Student seminar solutions Week 4

1. *Review the concepts introduced in the lecture by consulting the Jupyter Notebook uploaded on Moodle (you can open it, for example, with CoCalc). The notebook summarizes the key notions from the lecture and demonstrates how they can be computed using SageMath. Run all code cells to observe how the computations are carried out. Experiment by modifying the examples (e.g., changing input values) to strengthen your understanding of the concepts and see how the results change.*

   Done by yourself.

2. (a) *Let χ and ψ be primitive characters. Show that if $(f_\chi, f_\psi) = 1$, then $f_{\chi\psi} = f_\chi f_\psi$. Find a counterexample in the case where $(f_\chi, f_\psi) \neq 1$.*

   By definition, the Dirichlet character product $\chi\psi$ is the primitive character inducing

   $$(\chi\psi)^{\text{pre}} : \left(\mathbb{Z}\Big/ f_\chi f_\psi \mathbb{Z}\right)^\times \to \mathbb{C}^\times : a \mapsto \chi(a)\psi(a).$$

   Since the conductors f_χ and f_ψ are coprime, there is an isomorphism

   $$\left(\mathbb{Z}\Big/ f_\chi f_\psi \mathbb{Z}\right)^\times \cong (\mathbb{Z}/f_\chi\mathbb{Z})^\times \times (\mathbb{Z}/f_\psi\mathbb{Z})^\times.$$

   Under this isomorphism, we can identify χ as $(\chi_m, 1)$ and ψ as $(1, \psi_n)$. Hence, η correspond to (χ_m, ψ_n) and we want to show η is primitive (implying $f_\chi f_\psi = f_{\chi\psi}$). Suppose $\chi\psi$ is a character of modulus $d < mn$ with $d = d_1 d_2$, $d_1 | m$, $d_2 | n$ and $(d_1, d_2) = 1$. We must have

   $$\chi\psi(a, 1) = \chi_m(a)\psi_n(1) = \chi_m(a) = 1, \quad \forall a \equiv 1 \mod d_1$$

   $$\text{similarly, } \psi_n(b) = 1, \quad \forall b \equiv 1 \mod d_2$$

   This directly means χ (resp. ψ) is induced by a character modulo d_1, (resp. d_2). By primality of χ and ψ, we must have $d_1 = m$ and $d_2 = n$, contradicting $d_1 d_2 < mn$.

   A counterexample where $(f_\chi, f_\psi) \neq 1$ occurs for

   $$\chi = \psi : (\mathbb{Z}/3\mathbb{Z})^\times \to \mathbb{C}^\times : \quad 1 \mapsto 1; \quad 2 \mapsto -1$$

   Then,

   $$\eta : (\mathbb{Z}/9\mathbb{Z})^\times \to \mathbb{C}^\times : a \mapsto \chi(a)\psi(a)$$

   is the principal character. Thus, $f_{\chi\psi} = 1$ while $f_\chi f_\psi = 9$.

(b) *Show that the set of all even Dirichlet characters is a subgroup of the group of all Dirichlet characters.*

Let χ and ψ be even Dirichlet characters (EDC). We check the requirements one by one:

i. $(\chi\chi^{-1})(-1) = \chi(-1)\chi^{-1}(-1) = 1 \Rightarrow \chi^{-1}(-1) = 1$..

ii. $(\chi\psi)(-1) = \chi(-1)\psi(-1) = 1$.

iii. $\chi_0(-1) = 1$.

