Notes on Abelian Class field theory

S. Subramanian

1. Let $K$ be a number field which for us would be a finite Galois extension of $Q$, the field of rational numbers (in particular, $Q$ itself is a number field). The problem that is of interest is to understand $\text{Gal}(\overline{K}/K)^{ab}$ which is the abelianisation of $\text{Gal}(\overline{K}/K)$, the Galois group of $K$, where $\overline{K}$ denotes an algebraic closure of $K$. We let $\mathcal{O}_K$ denote the ring of integers of $K$, and $\mathbb{Z}$ the ring of integers of $Q$.

Let $M$ be a finitely generated $\mathcal{O}_K$ submodule of $K$. Since $M \subset K$, it is clear that $M \otimes_{\mathcal{O}_K} K = K$, so that rank of $M$ as an $\mathcal{O}_K$ module is one. Let $M^*$ denote the dual $\mathcal{O}$-module $M^* = \text{Hom}_{\mathcal{O}_K}(M, \mathcal{O}_K)$. Then $M^*$ is also a rank one $\mathcal{O}_K$-module, so that $M^* \otimes_{\mathcal{O}_K} K = K$. Since $M^*$ is finitely generated as an $\mathcal{O}_K$-module let $m_1, \ldots, m_r$ be generates for $M^*$. The isomorphism $M^* \otimes_{\mathcal{O}_K} K \rightarrow K$ enables us to regard $m_i \otimes 1$ as elements of $K$, so we see that $M^*$ is also a finitely generated $\mathcal{O}_K$ submodule of $K$. It is now clear that $M \otimes_{\mathcal{O}_K} M^* = \mathcal{O}_K$ and further $M \otimes_{\mathcal{O}_K} M^* = MM^*$ where on the right hand side, the multiplication is in $K$, regarding $M$ and $M^*$ as submodules of $K$. Let $\mathcal{C}(K)$ denote the group of such finitely generated $\mathcal{O}_K$ submodules of $K$. It is clear that $\mathcal{C}(K)$ is an abelian group.

Let $p_1, p_2, q_1, q_2$ be prime elements of $\mathcal{O}_K$ (we emphasise: prime elements,
not prime ideals) such that \( p_1 p_2 = q_1 q_2 \) and the \( p_i, q_i \) are all distinct. Consider the \( \mathcal{O}_K \)-module \( M \) generated by \( \frac{1}{p_1}, \frac{1}{q_1} \), in \( K \). Then \( M \otimes_{\mathcal{O}_K} \mathcal{O}_K[\frac{1}{p_2}, \frac{1}{q_2}] \) is isomorphic to \( \mathcal{O}_K[\frac{1}{p_2}, \frac{1}{q_2}] \) as an \( \mathcal{O}_K[\frac{1}{p_2}, \frac{1}{q_2}] \) module, but \( M \) is not isomorphic to \( \mathcal{O}_K \) as an \( \mathcal{O}_K \)-module. This is a simple example of the fact that \( \mathcal{O}_K \) is a UFD if and only if \( \mathcal{C}_\ell(K) = 1 \). Since \( K/Q \) is a finite Galois extension, all but finitely many primes in \( \mathbb{Z} \) remain unramified in \( \mathcal{O}_K \). Let \( \{p_1, \cdots, p_m\} \) be the set of primes in \( \mathbb{Z} \) outside which \( \text{Spec} \mathcal{O}_K \to \text{Spec} \mathbb{Z} \) is unramified. Let \( S \) be the inverse image in \( \mathcal{O}_K \) of the set \( \{p_1, \cdots, p_m\} \). We observe first that for \( M \in \mathcal{C}_\ell(K) \) we have an inclusion

\[
\mathcal{O}_K \subset M
\]

such that \( M/\mathcal{O}_K \) is a torsion \( \mathcal{O}_K \)-module. Also, we have a strictly decreasing sequence

\[
M \supset M^2 \supset M^3 \supset \cdots \supset \mathcal{O}_K
\]

and hence it follows that \( M^n = \mathcal{O}_K \) for some positive integer \( n \), so that every element of \( \mathcal{C}_\ell(K) \) is of finite order.

We need the following lemma:

**Lemma (1.1):** Let \( X \) be an affine one-dimensional scheme (like \( \text{Spec} \mathbb{Z} \) or \( \text{Spec} \mathcal{O}_K \)) and \( \pi : Y \to X \) a finite Galois etale morphism. Suppose every line bundle on \( X \) is trivial. Then every line bundle on \( Y \) is trivial.

