

Math 286X: Arithmetic Statistics

Spring 2020

Problem set #8

Problem 1. Let G be a finite abelian group and let K be a number field. Consider the invponent $d : G \rightarrow \mathbb{R}^{\geq 0} \cup \{\infty\}$ given by $d(g) = |G| \cdot (1 - \frac{1}{\text{ord}(g)})$ corresponding to the discriminant invariant. Let p be the smallest prime factor of $|G|$ and let the p -torsion subgroup $G[p]$ of G have size p^k . Show that $a(d) = |G| \cdot (1 - \frac{1}{p})$ and $b(d, K) = \frac{p^k - 1}{[K(\zeta_p) : K]}$.

Solution. Since the function $\mathbb{Z}^{\geq 1} \rightarrow \mathbb{R}^{\geq 0}$ given by $x \mapsto |G| \cdot (1 - \frac{1}{x})$ is strictly increasing, $d(g)$ attains its minimum value exactly when $\text{ord}(g)$ is minimal. The minimal order of the elements of any group G is the smallest prime factor p dividing $|G|$. This shows that $a(d) = |G| \cdot (1 - \frac{1}{p})$. We have $\text{ord}(g) = p$ if and only if $g \in G[p] \setminus \{\text{id}\}$. The action of $(\mathbb{Z}/|G|\mathbb{Z})^\times$ on $G[p]$ factors through the free action of $(\mathbb{Z}/p\mathbb{Z})^\times$. The image of $U = \text{Gal}(K(\zeta_{|G|})|K) \subseteq (\mathbb{Z}/|G|\mathbb{Z})^\times$ in $(\mathbb{Z}/p\mathbb{Z})^\times$ is $\text{Gal}(K(\zeta_p)|K)$. Hence, each U -orbit in $G[p] \setminus \{\text{id}\}$ has exactly $[K(\zeta_p) : K]$ elements, so the number of orbits is $b(d, K) = \frac{p^k - 1}{[K(\zeta_p) : K]}$. \square

Problem 2 (Kummer theory for C_3 -extensions of \mathbb{Q}). Let C_3 be the cyclic group of order 3. Consider the algebraic group \mathcal{G} defined over \mathbb{Q} given by $\mathcal{G}(K) = (\mathbb{Q}(\zeta_3) \otimes_{\mathbb{Q}} K)^\times = (K[Z]/(Z^2 + Z + 1))^\times$ for any number field K . (As a variety, \mathcal{G} is the subvariety of \mathbb{A}^2 of pairs (a, b) , corresponding to $a + bZ$, such that $[N(a + bZ) = (a + bZ)(a + bZ^2) =]a^2 - ab + b^2 \neq 0$. This is also called the *Weil restriction* of the multiplicative group \mathbb{G}_m from $\mathbb{Q}(\zeta_3)$ to \mathbb{Q} .) Denote the automorphism of $\mathbb{Q}(\zeta_3)$ sending ζ_3 to ζ_3^2 by σ_2 . We also denote by σ_2 the resulting automorphism of $\mathcal{G}(K)$.

- a) Show that the kernel of the map $\mathcal{G}(\overline{\mathbb{Q}}) \rightarrow \mathcal{G}(\overline{\mathbb{Q}})$ sending x to x^3 is isomorphic to $C_3 \times C_3$.

Solution. First, note that there is an isomorphism $\mathbb{Q}(\zeta_3) \otimes_{\mathbb{Q}} \overline{\mathbb{Q}} \cong \overline{\mathbb{Q}}[Z]/(Z^2 + Z + 1) \cong \overline{\mathbb{Q}}[Z]/(Z - \zeta_3)(Z - \zeta_3^2) \cong \overline{\mathbb{Q}} \times \overline{\mathbb{Q}}$ of $\overline{\mathbb{Q}}$ -algebras given by $a \otimes b \mapsto (ab, \sigma_2(a)b)$.

This implies that $\mathcal{G}(\overline{\mathbb{Q}})$ is as a group isomorphic to $\overline{\mathbb{Q}}^\times \times \overline{\mathbb{Q}}^\times$.