3. *Let $p > 2$ be a prime and let $n > 0$ be an integer. Calculate the absolute discriminant of $\mathbb{Q}(\zeta_{p^n})$. Hint: Use the Conductor Discriminant Formula*

Let $K = \mathbb{Q}(\zeta_{p^n})$ and $G = \mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/p^n\mathbb{Z})^\times$ which is a cyclic group of order $\varphi(p^n) = p^{n-1}(p-1)$. To use the Conductor Discriminant Formula as hinted, we need to find the number of pairs of complex embeddings of K. First, $p^n \neq 2$, so there are no real embeddings. This means the total number of complex embeddings is the number of embeddings which is $\varphi(p^n)$. So the number of pairs of complex embeddings r_2 is

$$r_2 = \frac{p^{n-1}(p-1)}{2}.$$

Since what is taken into account in the Conductor Discriminant Formula is the parity of r_2, we will use the congruence $r_2 \equiv \frac{p-1}{2} \mod 2$.
Now, we want to be able to compute the products of conductors $\prod_\chi f_\chi$ running over all primitive characters of G. Observe that the characters of $(\mathbb{Z}/p^k\mathbb{Z})^\times$ embed into characters of $(\mathbb{Z}/p^{k+1}\mathbb{Z})^\times$: this way, we have $a_{k+1} := \varphi(k+1) - \varphi(k)$ primitive characters of modulus p^{k+1}. Hence, we obtain

$$\prod_\chi f_\chi = \prod_{k=1}^{n} (p^k)^{a_k} = p^{\sum_{k=1}^n k a_k} = p^{\sum_{k=1}^n k\varphi(p^k) - \sum_{k=1}^n k\varphi(p^{k-1})}$$

The sum S in the exponent can be easily worked out through telescopy to obtain

$$S = n\varphi(p^n) + p^{n-1} = p^{n-1}(n(p-1)+1)$$

So, using the Conductor Discriminant Formula:

$$d_K = (-1)^{(p-1)/2} p^{p^n(n(p-1)-1)}.$$

4. *Let X_1 and X_2 be the group of Dirichlet characters corresponding to the fields L_1 and L_2, respectively. Show that:*

(a) *The group generated by X_1 and X_2 corresponds to the compositum L_1L_2.*

Let $K = \mathbb{Q}(\zeta_m)$ be a field containing both L_1 and L_2 (we can use the Kronecker-Weber

Theorem) and let $G = \mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$. By the correspondence seen in class, the compositum L_1L_2 corresponds to

$$K^H, \quad H = \bigcap_{\chi \in X_1, X_2} \ker \chi = H_1 \cap H_2$$

for $H_i = \bigcap_{\chi \in X_i} \ker \chi$. Hence, $K^H = K^{H_1 \cap H_2} = L_1L_2$ by Galois theory (since fixing L_1L_2 is equivalent to fixing both L_1 and L_2).

(b) *The group $X_1 \cap X_2$ corresponds to $L_1 \cap L_2$.*

Using Galois theory again, this follows from the isomorphism

$$\mathrm{Gal}(K/L_1 \cap L_2) \cong H_1H_2.$$

Indeed, this implies that $L_1 \cap L_2$ correspond to

$$(H_1H_2)^\perp \cong H_1^\perp \cap H_2^\perp = X_1 \cap X_2.$$

5. *In this exercise we study quadratic Dirichlet characters and their associated fields.*

(a) *Let m be an odd positive integer. How many quadratic Dirichlet characters modulo m are there? How many of them are primitive?*
Hint: Consider the decomposition of a quadratic character. What is the group structure of $(\mathbb{Z}/p^a\mathbb{Z})^\times$?

Since m is odd, it decomposes as $m = \prod_{i \in I} p_i^{a_i}$ uniquely, for p_i odd primes. As

$$(\mathbb{Z}/m\mathbb{Z})^\times \cong \left(\mathbb{Z}/\prod_{i \in I} p_i^{a_i}\mathbb{Z}\right)^\times \overset{\text{CRT}}{\cong} \prod_{i \in I} \left(\mathbb{Z}/p_i^{a_i}\mathbb{Z}\right)^\times,$$

