Solutions 24

Abelian Extensions, Group cohomology

1. For an integer $n \geqslant 2$ let L be the maximal abelian extension of $\mathbb{Q}$ for which $\mathrm{Gal}(L/\mathbb{Q})$ has exponent dividing n. Determine $\mathrm{Gal}(L/\mathbb{Q})$ up to isomorphism.

   Solution: Since $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) \cong \hat{\mathbb{Z}}^\times \cong \prod_p \mathbb{Z}_p^\times$, we have $\mathrm{Gal}(Ł/\mathbb{Q}) \cong \prod_p \mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^n$. Here each $\mathbb{Z}_p^\times$ is a topologically finitely generated abelian group; hence $\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^n$ is a finite abelian group of order dividing n. By the classification of finite abelian groups that is more specifically a direct product of cyclic groups of prime power order dividing n. We claim that every prime power $\ell^k|n$ occurs infinitely often as factor. As the product has countably many factors, this implies that

$$\mathrm{Gal}(L/K) \;\cong\; \prod_{\ell^k}(\mathbb{Z}/\ell^k\mathbb{Z})^{\mathbb{N}} \;\cong\; \prod_{m|n}(\mathbb{Z}/m\mathbb{Z})^{\mathbb{N}}.$$

   To prove the claim consider any prime $p \equiv 1+\ell^k \bmod \ell^{k+1}$. Then we have $\ell^k|p-1$ and $\ell^{k+1} \nmid p-1$; hence the ℓ-Sylow subgroup of $\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^n$ is isomorphic to that of $\mathbb{F}_p^\times/(\mathbb{F}_p^\times)^n$ and cyclic of order ℓ^k. As there are infinitely many such primes by Dirichlet's theorem on primes in arithmetic progressions, this proves the claim.

2. Is there an abelian extension $K/\mathbb{Q}$ of degree 2023 that is unramified at all primes not dividing 2024, or vice versa?

   Solution: By the Kronecker-Weber theorem the maximal abelian extension of $\mathbb{Q}$ that is unramified outside $2024 = 2^3 \cdot 11 \cdot 23$ is generated by all roots of unity of order a power of $2, 11, 23$, and its Galois group over $\mathbb{Q}$ is

$$\mathbb{Z}_2^\times \times \mathbb{Z}_{11}^\times \times \mathbb{Z}_{23}^\times \;\cong\; \mu_2 \times \mathbb{Z}_2 \times \mu_{10} \times \mathbb{Z}_{11} \times \mu_{22} \times \mathbb{Z}_{23}.$$

   Since $2023 = 7 \cdot 17^2$ is coprime to all the prime factors $2, 5, 11, 23$ of the orders on the right hand side, this group does not have a subgroup of index 2023. Thus the desired field does not exist.

   Similarly, the maximal abelian extension of $\mathbb{Q}$ that is unramified outside $2023 = 7 \cdot 17^2$ is generated by all roots of unity of order a power of 7 and 17, and its Galois group over $\mathbb{Q}$ is

$$\mathbb{Z}_7^\times \times \mathbb{Z}_{17}^\times \;\cong\; \mu_6 \times \mathbb{Z}_7 \times \mu_{16} \times \mathbb{Z}_{17}.$$

   Since the factors 11 and 13 of $2024 = 2^3 \cdot 11 \cdot 23$ do not appear among the prime factors $2, 3, 7, 17$ of the orders on the right hand side, this group does not have a subgroup of index 2024. Thus again the desired field does not exist.

3. Show that, up to isomorphism, the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ from exercise 4 of sheet 20 is the unique Galois extension of $\mathbb{Q}$ with Galois group isomorphic to $\mathbb{Z}_p$.

   Solution: By the theorem of Kronecker-Weber, any $\mathbb{Z}_p$-extension of $\mathbb{Q}$ can be identified with a subfield of $\mathbb{Q}^{\mathrm{ab}}$. Since $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) \cong \hat{\mathbb{Z}}^\times$, by the Galois correspondence it suffices to prove that there is a unique closed subgroup $\Gamma < \hat{\mathbb{Z}}^\times$ with quotient isomorphic to $\mathbb{Z}_p$. So consider such a subgroup Γ and look at the continuous homomorphism $\pi\colon \hat{\mathbb{Z}}^\times \twoheadrightarrow \hat{\mathbb{Z}}^\times/\Gamma \cong \mathbb{Z}_p$.

