ON SOME INFINITE ABELIAN EXTENSIONS OF ALGEBRAIC NUMBER FIELDS

by Kenkichi Iwasawa

Let \( l \) be a prime number and let \( \mathbb{Z}_l \) and \( \mathbb{Q}_l \) denote the ring of \( l \)-adic integers and the field of \( l \)-adic numbers respectively; their additive groups will be also denoted by the same letters.

Now, an extension \( K \) of a field \( k \) is called a \( \mathbb{Z}_l \)-extension if \( K/k \) is a Galois extension and its Galois group is topologically isomorphic to the additive group \( \mathbb{Z}_l \). For such an extension \( K/k \), there exists a sequence of fields

\[
k = k_0 \subset k_1 \subset \ldots \subset k_n \subset \ldots
\]

such that each \( k_n/k \) is a cyclic extension of degree \( l^n \) and \( K \) is the union of all \( k_n \), \( n \geq 0 \). Conversely, if there is a sequence of cyclic extensions \( k_n/k \) such as mentioned above, then the union \( K \) of all \( k_n \), \( n \geq 0 \), is a \( \mathbb{Z}_l \)-extension of \( k \).

In the following, we shall consider \( \mathbb{Z}_l \)-extensions of which the ground fields are finite algebraic number fields, i.e. finite extensions of the rational field \( \mathbb{Q} \). We first give some examples. For each \( n \geq 0 \), let \( P_{l,n} \) denote the cyclotomic field of \( l^{n+1} \)-th or \( 2^{n+2} \)-th roots of unity according as \( l > 2 \) or \( l = 2 \). Let \( P_l = P_{l,0} \) and let \( P_{l,\infty} \) be the union of all \( P_{l,n}, n \geq 0 \). Then \( P_{l,\infty}/P_l \) is a \( \mathbb{Z}_l \)-extension with intermediate fields \( P_{l,n}, n \geq 0 \). The field \( P_{l,\infty} \) has a unique subfield \( Q_{l,\infty} \) such that \( P_l \cap Q_{l,\infty} = \mathbb{Q} \), \( P_l/Q_{l,\infty} = P_{l,\infty} \), and this \( Q_{l,\infty} \) gives us the unique \( \mathbb{Z}_l \)-extension of the rational field \( \mathbb{Q} \). Furthermore, for any finite algebraic number field \( k \), the composite \( kQ_{l,\infty} \) is a \( \mathbb{Z}_l \)-extension of \( k \). Hence each \( k \) has at least one \( \mathbb{Z}_l \)-extension over it.

Let \( K \) be a \( \mathbb{Z}_l \)-extension of a finite algebraic number field \( k \) and let \( k_n, n \geq 0 \), be the intermediate fields of \( k \) and \( K \). Let \( C_n \) denote the ideal-class group of \( k_n \), and \( A_n \) the Sylow \( l \)-subgroup of \( C_n \). Denote by \( l^n \) the order of \( A_n \), i.e. the highest power of \( l \) dividing the class number of \( k_n \). Then, for all sufficiently large \( n \), the exponent \( e_n \) is given by a formula

\[
e_n = \lambda n + \mu l^n + \nu,
\]

where \( \lambda, \mu, \) and \( \nu \) are integers (\( \lambda, \mu \geq 0 \)), independent of \( n \). Since these integers are uniquely determined for given \( K/k \) by the above formula, we shall denote them by \( \lambda(K/k), \mu(K/k), \) and \( \nu(K/k) \) respectively. For the special \( \mathbb{Z}_l \)-extension \( K = kQ_{l,\infty} \) over \( k \), they will be denoted also by \( \lambda_l(k), \mu_l(k), \) and \( \nu_l(k) \) respectively; furthermore we

\[ (*) \text{ In earlier papers, the author called such extensions } \Gamma \text{-extensions.} \]
simply put \( \lambda_i = \lambda_i(P_l), \mu_i = \mu_i(P_l), v_i = v_i(P_l) \). Thus we obtain arithmetic invariants \( \lambda_i(k), \mu_i(k), v_i(k) \) depending upon \( k \) and \( l \), and \( \lambda_i, \mu_i, v_i \) for each prime number \( l \).