we obtain that a quadratic character χ modulo m is the same as a product of quadratic characters $(\chi_i)_{i \in I}$, each modulo $p_i^{a_i}$. Since each factor $(\mathbb{Z}/p_i^{a_i}\mathbb{Z})^\times$ is cyclic of order $p_i^{a_i-1}(p_i-1)$, which is an even number, we conclude that both $k \mapsto 1$ and $k \mapsto -1$ engender valid quadratic characters, for k a generator. This means that for each prime p_i, there are two quadratic characters modulo $p_i^{a_i}$ (one of which is trivial), so that the total number of quadratic characters modulo m is $2^{|I|}$.
χ is primitive if and only all the χ_i are primitive. Observe that the group of squares in a cyclic group of even order $(\mathbb{Z}/p_i^{a_i}\mathbb{Z})^\times$ has index 2 and already appears modulo p. In other words, let π be the reduction modulo p. Then, if $a_i > 1$, we have a non-trivial quadratic Dirichlet character modulo p, inducing the χ_i if non-trivial:

$$\left(\frac{\bullet}{p}\right) : (\mathbb{Z}/p_i\mathbb{Z}) \to \mathbb{C}^\times.$$

We conclude that

$$\#\{\text{primitive, quadratic } \chi \mod m\} = \begin{cases} 1 & a_i = 1, \forall i \in I \quad (m \text{ is squarefree}) \\ 0 & \text{else} \end{cases}$$

(b) *What does your answer to part (a) tell you about the quadratic subfield(s) of $\mathbb{Q}(\zeta_p)$, where p is an odd prime? Does a quadratic subfield always exist? Is it unique? When is it real? Calculate the quadratic subfield(s) and the discriminant(s).*
Hint: Is the quadratic character even/odd? Use the conductor discriminant formula and [Sh2, Ex4].

Preliminary Observation: We know that any quadratic subfield corresponds uniquely to some Dirichlet subgroup $X \leq \widehat{G}$. It happens precisely when $|X| = 2 \iff X = \{\chi_0, \chi\}$ for χ non-trivial, quadratic and primitive ($|X| = 2$ since the correspondence preserves the order). If not primitive, two characters could define the same fields, so we should reduce them modulo their conductor and then apply this procedure. Since L is a quadratic subfield, we can write $L = \mathbb{Q}(\sqrt{d})$ for some $d \in \mathbb{Z}$. By both Sheet 2, Exercise 4 and the conductor discriminant formula, we obtain

$$d_L = \begin{cases} d & d \equiv 1 \mod 4 \\ 4d & \text{else} \end{cases} = (-1)^{r_2} f_\chi$$

If f_χ is not divisible by 4, we directly deduce $|d| = f_\chi$. If it is, then $|d| = f_\chi/4$. To determine whether d is positive or negative, we evaluate χ at -1, since -1 corresponds to complex conjugation $\zeta_p \to \zeta_p^{-1}$. $\chi(-1) = 1$ means complex conjugation on L is trivial, i.e. L is real ($d > 0$). On the other hand, non-trivial complex conjugation on L means it is complex ($d < 0$).

Now, we can return to our original questions and answer them. By part (a), we know that there is one and only one unique non-trivial quadratic Dirichlet character of module p (determined by sending a generator to -1) which also turns out to be primitive and which we have seen, is $(\frac{\bullet}{p})$. Using the quadratic reciprocity, we directly have $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$. Therefore, by applying our **observation** above, we directly deduce that $L = \mathbb{Q}(\sqrt{p^*})$ and $d_L = p^*$ where $p^* = (-1)^{\frac{p-1}{2}} p$.

(c) *Let p be an odd prime. How many quadratic Dirichlet characters modulo $4p$ are there? How many of them are primitive? What does this tell you about the quadratic subfield(s) of $\mathbb{Q}(\zeta_{4p})$, where p is an odd prime? Calculate all quadratic subfield(s).*

