6. Cyclic and Solvable Extensions. Resolvents.

Let G be group. A *G-module* is an abelian group A together with a G-action $G \times A \to A$ compatible with the group operation in A (i.e., $\sigma : A \to A$ is an automorphism of A for all $\sigma \in G$). A *crossed homomorphism* from G to A is a map $f : G \to A$ satifying $f(\sigma\tau) = \sigma f(\tau) + f(\sigma)$. Crossed homomorphisms fit into a larger scheme called group cohomology, wherefore they are also known as 1-*cocycles*. Such an f is said to be a *coboundary* if $f(\sigma) = \sigma\beta - \beta$ for some $\beta \in A$.

If G is finite and A is written additively, the *G-trace* of an element $\alpha \in A$ is defined as

$$tr_G(\alpha) = \sum_{\sigma \in G} \sigma(\alpha)\,.$$

If A is written multiplicatively, it is customary to call this the *G-norm* and write it as $\mathrm{N}_G(\alpha)$.

1. Let $G = \langle\sigma\rangle$ be finite cyclic, A a G-module.
  (i) Show that any crossed homomorphism $f : G \to A$ is determined by the single value $f(\sigma)$.
  (ii) Show that there is a bijection between crossed homomorphisms and elements $\alpha \in A$ such that $\mathrm{tr}_G(\alpha) = 0$.

2. Let G be a finite group of automorphisms of a field K.
  (i) Show that every crossed homomorphism $f : G \to K^\times$ is a coboundary. [*Hint*: imitate Lagrange resolvents.]
  (ii) Show that every crossed homomorphism $f : G \to K^+$ is a coboundary. [*Hint*: imitate (i).]

3. Let k be a a field of characteristic $p > 0$.
  (i) For $0 \neq a \in k$ let K be a splitting field of the polynomial $X^p - X + a$. Show that K/k is cyclic of degree p.
  (ii) Show that any cyclic extension K/k of degree p has the form $K = k(\alpha)$ with $\alpha^p - \alpha \in k$.

4. Let $k = \mathbf{Q}$ and consider the complex numbers $\omega = e^{2\pi i/9}$ and $\theta = \omega + \bar{\omega}$.
  (i) Find the minimal polynomials over k of ω and θ.
  (ii) Show that $k(\omega)$ and $k(\theta)$ are cyclic extensions of k.

5. A *derivation* on a ring R is an additive endomorphism D satisfying $D(ab) = aD(b) + D(a)b$.
  (i) Show: for any field F, the ring $F[x]$ of polynomials has a unique F-linear derivation with $D(x) = 1$.
  (ii) Let $P_0, P_1, \ldots, P_n$, with $n > 1$, be points dividing the semi-circle of radius 1 into n equal parts. If d_k denotes the distance from P_0 to P_k, show that $d_1 d_2 \cdots d_n = 2\sqrt{n}$.

6. For a prime $p > 2$, let ζ be a primitive p-th root of 1, and $\alpha = 2^{1/p} > 0$ be real.
  (i) If $F = \mathbf{Q}(\zeta)$, $K = \mathbf{Q}(\alpha)$, and $E = \mathbf{Q}(\alpha, \zeta)$, show that E/F and E/K are cyclic of degree p and $p - 1$, respectively.
  (ii) Show the $E/\mathbf{Q}$ is Galois and that $\mathrm{Aut}(E)$ is isomorphic to the subgroup $G \subset GL_2(\mathbf{F}_p)$ of matrices having $[0, 1]$ for their second row.