   We study the restriction of π to each factor in the decomposition $\hat{\mathbb{Z}}^\times \cong \bigtimes_\ell \mathbb{Z}_\ell^\times$. For this recall that $\mathbb{Z}_\ell^\times$ is topologically isomorphic to the product of $\mathbb{Z}_\ell$ with a discrete finite group. Since $\mathbb{Z}_p$ does not contain any non-trivial element of finite order, the restriction of π to that finite group must be trivial. Also, for $\ell \neq p$ and any $n \geqslant 0$ the multiplication by p^n is an isomorphism on $\mathbb{Z}_\ell$. Thus the subgroup isomorphic to $\mathbb{Z}_\ell$ must map into $p^n\mathbb{Z}_p$ under π. Varying n this shows that its image is contained in $\bigcap_{n\geqslant 0} p^n\mathbb{Z}_p = \{0\}$. Together this proves that the restriction of π to $\mathbb{Z}_\ell^\times$ is trivial for every $\ell \neq p$.

   Letting Γ' be the product of all those factors as well as the finite factor of $\mathbb{Z}_p^\times$, this shows that $\Gamma' < \Gamma$. On the other hand we now already have $\hat{\mathbb{Z}}^\times/\Gamma' \cong \mathbb{Z}_p$. Thus if $\Gamma' \neq \Gamma$, then $\hat{\mathbb{Z}}^\times/\Gamma$ would be isomorphic to the factor group of $\mathbb{Z}_p$ by a nontrivial closed subgroup. But any nontrivial closed subgroup of $\mathbb{Z}_p$ contains an element of the form $p^n u$ for some $n \geqslant 0$ and some $u \in \mathbb{Z}_p^\times$, and being closed it then contains the whole subgroup $p^n\mathbb{Z}_p$. In particular the factor group is then finite. Thus $\hat{\mathbb{Z}}^\times/\Gamma$ implies that $\Gamma' = \Gamma$, proving the desired uniqueness.

4. Consider a finite cyclic group G of order n and a $\mathbb{Z}[G]$-module M. Take $i \in \{0, -1\}$.

   (a) Show that $\hat{H}^i(G, M)$ is annihilated by n.

   (b) Show that $\hat{H}^i(G, M)$ is finite if M is finitely generated.

   Solution

   (a) For any $m \in M^G$ we have $g'm = m$ for all $g' \in G$. From $N_G := \sum_{g'\in G} g'$ we thus obtain $nm = N_G m \in N_G M$ and hence $n[m] = 0$ in $M^G/N_G M$. Therefore $n \cdot \hat{H}^0(G, M) = 0$.

   Next consider any $m \in M$ with $N_G m = 0$. Then $nm = nm - N_G m = \sum_{g'\in G}(1 - g')m \in I_G M$ and hence $n[m] = 0$ in $\ker(N_G|M)/I_G M$. Therefore $n \cdot \hat{H}^{-1}(G, M) = 0$.

   (b) The ring $\mathbb{Z}[G]$ is a free $\mathbb{Z}$-module of finite rank n. Since M is finitely generated over $\mathbb{Z}[G]$, it is also finitely generated over $\mathbb{Z}$. Since $\mathbb{Z}$ is noetherian, the same follows for its submodules M^G and $\ker(N_G|M)$ and hence for $\hat{H}^i(G, M)$. By (a) this is also annihilated by n and thus a finitely generated module over the finite ring $\mathbb{Z}/n\mathbb{Z}$. It is therefore finite.

5. Prove the *Normal Basis Theorem* for an arbitrary finite Galois extension L/K: There exists $b \in L$ such that the elements ${}^{\gamma}b$ for $\gamma \in \mathrm{Gal}(L/K)$ form a basis of L over K.

   Solution See [Artin: Galois Theory, Theorem 28].