Let \( O \) denote the ring of all algebraic integers in \( K \), \( I \) the group of all invertible \( O \)-modules in \( K \), and \( C \) the factor group of \( I \) modulo the principal \( O \)-modules \((2)\); we may simply call \( I \) and \( C \) the ideal group and the ideal-class group of \( O \) in \( K \), respectively. Let \( A \) be the Sylow \( l \)-subgroup (i.e. the \( l \)-primary component) of \( C \). Then \( C \) is the direct limit of \( C_n, n \geq 0 \), and \( A \) that of \( A_n, n \geq 0 \), and the Galois group \( \text{Gal}(K/k) \) acts on \( C \) and \( A \) in the obvious manner. The above formula for \( e_n \) is obtained by analysing the structure of this Gal \((K/k)\)-module \( A \). Thus we see in particular that the Tate module \( T(A) \) for the abelian \( l \)-group \( A \) is a free \( \mathbb{Z}_l \)-module and its rank over \( \mathbb{Z}_l \) is equal to the invariant \( \lambda \).

At the present, little is known on the nature of the invariants \( \lambda(K/k), \mu(K/k), v(K/k) \) defined above. Yet it is clear that they play an essential role in the theory of \( \mathbb{Z}_l \)-extensions. It seems particularly interesting to see when \( \lambda = 0 \) or \( \mu = 0 \) or \( \lambda = \mu = 0 \). It is easy to find a \( \mathbb{Z}_l \)-extension \( K/k \) for which \( \lambda(K/k) \) is arbitrary large. On the other hand, no example of \( K/k \) with \( \mu(K/k) = 0 \) is quite limited, we are tempted to conjecture that \( \mu(K/k) = 0 \) for every \( \mathbb{Z}_l \)-extension \( K/k \), or at least that \( \mu_i(k) = 0 \) for every \( k \) and \( l \) or \( \mu_i = 0 \) for every \( l \).

For the invariants \( \lambda_i \) and \( \mu_i \), we know that \( \lambda_i = \mu_i = 0 \) if and only if \( l \) is a regular prime, and if this is the case, then \( v_i = 0 \) also. Let \( P_l^i \) denote the maximal real subfield of \( P_l \) and put
\[
\lambda_i' = \lambda_i(P_l^i), \quad \mu_i' = \mu_i(P_l^i), \quad v_i' = v_i(P_l^i).
\]

Then \( \lambda_i' \leq \lambda_i, \mu_i' \leq \mu_i \). Now, a well-known conjecture of Vandiver states that the class number of \( P_l^i \) is not divisible by \( l \) for every prime number \( l \); it is checked by numerical computation for a large number of primes. For given \( l \), the conjecture is equivalent with \( \lambda_i' = \mu_i' = v_i' = 0 \). Unlike what is said above for \( \lambda_i, \mu_i, \) and \( v_i \), it is not known whether \( \lambda_i' = \mu_i' = 0 \) implies \( v_i' = 0 \) and, hence, Vandiver's conjecture. Nevertheless, it would be an interesting problem to find out if \( \lambda_i' = \mu_i' = 0 \) for every \( l \).

Let \( T(A) \) be the Tate module defined above and let \( V \) denote the tensor product of \( T(A) \) and \( Q_l \) over \( \mathbb{Z}_l \). \( V = V_l(A) = T_l(A) \otimes Q_l \). \( V \) is a vector space of dimension \( \lambda \) over \( Q_l \) and the Galois group \( \text{Gal}(K/k) \) acts on \( V \) continuously so that it defines an \( l \)-adic representation of \( \text{Gal}(K/k) \). It is clear that the definition of \( V \) above is completely parallel to the usual construction of such \( l \)-adic representations by means of, say, abelian varieties \((3)\). Note also that if \( k' \) is a subfield of \( k \) such that \( K/k' \) is a Galois extension, then the same vector space \( V \) defines an \( l \)-adic representation of the larger group \( \text{Gal}(K/k') \).

Let \( l > 2 \) and \( k = P_1, K = P_{l, \infty} \) in the above \((4)\). Then \( V \) is decomposed into the direct sum of \( l - 1 \) subspaces \( V_l \), \( 0 \leq l < l - 1 \), with respect to the action of

---

\((2)\) In other words, \( C = \text{Pic}(O) \). Note that the ring \( O \) is not noetherian.