**Proof of Lemma (1.1):** Let \( L \) be a line bundle on \( Y \), possibly non trivial. We consider the vector bundle \( \pi_*L \) on \( X \). Let rank \( \pi_*L = r = \text{degree of } \pi \). Since \( X \) is affine and one dimensional, we obtain an exact sequence

\[
\mathcal{O} \to \mathcal{O}_X^{\oplus (r-1)} \to \pi_*L \to M \to 0
\]
where $M$ is a line bundle on $X$ (equal to $\det \pi_* L$). By hypothesis, $M$ is trivial, and on an affine scheme, extensions split, so $\pi_* L$ is trivial. This implies that $L$ is trivial. Q.E.D.

Let $\mathcal{O}_{K, S}$ denote the localisation of $\mathcal{O}_K$ obtained by inverting all the elements of $S$, and $\mathbb{Z}_{(p_1, \ldots, p_m)}$ the localisation of $\mathbb{Z}$ obtained by inverting $p_1, \ldots, p_m$. Then the morphism $\text{Spec} \mathcal{O}_{K, S} \to \text{Spec} \mathbb{Z}_{(p_1, \ldots, p_m)}$ is etale, and hence by Lemma 1 above every line bundle on $\text{Spec} \mathcal{O}_{K, S}$ is trivial. This forces:

**Lemma (1.2):** Any $M \in \mathcal{C}_\ell(K)$ satisfies $M \subset \mathcal{O}_{K, S}$.

In particular:

**(Lemma 1.3):** $\mathcal{C}_\ell(K)$ is finite.

2. Let $K$ be a number field as before, and $L/K$ a finite, Galois extension (not necessarily abelian), with Galois group $G$ and let $G^{ab}$ be the abelianisation of $G$, so that we have an exact sequence

$$1 \to [G, G] \to G \to G^{ab} \to 1.$$ 

We have

**Proposition (2.1):** Let $M \in \mathcal{C}_\ell(L)$ such that $M$ is not the pullback of an element of $\mathcal{C}_\ell(K)$. Then

$$\sigma_1^* \sigma_2^* M = \sigma_2^* \sigma_1^* M$$

$\forall \sigma_1, \sigma_2 \in G$ such that $\sigma_1 \sigma_2 \neq \sigma_2 \sigma_1$. 
Proof. Since $\sigma_1, \sigma_2$ do not commute in $G$, the orbit of $M$ under $< \sigma_1, \sigma_2 >$ is a non-abelian subgroup of $\mathcal{C}\ell(L)$ which is abelian (here $< \sigma_1, \sigma_2 >$ denotes the group generated by $\sigma_1, \sigma_2$). It follows that the commutator $[G, G]$ acts trivially on $\mathcal{C}\ell(L)$. Q.E.D.

Proposition (2.2): Any element $M \in \mathcal{C}\ell(L)$ fixed by $G^{ab}$, descends to an element of $\mathcal{C}\ell(K)$.

Proof: Follows from the above proposition and Galois descent. Q.E.D.

Theorem (2.3): Let $K$ be a number field, and let $M \in \mathcal{C}\ell(K)$, $M \neq \mathcal{O}_K$. Let $M^n = \mathcal{O}$, where $n$ is the order of $M$. Then there is a finite cyclic $\mathbb{Z}/n$ extension $L/K$ such that $M$ becomes trivial in $\mathcal{C}\ell(L)$.

Proof: Let $\mathcal{O}_K$ be the ring of integers of $K$ and consider the ring

$$R = \mathcal{O}_K \oplus M \oplus M^2 \oplus \cdots \oplus M^{n-1}$$

$R$ is an $\mathcal{O}_K$-algebra, and defines an integral extension of $\mathcal{O}_K$, whose quotient field does the job. Q.E.D.

Theorem (2.4): Let $K$ be a number field such that $\mathcal{C}\ell(K)$ is nontrivial. Then there exists a finite abelian Galois extension $L/K$ such that every $M \in \mathcal{C}\ell(K)$ becomes the trivial element of $\mathcal{C}\ell(L)$.