Of course, the map $\overline{\mathbb{Q}}^\times \rightarrow \overline{\mathbb{Q}}^\times$ sending x to x^3 has kernel $\langle \zeta_3 \rangle \cong C_3$, so the map $\overline{\mathbb{Q}}^\times \times \overline{\mathbb{Q}}^\times \rightarrow \overline{\mathbb{Q}}^\times \times \overline{\mathbb{Q}}^\times$ sending x to x^3 has kernel $C_3 \times C_3$. (The kernel is not contained in $\mathcal{G}(\overline{\mathbb{Q}})$!) \square

- b) Show that the map $\varphi : \mathcal{G}(\overline{\mathbb{Q}}) \rightarrow \mathcal{G}(\overline{\mathbb{Q}})$ sending x to $x^2/\sigma_2(x)$ is surjective and has kernel contained in $\mathcal{G}(\overline{\mathbb{Q}})$ and isomorphic to C_3 .

Solution. Recall the isomorphism $\mathbb{Q}(\zeta_3) \otimes_{\mathbb{Q}} \overline{\mathbb{Q}} \cong \overline{\mathbb{Q}} \times \overline{\mathbb{Q}}$, $a \otimes b \mapsto (ab, \sigma_2(a)b)$ constructed in a). Note that the automorphism σ_2 of the left-hand side corresponds to the automorphism of the right hand side swapping the two factors $\overline{\mathbb{Q}}$. Consider an element x of $\mathcal{G}(\overline{\mathbb{Q}})$, corresponding to a pair $(x_1, x_2) \in \overline{\mathbb{Q}}^\times \times \overline{\mathbb{Q}}^\times$. Now, $x^2/\sigma_2(x) = 1$ is equivalent to $x_1^2/x_2 = x_2^2/x_1 = 1$. There are exactly three such pairs: $(1, 1), (\zeta_3, \zeta_3^2), (\zeta_3^2, \zeta_3)$, which correspond to $1 \otimes 1, \zeta_3 \otimes 1, \zeta_3^2 \otimes 1$ in $\mathcal{G}(\overline{\mathbb{Q}})$. For surjectivity, consider any $(y_1, y_2) \in \overline{\mathbb{Q}}^\times \times \overline{\mathbb{Q}}^\times$. We have $\varphi(x_1, x_2) = (y_1, y_2)$ if and only if $x_1^2/x_2 = y_1$ and $x_2^2/x_1 = y_2$. For example, we can take any x_1 with $x_1^3 = y_1^2 y_2$ and then let $x_2 = x_1^2/y_1$. \square

- c) Show that the $\Gamma_{\mathbb{Q}}$ -module $\mathcal{G}(\overline{\mathbb{Q}})$ is (co-)induced by the $\Gamma_{\mathbb{Q}(\zeta_3)}$ -module $\overline{\mathbb{Q}}^\times$.

Solution. Let $\tau \in \Gamma_{\mathbb{Q}}$ and $a \in \mathbb{Q}(\zeta_3), b \in \overline{\mathbb{Q}}$. By definition of the variety \mathcal{G} , $\Gamma_{\mathbb{Q}}$ acts on the second factor: $\tau(a \otimes b) = a \otimes \tau(b)$. Let $\rho \in \Gamma_{\mathbb{Q}}$ be an arbitrary lift of $\sigma_2 \in \text{Gal}(\mathbb{Q}(\zeta_3)|\mathbb{Q})$. It follows that the map $\mathbb{Q}(\zeta_3) \otimes_{\mathbb{Q}} \overline{\mathbb{Q}} \rightarrow \mathbb{Q}[\Gamma_{\mathbb{Q}}] \otimes_{\mathbb{Q}[\Gamma_{\mathbb{Q}(\zeta_3)}]} \overline{\mathbb{Q}} = \text{Ind}_{\Gamma_{\mathbb{Q}(\zeta_3)}}^{\overline{\mathbb{Q}}} \overline{\mathbb{Q}}$ given by $a \otimes b \mapsto e \otimes ab + \rho \otimes a\rho^{-1}(b)$ is a Γ_K -equivariant isomorphism of \mathbb{Q} -algebras. \square

- d) Show that $H^1(\overline{\mathbb{Q}}|\mathbb{Q}, \mathcal{G}(\overline{\mathbb{Q}})) = 1$. (Hint: Shapiro's lemma.)

