QUIZ 4, MATH100C, SPRING 2021

1. Suppose A and B are finite abelian groups and $S^1 := \{z \in \mathbb{C} \mid |z| = 1\}$. Let $f : A \times B \to S^1$ be a pairing; this means that f is a group homomorphism with respect to each component separately. Let

$$f_A : A \to \widehat{B}, (f_A(a))(b) := f(a,b), \quad \text{and} \quad f^B : B \to \widehat{A}, (f^B(b))(a) := f(a,b),$$

where $\widehat{A}$ and $\widehat{B}$ are the duals of A and B, respectively. Suppose f_A is a group isomorphism.

   (a) (2 points) Suppose $b \in \ker f^B$. Prove that $b \in \ker \chi$ for every $\chi \in \widehat{B}$.

   Solution. The fact $b \in \ker f^B$ means $f^B(b)$ is the trivial homomorphism, i.e. $f(a,b) = (f^B(b))(a) = 1$ for any $a \in A$. If $\chi \in \widehat{B}$ because f_A is surjective there exists some $a \in A$ such that $\chi = f_A(a)$, but then $\chi(b) = (f_A(a))(b) = f(a,b) = 1$, so $b \in \ker \chi$.

   (b) (2 points) Prove that f^B is injective.

   Solution. Suppose $b \in \ker f^B$; by (a) we find $b \in \ker \chi$ for all $\chi \in \widehat{B}$, i.e. $\chi(b) = 1$. But we've seen in class that if $b \neq 0$ then there exists some $\chi \in \widehat{B}$ such that $\chi(b) \neq 1$, and thus we deduce $b = 0$, so f^B is injective.

   (c) (2 points) Prove that f^B is an isomorphism.

   Solution. Recall we know from class that $|\widehat{A}| = |A|$ and $|\widehat{B}| = |B|$. From the fact that f_A is an isomorphism, we conclude that $|A| = |\widehat{B}|$, and thus $|B| = |\widehat{A}|$, and so the fact that $f^B : B \to \widehat{A}$ is injective implies surjectivity as well.

2. Suppose F is a field of characteristic 0 which contains an element ζ of order n and $\overline{F}$ is an algebraic closure of F. Suppose $E \in \mathrm{Int}(\overline{F}/F)$, E/F is a Galois extension, and $\mathrm{Aut}_F(E)$ is a finite abelian group of exponent n. Let

$$\Delta(E) := ((E^\times)^n \cap F^\times)/(F^\times)^n.$$

   (a) (2 points) Define the Kummer pairing $f : \mathrm{Aut}_F(E) \times \Delta(E) \to M_n$ where $M_n := \{1, \zeta, \dots, \zeta^{n-1}\}$.

   Solution. The Kummer pairing is given by

$$f(\sigma, \overline{a}) := \frac{\sigma(\alpha)}{\alpha}$$

   for some choice of $\alpha \in E^\times$ satisfying $a = \alpha^n$ (and where our notation $\overline{a}$ means the coset $a(F^\times)^n$).

   (b) (3 points) Prove the Kummer pairing is well-defined.

   Solution. See Lemma 33.2.4 in the notes.

   (c) (3 points) Prove that $f^{\Delta(E)} : \Delta(E) \to \widehat{\mathrm{Aut}_F(E)}$ is injective where $f^{\Delta(E)}$ is given as in the first problem.

   Solution. See Lemma 34.3.3 in the notes.

   (d) (2 points) Prove that $|\Delta(E)| \le |\mathrm{Aut}_F(E)|$.

   Solution. By the previous part one has $|\Delta(E)| \le |\widehat{\mathrm{Aut}_F(E)}|$, and we know that $|\widehat{\mathrm{Aut}_F(E)}| = |\mathrm{Aut}_F(E)|$, giving us the result.

3. Suppose p is prime and $F := \mathbb{Q}[\zeta_p]$ where $\zeta_p := e^{\frac{2\pi i}{p}}$. Suppose $a_1, \ldots, a_n \in F^\times$ are such that
$$\overline{A} := \langle a_1(F^\times)^p, \ldots, a_n(F^\times)^p \rangle$$
is a group of order p^n. Let $E := F[\sqrt[p]{a_1}, \ldots, \sqrt[p]{a_n}]$ where $\sqrt[p]{a_i}$ is a zero of $x^p - a_i$ in $\overline{F}$.

(a) (3 points) Let $g : \mathbb{Z}_p^n \to \overline{A}$, $g([m_1]_p, \ldots, [m_n]_p) := (\prod_{i=1}^n a_i^{m_i})(F^\times)^p$. Prove that g is a well-defined isomorphism.

Solution. To see g is well-defined, suppose $([m_1]_p, \ldots, [m_n]_p) = ([m'_1]_p, \ldots, [m'_n]_p)$ for $m_i, m'_i \in \mathbb{Z}$; this means that $m_i \equiv m'_i \pmod p$. As a result one can write $m_i = m'_i + k_i p$ for some $k_i \in \mathbb{Z}$, and then
$$(\prod_{i=1}^n a_i^{m_i})(F^\times)^p = (\prod_{i=1}^n a_i^{m'_i + k_i p})(F^\times)^p = (\prod_{i=1}^n a_i^{m'_i})(\prod_{i=1}^n a_i^{k_i p})(F^\times)^p = (\prod_{i=1}^n a_i^{m'_i})(F^\times)^p,$$
where the last equality is because $\prod_{i=1}^n a_i^{k_i p} \in (F^\times)^p$. This shows g is well-defined. It is straightforward to verify that g is a homomorphism. For bijectivity, notice the image of g contains each $a_i(F^\times)^p$ (because this element equals $g([0]_p, \ldots, [0]_p, [1]_p, [0]_p, \ldots, [0]_p)$ with the $[1]_p$ in the i-th position), and because these generate the codomain we see g is surjective. Then we notice that the two groups have the same order, so g is an isomorphism.