By part (a), there are $2^2 = 4$ Dirichlet characters modulo $4p$ among which only 1 is primitive (not 0, because $(\mathbb{Z}/4\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z}$ contains a non-trivial quadratic primitive character modulo 4). Let $L = \mathbb{Q}(\sqrt{d})$ be the corresponding quadratic subfield to this primitive character. Using the **observation** above, we deduce that $d = \pm 4p$. We want to evaluate the primitive Dirichlet character χ at -1 as before, to determine what the sign of $|d|$ is. As a primitive Dirichlet character modulo $4p$ decomposes as two primitive Dirichlet characters ψ, ω (ψ modulo 4, ω modulo p, which we have seen is $\omega = (\frac{\bullet}{p})$). One can easily verify that ψ has to be the character

sending -1 to -1. Together,

$$\chi(-1) = \psi(-1)\omega(-1) = (-1)^{\frac{p+1}{2}}.$$

So,

$$L = \mathbb{Q}(\sqrt{4p}) = \mathbb{Q}(\sqrt{p}) \iff p \equiv 3 \mod (4)$$

$$L = \mathbb{Q}(\sqrt{-4p}) = \mathbb{Q}(\sqrt{-p}) \iff p \equiv 1 \mod (4).$$

Now, let's consider the two cases where the characters are not primitive. With the same decomposition notation as above, they are determined by

$$\psi_1\omega_1, \quad \psi_1(-1) = -1, \quad \omega_1 \equiv 1$$

$$\psi_2\omega_2, \quad \psi_2 \equiv 1, \quad \omega_2 = \left(\frac{\bullet}{p}\right)$$

Their primitive reductions χ_1, χ_2 are of module 4, p respectively and are described by sending a generator of their respective domain group to -1. Write $L_1 = \mathbb{Q}(\sqrt{d_1})$, $L_2 = \mathbb{Q}(\sqrt{d_2})$ for their associated subfield. Continuing the procedure of the **observation** above, we directly obtain $d_1 = -1$ (the case $d_1 = 1$ yields a trivial extension, not quadratic) and $d_2 = p^*$.

(d) *Answer similar questions about the quadratic subfield(s) of* $\mathbb{Q}(\zeta_8)$.

Recall $(\mathbb{Z}/8\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. For any non-trivial Dirichlet quadratic character χ modulo 8, one can verify that the possibilities are

	χ_1	χ_2	χ_3
$1 \mapsto$	1	1	1
$3 \mapsto$	-1	-1	1
$5 \mapsto$	-1	1	-1
$7 \mapsto$	1	-1	-1

among which, χ_1 and χ_3 are the primitive ones and χ_2 is induced by the primitive

$$\chi_2' : (\mathbb{Z}/4\mathbb{Z})^\times \to \mathbb{C}^\times : -1 \mapsto -1.$$

Using the same **observation** as in part (b) and (c), we obtain the three correspond subfields $L_i = \mathbb{Q}(\sqrt{d_i})$ with $d_1 = 8$, $d_2 = -1$ and $d_2 = -8$. Therefore, the quadratic subfields of $\mathbb{Q}(\zeta_8)$ are

$$\mathbb{Q}(i), \quad \mathbb{Q}(\sqrt{\pm 8}) = \mathbb{Q}(\sqrt{\pm 2})$$

(e) *Conclude that for any odd prime* p, $\mathbb{Q}(\sqrt{p}) \subseteq \mathbb{Q}(\zeta_m)$ *for* $m = p$ *or* $4p$. *Use this to show (without Kronecker-Weber) given any integer* d, *there is some* m *such that* $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{Q}(\zeta_m)$.

By part (b), if $p \equiv 1 \mod (4)$, then $\mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\zeta_p)$, and by part (c), if $p \equiv 3 \mod (4)$, then $\mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\zeta_{4p})$. In fact, we thus always have $\mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\zeta_{4p})$ for any odd prime p.

This is also true for $p = 2$ since part (d) exhibits $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\zeta_8)$.

Now let d be any integer. We can assume it is squarefree: $d = p_1...p_r$. Then $\mathbb{Q}(\sqrt{d})$ embeds into the compositum $\mathbb{Q}(\zeta_{4p_1})...\mathbb{Q}(\zeta_{4p_r}) = \mathbb{Q}(\zeta_{4\prod_{i=1}^{r} p_i}) = \mathbb{Q}(\zeta_{4d})$ as wanted.