Solution. By Shapiro's lemma and Hilbert 90,

$$H^1(\overline{\mathbb{Q}}|\mathbb{Q}, \mathcal{G}(\overline{\mathbb{Q}})) = H^1(\overline{\mathbb{Q}}|\mathbb{Q}(\zeta_3), \overline{\mathbb{Q}}^\times) = 1. \quad \square$$

- e) Show that there is a bijection between the set of C_3 -extensions of \mathbb{Q} and the quotient group $\varphi(\mathbb{Q}(\zeta_3)^\times) \backslash \mathbb{Q}(\zeta_3)^\times$.

Solution. Just like Kummer theory, this now follows from b), d), the cohomology long exact sequence induced by the short exact sequence

$$0 \rightarrow C_3 \rightarrow \mathcal{G}(\overline{\mathbb{Q}}) \xrightarrow{\varphi} \mathcal{G}(\overline{\mathbb{Q}}) \rightarrow 0,$$

and the fact that C_3 -extensions of \mathbb{Q} are in bijection with continuous homomorphisms $\Gamma_{\mathbb{Q}} \rightarrow C_3$. \square

Definition. If A and B are two finite groups with an action of B on A , we denote by $A \rtimes B$ their semidirect product: The group of pairs (a, b) with $a \in A$ and $b \in B$ with multiplication given by $(a, b)(a', b') = (a(ba'), bb')$.

Let G and H be finite groups and let I be a finite set with a left action of G . This induces a (permutation) action of G on $\prod_{i \in I} H$ given by $g(h_i)_{i \in I} = (h_{g^{-1}i})_{i \in I}$. The *wreath product* $H \wr_I G$ is the resulting semidirect product $(\prod_{i \in I} H) \rtimes G$ of order $|H|^{|I|} \cdot |G|$. Note that $H \wr_I G$ acts on $H \times G$ by $((h_i)_{i \in I}, g) \cdot (h', g') = (h_{gg'}h', gg')$. The stabilizer of $(\text{id}, \text{id}) \in H \times G$ is the subgroup $\{(h_i)_{i \in I}, g \mid h_{\text{id}} = \text{id}, g = \text{id}\} \cong \prod_{g \neq \text{id}} H$. A subgroup U of $H \wr_I G$ is called *transitive* if the resulting action of U on $H \times G$ is transitive. (I erroneously wrote down a weaker condition in class.)

Problem 3. Let $L|K$ be a finite Galois extension with Galois group G and let $M|L$ be a finite Galois extension with Galois group H . Let N be the Galois closure of $M|K$. Consider the wreath product $H \wr G = H \wr_G G$. Lift (extend) every element g of $G = \text{Gal}(L|K)$ to an element τ_g of $\text{Gal}(N|K)$. Construct a map $\varphi : \text{Gal}(N|K) \rightarrow H \wr G$ by letting

$$\varphi(\sigma) = ((\tau_{g'^{-1}} \sigma \tau_{g'^{-1}g}^{-1} | M)_{g' \in G}, g)$$

where $g = \sigma|_L$.

a) Show that φ is a well-defined group homomorphism.

Solution. By definition, $\tau_{g'^{-1}} \sigma \tau_{g'^{-1}g}^{-1} |_L = g'^{-1}g(g'^{-1}g)^{-1} = \text{id}_L$, so $\tau_{g'^{-1}} \sigma \tau_{g'^{-1}g}^{-1} |_M$ is an element of $H = \text{Gal}(M|L)$. Hence, φ is a well-defined map. To show that φ is a homomorphism, let $\sigma_1, \sigma_2 \in \text{Gal}(N|K)$

and let $g_1 = \sigma_1|_L$ and $g_2 = \sigma_2|_L$, so $g_1g_2 = \sigma_1\sigma_2|_L$. Then,

