First Galois cohomology and extensions of Galois representations

This note explains basics regarding first Galois cohomology and extensions of Galois representations. For this, it is better to first work with k-vector spaces for a field k (with discrete topology). We will remark about general cases later.

Let G be a (pro)finite group, acting on a finite dimensional k-vector space M. Then we have learned two equivalent ways to define $H^*(G, M)$:

(1) as $\mathrm{Ext}^*_{k[G]}(k, M)$, where k is the trivial $k[G]$-module,
(2) or as the cohomology of the complex $C^0(G, M) \to C^1(G, M) \to C^2(G, M) \to \cdots$.

From point of view of (1), there is a so-called Yoneda extension realization of Ext^1: a class $[c] \in \mathrm{Ext}^1_{k[G]}(k, M)$ is represented by a short exact sequence

$$0 \to M \to E_c \to k \to 0 \tag{0.0.1}$$

of $k[G]$-modules, where E_c is a $k[G]$-module that fits in (0.0.1), called *an extension of k by M*. (Be careful about the orders of k and M above; in my opinion, it is a little strange, but I guess this is probably for historical reasons that I don't know.)

Explicitly, given an extension (0.0.1), we may take the G-cohomology to get

$$\begin{tikzcd} (E_c)^G \arrow[r] & k^G = k \arrow[dll, rounded corners, "\delta"] \\ H^1(G, M) \arrow[r] & \cdots \end{tikzcd}$$

The image $\delta(1) \in H^1(G, M)$ is the class $[c]$.

(Exercise: when $\delta(1) = 0$, we must have $(E_c)^G \to k^G$ is surjective. Show that this implies that the exact sequence (0.0.1) splits.)

In terms of point of view of (2), we may make the extension (0.0.1) explicit as follows: Identify M with $k^{\oplus n}$ to write $\rho : G \to \mathrm{GL}_k(M) = \mathrm{GL}_n(k)$ for the representation given by M, and the class $[c] \in H^1(G, M)$ is represented by a cocycle class $g \mapsto c_g$ in $C^1(G, M)$ (we think of c_g as a column vector, after identifying M with $k^{\oplus n}$ as above). Then we explicitly construct the G-representation E_c as follows: $E_c \cong k^{\oplus n+1}$ as a k-vector space, and the G-action is given by

$$g \mapsto \begin{pmatrix} \rho(g) & c_g \\ 0 & 1 \end{pmatrix},$$

where this is a block matrix, and $\rho(g)$ has size $n \times n$.

Let us check that this representation is a homomorphism, i.e. we need

$$\begin{pmatrix} \rho(g) & c_g \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \rho(h) & c_h \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \rho(gh) & c_{gh} \\ 0 & 1 \end{pmatrix}.$$

Computing entries, we see that we need

$$c_{gh} = \rho(g)c_h + c_g.$$

This is precisely the cocycle condition for group cohomology.

Exercise: if we fix a different isomorphism $E_c \cong k^{\oplus n+1}$ (still respecting the subspace M identified with $k^{\oplus n}$, i.e. just change the last vector to something else in $k^{\oplus n+1}$), then the end representation corresponds to changing the cocycle c by a coboundary.

Exercise: The two processes above are inverse of each other, if you can interested, you can check that.

Remarks on general cases:

(1) General coefficients: if M is just a finite abelian group with (continuous) G-action, $[c] \in H^1(G, M)$ corresponds to an extension

$$0 \to M \to E_c \to \mathbb{Z} \to 0$$

where E_c is just an abelian group with G-action. When M is an $\mathbb{F}_p$-vector space, we can tensor the above extension with $\mathbb{F}_p$ to get back to (0.0.1).

In general, such construction work with continuous version of group cohomology and continuous chain complexes and so on.

(2) For $H^i(G, M)$ with $i > 1$, we have similar extensions. For example, $i = 2$, $H^2(G, M)$ classifies the following extensions (up to equivalence)

$$0 \to M \to E_1 \to E_2 \to k \to 0$$

If for two such extensions, we have a commutative digram

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r] \arrow[d, equal] & E_1 \arrow[r] \arrow[d] & E_2 \arrow[r] \arrow[d] & k \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & M \arrow[r] & E_1' \arrow[r] & E_2' \arrow[r] & k \arrow[r] & 0,
\end{tikzcd}$$

the two extension are equivalent, and the equivalent relations among all such extensions are generated by those above.