\((4)\) For \( l = 2 \), slight modification is needed in what is said below about the decomposition of \( V \) and the definition of \( \sigma_0 \).
Gal \((P_i/Q)\). Let \(W\) denote the group of all roots of unity in \(P_{l,\infty}\) with order a power of \(l\). Let \(\sigma_0\) be the automorphism of \(K/k\) such that \(\sigma_0(\zeta) = \zeta^{1+l}\) for every \(\zeta\) in \(W\) and let \(f(x)\) be the characteristic polynomial of \(\sigma_0\) acting on \(V_i\). Assuming Vandiver’s conjecture for the prime \(l\), we can describe the representation of \(\text{Gal}(K/k)\) on each \(V_i\) rather explicitly. It then follows \(^4\) in particular that the characteristic polynomials \(f(x), 0 \leq i < l - 1\), are closely related to the \(l\)-adic \(L\)-functions of Kubota-Leopoldt associated with the characters \(\text{Gal}(P_i/Q) \to \mathbb{Z}_l^*\).

For a \(Z_l\)-extension \(K/k\) in general, we know very little on the structure of the \(l\)-adic representation \(\text{Gal}(K/k) \to GL(V)\). However the following fact might be of some interest, in particular when viewed as an analogue of a similar result in algebraic geometry. Let \(k\) be any finite algebraic number field containing \(P_i\) and let

\[
\begin{align*}
K &= kQ_{l,\infty} = kP_{l,\infty}.
\end{align*}
\]

Let \(O'\) denote the ring of all \(l\)-integers in \(K\), i.e., the union of all \(l^{-n}O, n \geq 0\). Let \(C'\) be the ideal class group of \(O'\) in \(K\), and \(A'\) the Sylow \(l\)-subgroup of \(C'\). Let \(V' = T(A') \otimes O_i\) over \(Z_l\), where \(T(A')\) denotes the Tate module for \(A'\). As before, \(V'\) defines an \(l\)-adic representation of \(\text{Gal}(K/k)\), and the natural map \(A \to A'\) induces an epimorphism \(\text{Gal}(K/k) \to \text{Gal}(A')\) so that \(V'\) is a factor space of the representation space \(V\). Now, an element \(\alpha\) in \(K\) will be called \(l\)-hyperprimary \((n \geq 0)\) if \(\alpha\) is an \(l\)-th power in the \(v\)-completion \(K_v\) for every place \(v\) of \(K\) lying above the place \(l\) of \(Q\) \(^6\), and an \(O'\)-module \(\alpha\) of \(K\) will be called hyperprimary if, for some \(n \geq 0\), \(\alpha^{l^n} = (\alpha)\) with an \(l\)-hyperprimary element \(\alpha\) in \(K\). Let \(B'\) be the subgroup of all classes in \(A'\) which are represented by hyperprimary \(O'\)-modules and let \(V'' = T(B') \otimes Z_l\). Then \(V''\) again defines an \(l\)-adic representation of \(\text{Gal}(K/k)\), and \(B' \to A'\) induces a monomorphism \(\text{Gal}(B') \to \text{Gal}(A')\) so that \(V''\) is a subspace of \(V'\). Hence \(V''\) is involved in the original representation space \(V\). Let \(W\) be the group of roots of unity as defined above and let \(V_0 = T(W) \otimes Z_l\). Then \(V_0\) defines a one-dimensional \(l\)-adic representation of \(\text{Gal}(K/k)\) through its action on \(W\).

Now, suppose that the ground field \(k\) is abelian either over the rational field or over an imaginary quadratic field. Then we can prove \(^7\) that there exists a non-degenerate skew-symmetric \(O_i\)-bilinear form

\[
V'' \times V'' \to V_0
\]

such that

\[
\langle \sigma u, \sigma v \rangle = \sigma(\langle u, v \rangle)
\]

for all \(u, v\) in \(V''\) and \(\sigma\) in \(\text{Gal}(K/k)\). It follows that \(V''\) is even dimensional and that the characteristic polynomial of each \(\sigma\) in \(\text{Gal}(K/k)\) acting on \(V''\) satisfies a functional equation similar to the one for the zeta-function of an algebraic curve defined over a finite field \(^8\).


\(^{(*)}\) There exist only a finite number of such places \(v\) in \(K\).

\(^{(*)}\) The proof will be published elsewhere.

\(^{(*)}\) Actually we can prove the above result for a wider class of ground fields including those mentioned above. It seems likely that the same result holds for an arbitrary ground field \(k\) containing \(P_i\), without any further assumption on \(k\).
As already mentioned, the skew-symmetric form defined above is essentially an analogue of the classical Riemann forms on complex tori, of which a purely algebraic construction was given by Weil for abelian varieties of arbitrary characteristic (\(^{(9)}\)). It would be interesting to pursue such analogy further in studying the structure of the representation space \(V''\).


Princeton University
Department of Mathematics,
Princeton, New Jersey 08540
(U. S. A.)