$$\begin{aligned}
\varphi(\sigma_1)\varphi(\sigma_2) &= ((\tau_{g'^{-1}}\sigma_1\tau_{g'^{-1}g_1}^{-1}|_M)_{g' \in G}, g_1)((\tau_{g'^{-1}}\sigma_2\tau_{g'^{-1}g_2}^{-1}|_M)_{g' \in G}, g_2) \\
&= ((\tau_{g'^{-1}}\sigma_1\tau_{g'^{-1}g_1}^{-1}|_M)_{g' \in G}(\tau_{(g_1^{-1}g')^{-1}}\sigma_2\tau_{(g_1^{-1}g')^{-1}g_2}^{-1}|_M)_{g' \in G}, g_1g_2) \\
&= ((\tau_{g'^{-1}}\sigma_1\tau_{g'^{-1}g_1}^{-1}\tau_{(g_1^{-1}g')^{-1}}\sigma_2\tau_{(g_1^{-1}g')^{-1}g_2}^{-1}|_M)_{g' \in G}, g_1g_2) \\
&= ((\tau_{g'^{-1}}\sigma_1\tau_{g'^{-1}g_1}^{-1}\tau_{g'^{-1}g_1}\sigma_2\tau_{g'^{-1}g_1g_2}^{-1}|_M)_{g' \in G}, g_1g_2) \\
&= ((\tau_{g'^{-1}}\sigma_1\sigma_2\tau_{g'^{-1}g_1g_2}^{-1}|_M)_{g' \in G}, g_1g_2) \\
&= \varphi(\sigma_1\sigma_2). \quad \square
\end{aligned}$$

b) Show that L is the fixed field of $\varphi^{-1}(\prod_{g \in G} H) \subset \text{Gal}(N|K)$.

Solution. Of course, $\varphi(\sigma) \in \prod_{g \in G} H$ if and only if $g = \sigma|_L = \text{id}_L$, which is equivalent to $\sigma \in \text{Gal}(N|L)$. \square

c) Show that M is the fixed field of $\varphi^{-1}(T)$, where $T \cong \prod_{g \neq \text{id}} H$ is the stabilizer of $(\text{id}, \text{id}) \in H \times G$ for the action of $H \wr G$ on $H \times G$ defined above.

Solution. We have $\varphi(\sigma) \in T$ if and only if $g = \sigma|_L = \text{id}_L$ and furthermore $\tau_{\text{id}_L}\sigma\tau_{\text{id}_L}^{-1}|_M = \text{id}_M$, so $\tau_{\text{id}_L}\sigma\tau_{\text{id}_L}^{-1}|_M = \text{id}_M$. Since $\tau_{\text{id}_L}|_L = \text{id}_L$, the map $\tau_{\text{id}_L}|_M$ is an automorphism of M . It follows that $\varphi(\sigma) \in T$ if and only if $\sigma|_M = \text{id}_M$, which is equivalent to $\sigma \in \text{Gal}(N|M)$. \square

d) Show that φ is injective.

Solution. By c), the field M is certainly fixed by the kernel of φ , which is a normal subgroup of $\text{Gal}(N|K)$. Let N' be the subfield of N fixed by the kernel. It is a Galois extension of K containing M . As N is the Galois closure of $M|K$, we must have $N' = N$, so the kernel of φ is trivial. \square

e) Show that the image of φ is a transitive subgroup of $H \wr G$.

Solution. Let R be the image of φ . By c) and d), we have $R \cong \text{Gal}(N|K)$ and $R \cap T \cong \varphi^{-1}(T) \cong \text{Gal}(N|M)$, so $[R : R \cap T] = [\text{Gal}(N|K) : \text{Gal}(N|M)] = [M : K] = |H| \cdot |G|$. The stabilizer of $(\text{id}, \text{id}) \in H \times G$ under the action of $R \subseteq H \wr G$ is $R \cap T$. Therefore, the orbit has size $[R : R \cap T] = |H| \cdot |G|$, so the action is indeed transitive. \square

- f) Show that another homomorphism $\varphi' : \text{Gal}(N|K) \rightarrow H \wr G$ is the homomorphism resulting from a different choice of $(\tau'_g)_{g \in G}$ as above if and only if there is an element a of $\prod_{g \in G} H$ such that $\varphi'(\sigma) = a\varphi(\sigma)a^{-1}$ for all $\sigma \in \text{Gal}(N|K)$. (“ φ is unique up to conjugation by elements of $\prod_{g \in G} H \subset H \wr G$.”)