Proof: By Theorem (2.3) above, we can do it for every element of $\mathcal{C}\ell(K)$, and since $\mathcal{C}\ell(K)$ is finite, we obtain a finite extension where this happens. Q.E.D.
**Theorem (2.5):** Let $K$ be a number field such that $\mathcal{C}\ell(K)$ is nontrivial. Then there is a finite, Galois, abelian extension $L/K$ whose Galois group is $\mathcal{C}\ell(K)$ such that every $M \in \mathcal{C}\ell(K)$ becomes trivial in $\mathcal{C}\ell(L)$.

**Proof:** Follows from previous steps. Q.E.D.

3. We now consider a number field $K$ such that $\mathcal{C}\ell(K) = 1$. As remarked before, it is easy to see that in this case the ring of integers $\mathcal{O}_K$ is a UFD and hence a principal ideal domain. The typical case is $\mathbb{Z}$ in $\mathbb{Q}$ and the arguments in the general case are similar.

Let $L/\mathbb{Q}$ be a finite, Galois, abelian extension of $\mathbb{Q}$ with Galois group $G$. Since $G$ is a finite abelian group, by the Chinese Remainder Theorem, $G = \mathbb{Z}/p_1^{a_1} \otimes \cdots \otimes \mathbb{Z}/p_n^{a_n}$ where $p_1, \ldots, p_n$ are rational primes. By going modulo a subgroup of $G$ (every subgroup of $G$ is normal since $G$ is abelian) we may assume that the Galois group of $L/K$ is $\mathbb{Z}/p^a$. Unlike in the coprime case, when we used the Chinese Remainder Theorem, and could have assumed the base field was $\mathbb{Q}$ without loss of generality, the group $\mathbb{Z}/p^a$ is a non split extension of $\mathbb{Z}/p$ factors. We first consider the case when $L/K$ is a Galois extension with Galois group $\mathbb{Z}/p$, and as before, we consider the case $K = \mathbb{Q}$ (the general case in similar). Let $\mathcal{O}_L$ be the ring of integers of $L$ and let $q$ be a rational prime in $\mathbb{Z}$. These are two cases to consider: $p \neq q, p = q$.

**Case (i)** $q \neq p$. 
**Claim:** In this case, $\text{Spec} \mathcal{O}_L \to \text{Spec} \mathbb{Z}$ is etale at $q$. For, we consider a prime $q_1 \in \mathcal{O}_L$ such that $q_1^2$ divides $q$ in $\mathcal{O}_L$. We consider the completion $L_{q_1}$ of $L$ at $q_1$ and the completion $Q_q$ of $Q$ at $q$. We thus obtain an extension of local fields $L_{q_1}/Q_q$, again with Galois group $\mathbb{Z}/p$. However, the residue field extension $\mathcal{O}_L/q_1$ over $\mathbb{Z}/q$ is an extension of the finite field $\mathbb{Z}/q$ and hence its Galois group is cyclic (generated by the Frobenius at $q$). This cyclic group has to be a quotient of $\mathbb{Z}/p$ and hence has to be isomorphic to $\mathbb{Z}/p$. This shows that $q$ remains unramified.

**Case (ii) the case $q = p$.** We recall that $L/Q$ is a Galois extension with Galois group $\mathbb{Z}/p$ and by Case (i) treated above, $\mathcal{O}_L$ is unramified outside $p$. By Lemma (1.2) above, it follows that $\mathcal{C}_L(L) = 1$.

From the above arguments, it follows that $\pm 1 \in \mathbb{Z}$ are the only points ramified in the extension (possibly except for $p$) and hence the field extension is obtained by adjoining roots of unity.

Further, since every time the class group remains trivial (in the case of a $\mathbb{Z}/p^a$ extension), we can repeat the argument. We thus obtain

**Theorem (3.1):** Let $K$ be a number field with $\mathcal{C}_L(K) = 1$. Then any abelian extension of $K$ is obtained by adjoining roots of unity.

**Remark:** The exception occurs in the case of $\mathbb{Z}/2$ extension of $Q$, where $Q(\sqrt{p})$ is an abelian $\mathbb{Z}/2$ extension not obtained by adjoining a root of unity, where $p$ is a rational prime. This can be seen by looking at the arguments in Cases (i) and (ii) above. These fields have trivial class group by Lemma (1.2) above.
Address: School of Mathematics, Tata Institute of Fundamental Research, Mumbai 400005, India

Email: subramnn@math.tifr.res.in