(b) (3 points) Suppose $K \in \mathrm{Int}(E/F)$ and $[K : F] = p$. Prove that K/F is Galois $\mathrm{Aut}_F(K) \simeq \mathbb{Z}_p$.

Solution. One has by Kummer theory that E/F is Galois (or one can directly see that E is a splitting field of $\prod_i (x^p - a_i)$ over F) and also $\mathrm{Aut}_F(E) \simeq \widehat{\Delta(E)} = \widehat{\overline{A}} \simeq \widehat{\mathbb{Z}_p^n} \simeq \mathbb{Z}_p^n$. In particular because the automorphism group is abelian one has that K/F is Galois, and thus $|\mathrm{Aut}_F(K)| = [K : F] = p$, which implies $\mathrm{Aut}_F(K) \simeq \mathbb{Z}_p$.

(c) (2 points) Suppose $K \in \mathrm{Int}(E/F)$ and $[K : F] = p$. Prove that $K = F[\sqrt[p]{a}]$ for some $a \in F$, where $\sqrt[p]{a}$ is a zero of $x^p - a$ in $\overline{F}$.

Solution. This follows immediately from the cyclic case of Kummer theory, i.e. surjectivity of Λ in Theorem 34.2.3; alternatively we proved this as Theorem 31.3.1.

(d) (1 points) Suppose $K \in \mathrm{Int}(E/F)$ and $K = F[\sqrt[p]{a}]$ for some $a \in F$. Prove that $a(F^\times)^p \in \Delta(E)$, where $\Delta(E)$ is given by Kummer theory (see problem 2).

Solution. Because $\sqrt[p]{a} \in K \subseteq E$ one has $a = (\sqrt[p]{a})^p \in (E^\times)^p \cap F^\times$, and thus $a(F^\times)^p \in ((E^\times)^p \cap F^\times)/(F^\times)^p = \Delta(E)$.

(e) (2 points) Suppose $K \in \mathrm{Int}(E/F)$ and $[K : F] = p$. Prove that $K = F[\sqrt[p]{a}]$ for some $a(F^\times)^p \in \overline{A}$ that has order p.

Solution. One knows from the cyclic case of Kummer theory that $\Delta(K)$ is cyclic, i.e. $\Delta(K) = \langle a(F^\times)^p \rangle$ for some $a \in F^\times$. But because $\Lambda \circ \Delta = \mathrm{id}$ one has $K = \Lambda(\Delta(K)) = \Lambda(\langle a(F^\times)^p \rangle) = F[\sqrt[p]{a}]$, and in addition $\mathrm{Aut}_F(K) \simeq \langle a(F^\times)^p \rangle$, which implies that $a(F^\times)^p$ has order p (since $|\mathrm{Aut}_F(K)| = p$ by part (b)) which gives the result.

(f) (2 points) Prove that there is a bijection between $\{K \in \mathrm{Int}(E/F) \mid [K : F] = p\}$ and one-dimensional subspaces of $\mathbb{Z}_p^n$.

Solution. One-dimensional subspaces of $\mathbb{Z}_p^n$ are the same as subgroups of order p, and then so we see using (a) it suffices to give a bijection between $\{K \in \mathrm{Int}(E/F) \mid [K : F] = p\}$ and subgroups of $\overline{A}$ of order p. On one hand if $[K : F] = p$ then we have seen that $K = F[\sqrt[p]{a}]$ for some $a \in F^\times$ with $a(F^\times)^p$ order p in $\Delta(E) = \overline{A}$. But this means that $\Delta(K) = \langle a(F^\times)^p \rangle$ is a subgroup of $\overline{A}$ of order p; conversely, if $H = \langle a(F^\times)^p \rangle$ is a subgroup of $\overline{A}$ of order p then $\Lambda(H) = F[\sqrt[p]{a}]$ is an intermediate field of E/F with degree p over F. In particular we see that Λ and Δ (restricted to the proper domains) give the inverse functions we need.

(g) (1 points) Prove that $|\{K \in \mathrm{Int}(E/F) \mid [K : F] = p\}| = \frac{p^n-1}{p-1}$.

Solution. By (f) we can count one-dimensional linear subspaces of $\mathbb{Z}_p^n$; any such subspace is generated by a nonzero element, and conversely any nonzero element of $\mathbb{Z}_p^n$ spans such a subspace; this gives $p^n - 1$ potential generating elements. In addition, two (nonzero) elements will generate the same subspace if and only if they are equal up to multiplication by an element of $\mathbb{Z}_p^\times$, of which there are $p-1$ elements, so this leads to the total number $\frac{p^n-1}{p-1}$ of one-dimensional subspaces.