Solution. Since $\tau'_g = \tau_g$, we can write $\tau'_g = s_g \tau_g$ for some $s_g \in \text{Gal}(N|L)$. Let $a_g = s_{g^{-1}}|_M$ and $a = (a_g)_{g \in G} \in \prod_{g \in G} H$. It then follows that $\varphi'(\sigma) = a\varphi(\sigma)a^{-1}$ for all $\sigma \in \text{Gal}(N|K)$.

Conversely, for any $a = (a_g)_{g \in G} \in \prod_{g \in G} H$, we can choose a lift $s_g \in \text{Gal}(N|L)$ of $a_{g^{-1}}$ and then let $\tau'_g = s_g \tau_g$. \square

Problem 4. Let p be an odd prime. Write $C_2 = \{\text{id}, \sigma\}$ and $C_p = \langle \tau \rangle$ and write elements of $\prod_{g \in C_2} C_p$ as pairs $(a_{\text{id}}, a_\sigma)$. Show that the following are the only transitive subgroups of $C_p \wr C_2$ up to conjugation by elements of $\prod_{g \in C_2} C_p$:

- i) The entire group $C_p \wr C_2$.
- ii) The subgroup of elements of the form $((a, a), b)$ with $a \in C_p$ and $b \in C_2$, which is isomorphic to the cyclic group C_{2p} of order $2p$.
- iii) The subgroup of elements of the form $((a, a^{-1}), b)$ with $a \in C_p$ and $b \in C_2$, which is isomorphic to the dihedral group D_p of order $2p$.

Solution. It is easy to verify that the three subgroups given are indeed transitive subgroups. The group in ii) is the cyclic group generated by $((\tau, \tau), \sigma)$. In iii), $((\tau, \tau^{-1}), \text{id})$ corresponds to a rotation and $((\text{id}, \text{id}), \sigma)$ corresponds to a reflection in D_p .

Let G be a transitive subgroup of $C_p \wr C_2$. We interpret the subgroup $N = \prod_{h \in C_2} C_p$ as the two-dimensional \mathbb{F}_p -vector space \mathbb{F}_p^2 . The element σ of C_2 acts on N as the reflection $r : \mathbb{F}_p^2 \rightarrow \mathbb{F}_p^2, (x, y) \mapsto (y, x)$. The intersection $V = G \cap N$ must be a vector subspace. The set W of vectors $w \in \mathbb{F}_p^2$ such that $(w, \sigma) \in G$ is a translate of V : It is nonempty by transitivity. If $v \in V$ and $w \in W$, then $(v + w, \sigma) = (v, \text{id})(w, \sigma) \in G$, so $vw \in W$. If $w_1, w_2 \in W$, then $(w_1 - w_2, \text{id}) = (w_1, \sigma)(w_2, \sigma)^{-1} \in G$.

If $V = \mathbb{F}_p^2$, then $G = C_p \wr C_2$. If $V = 1$, then G cannot be a transitive subgroup of G . Hence, let us assume that V is a line in \mathbb{F}_p^2 . The line V must be invariant under the reflection r : For any $v \in V$ and $w \in W$, we have $(r(v), \text{id}) = (w, \sigma)(v, \text{id})(w, \sigma)^{-1} \in G$, so $r(v) \in V$.

Hence, V must be either the line spanned by $(1, 1)$ or the line spanned by $(1, -1)$.

Assume $V = \langle(1, 1)\rangle$ and $W = \langle(1, 1)\rangle + (a, b)$. Conjugating the subgroup G by $(\frac{a-b}{2}, 0) \in N$, we may assume $a = b = 0$, giving rise to the subgroup in ii).

On the other hand, if $V = \langle(1, -1)\rangle$ and $W = \langle(1, -1)\rangle + (a, b)$, it follows that $((a+b, a+b), \text{id}) = ((a, b), \sigma)((a, b), \sigma) \in G$, so $(a+b, a+b) \in \langle(1, -1)\rangle$, which implies that $a = -b$, so $(a, b) \in \langle(1, -1)\rangle$. Hence, $W = \langle(1, -1)\rangle$, giving rise to the subgroup in iii). \square

Problem 5 (Roughly [Klü06]). Fix a prime number $p \neq 2$.

