

Also, each \( \psi_p \) are Frobenius lifts, since \( A \otimes_{\mathcal{O}} \mathcal{O}_p \) is a \( \Lambda_{\mathcal{O}_p} \)-ring. This proves Theorem 1.2.
REFERENCES

[1] James Borger and Bart de Smit. Galois theory and integral models of \( \Lambda \)-rings. *Bull. Lond. Math. Soc.*, 40(3):439–446, 2008.

[2] Clarence Wilkerson. Lambda-rings, binomial domains, and vector bundles over \( \mathbb{C}P(\infty) \). *Comm. Algebra*, 10(3):311–328, 1982.

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