- a) Let K be a quadratic field extension of \mathbb{Q} . Show that if L is an unramified Galois extension of K with Galois group C_p , then L is a Galois extension of \mathbb{Q} with Galois group D_p (as in Problem 4iii).
- b) Assuming MCS, show that the number of Galois extensions L of \mathbb{Q} with Galois group D_p such that $L|K$ is unramified, where K is the subfield fixed by the group C_p of rotations in D_p , and $|D_K| \leq T$ is $\sim C \cdot T$ for $T \rightarrow \infty$ and some constant $C \geq 0$.
- c) Order the quadratic number fields K by $|D_K|$. Conclude that (assuming MCS), the expected size of the p -torsion subgroup of the class group of a random quadratic number field K is $C + 1$. (Hint: Look at the Hilbert class field of K .)

Remark. The *Cohen–Lenstra heuristics* predict that $C = \frac{p+1}{2p}$. (This is currently only known for $p = 3$, using the fact that $D_3 = S_3$ and our nice parametrization of cubic extensions! The average size is $1 + 1$ for imaginary quadratic number fields and $p^{-1} + 1$ for real quadratic number fields.) In fact, they predict with what probability the p -Sylow subgroup of $\text{Cl}(K)$ is a given fixed p -group.

Problem 6 (Counterexample to Malle’s conjecture, see [Klü05]). a) Let L be a Galois extension of $K = \mathbb{Q}(\zeta_3)$ with Galois group C_3 . Let M be the Galois closure of $L|\mathbb{Q}$. Show that one of the following is true:

- i) The Galois group is $\text{Gal}(M|\mathbb{Q}) \cong C_3 \wr C_2$ and we have

$$\text{Nm disc}(L|\mathbb{Q}(\zeta_3)) = |\text{disc}(M^H)|,$$

where $H \subset C_3 \wr C_2$ is the stabilizer of $(\text{id}, \text{id}) \in C_3 \times C_2$.

ii) The Galois group is $\text{Gal}(M|\mathbb{Q}) \cong C_6$ and $M = L$ and

$$\text{Nm disc}(L|\mathbb{Q}(\zeta_3)) \asymp |\text{disc}(M)|.$$

iii) The Galois group is $\text{Gal}(M|\mathbb{Q}) \cong S_3$ and $M = L$ and

$$\text{Nm disc}(L|\mathbb{Q}(\zeta_3)) \asymp |\text{disc}(M)|.$$

b) Assuming MCS, show:

i) The number of Galois extensions M of \mathbb{Q} with $\text{Gal}(M|\mathbb{Q}) \cong C_3 \wr C_2$ and $|\text{disc}(M^H)| \leq T$ is $\asymp X^{1/2}$.

ii) The number of Galois extensions M of \mathbb{Q} with $\text{Gal}(M|\mathbb{Q}) \cong C_6$ and $|\text{disc}(M)| \leq T$ is $\asymp X^{1/3}$.

iii) The number of Galois extensions M of \mathbb{Q} with $\text{Gal}(M|\mathbb{Q}) \cong S_3$ and $|\text{disc}(M)| \leq T$ is $\asymp X^{1/3}$.

c) Assuming MCS, show that the number of Galois extensions L of $\mathbb{Q}(\zeta_3)$ with $\text{Gal}(L|\mathbb{Q}(\zeta_3)) \cong C_3$ and $\text{Nm disc}(L|\mathbb{Q}(\zeta_3)) \leq T$ is $\asymp X^{1/2} \log X$.

d) Conclude that MCS is false in one of the four cases used above. (In fact, it turns out that i is wrong and ii, iii, c are correct.)

References

- [Klü05] Jürgen Klüners. “A counterexample to Malle’s conjecture on the asymptotics of discriminants”. In: *C. R. Math. Acad. Sci. Paris* 340.6 (2005), pp. 411–414. ISSN: 1631-073X. DOI: 10.1016/j.crma.2005.02.010. URL: <https://doi.org/10.1016/j.crma.2005.02.010>.
- [Klü06] Jürgen Klüners. “Asymptotics of number fields and the Cohen-Lenstra heuristics”. In: *J. Théor. Nombres Bordeaux* 18.3 (2006), pp. 607–615. ISSN: 1246-7405. URL: http://jtnb.cedram.org/item?id=JTNB_2006__18_3_607_0.