Student seminar solutions Week 2

1. (a) From the course, we know that $Z(\mathfrak{P}/\mathfrak{p}) \cong Gal(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$ and that the Frobenius element
$$\left(\frac{\mathfrak{P}}{K/F}\right) \in Z(\mathfrak{P}/\mathfrak{p}) \subset G$$
is the image by that isomorphism of the generator $\varphi_{\mathfrak{p}} \in Gal(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$ with
$$\varphi_{\mathfrak{p}}(x) = x^{N\mathfrak{p}} \quad \forall x \in \mathbb{F}_{\mathfrak{P}}$$
with $N\mathfrak{p} = |\mathbb{F}_{\mathfrak{p}}|$. From that definition and the fact that the elements of $Z(\mathfrak{P}/\mathfrak{p})$ send $\mathfrak{P}$ to itself, we directly get that
$$\left(\frac{\mathfrak{P}}{K/F}\right)(\alpha) \equiv \alpha^{N\mathfrak{p}} \pmod{\mathfrak{P}} \quad \forall \alpha \in \mathcal{O}_K.$$
To show unicity, we now let $\sigma \in G$ with
$$\sigma(\alpha) \equiv \alpha^{N\mathfrak{p}} \pmod{\mathfrak{P}} \quad \forall\, \alpha \in \mathcal{O}_K,$$
From that property, it is obvious that σ sends $\mathfrak{P}$ to itself, meaning i.p. that $\sigma \in Z(\mathfrak{P}/\mathfrak{p})$. Through the isomorphism $Z(\mathfrak{P}/\mathfrak{p}) \cong Gal(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$, we see that σ induces the same automorphism $\varphi_{\mathfrak{p}}$ on $\mathbb{F}_{\mathfrak{P}}$ as $\left(\frac{\mathfrak{P}}{K/F}\right)$, i.e.
$$\sigma = \left(\frac{\mathfrak{P}}{K/F}\right)$$

   (b) Let K/F be abelian, $F \subset L \subset K$ some intermediate extension, and $\mathfrak{p} \subset \mathcal{O}_F$ an unramified prime in K. Choose a prime $\mathfrak{P} \subset \mathcal{O}_K$ above $\mathfrak{p}$ and let $\mathfrak{P}_L = \mathfrak{P} \cap \mathcal{O}_L$.
   By definition $\left(\frac{\mathfrak{p}}{K/F}\right) \in \mathrm{Gal}(K/F)$ (which is independent of $\mathfrak{P}$ as seen in class) is the unique element inducing the map $x \mapsto x^{N\mathfrak{p}}$ on $\mathbb{F}_{\mathfrak{P}}$. Its restriction $\left(\frac{\mathfrak{p}}{K/F}\right)\Big|_L \in \mathrm{Gal}(L/F)$ stabilizes $\mathfrak{P}_L$ as it stabilizes $\mathfrak{P}$ and therefore induces an automorphism of the residue field $\mathbb{F}_{\mathfrak{P}_L} = \mathcal{O}_L/\mathfrak{P}_L$. But $\mathbb{F}_{\mathfrak{P}_L} \subset \mathbb{F}_{\mathfrak{P}}$ therefore the map $\left(\frac{\mathfrak{p}}{K/F}\right)\Big|_L$ with domain $\mathbb{F}_{\mathfrak{P}_L}$ is defined directly by what $\left(\frac{\mathfrak{p}}{K/F}\right)$ does on $\mathbb{F}_{\mathfrak{P}}$, i.e.
$$\left(\frac{\mathfrak{p}}{K/F}\right)\Big|_L(x) = \left(\frac{\mathfrak{p}}{K/F}\right)(x) = x^{N\mathfrak{p}},$$
for all $x \in \mathbb{F}_{\mathfrak{P}_L}$ so $\left(\frac{\mathfrak{p}}{K/F}\right)\Big|_L$ induces the map $x \mapsto x^{N\mathfrak{p}}$ on $\mathbb{F}_{\mathfrak{P}_L}$ which is exactly the map $\left(\frac{\mathfrak{p}}{L/F}\right)$.

2. (a) Let $K = \mathbb{Q}(\zeta_m),\ \zeta = \zeta_m,\ G = \mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^\times$.
Let a prime $\mathfrak{p}$ and a prime $\mathfrak{P}$ of $\mathcal{O}_K$ above $\mathfrak{p}$. For an element $x \in \mathcal{O}_K$ or O_F, denote by $\overline{x}$ its class in $\mathbb{F}_\mathfrak{P}$ or $\mathbb{F}_\mathfrak{p}$ respectively. Consider the inertia group

$$T := T(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in G : \sigma(x) \equiv x \mod \mathfrak{P} \quad \forall x \in \mathcal{O}_K\} \subset Z(\mathfrak{P}/\mathfrak{p})$$

i.e. the kernel of the natural surjection $\varphi : Z(\mathfrak{P}/\mathfrak{p}) \to \mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})$. We have the following equality for the ramification index: $e = |T|$. In particular, $\mathfrak{p}$ is ramified iff T is non-trivial.
Now note that each $\sigma \in G$ has the form $\sigma_a(\zeta) = \zeta^a$ for some $a \in (\mathbb{Z}/m\mathbb{Z})^\times$. Let $\sigma_a \in T$, then by definition

$$\varphi(\sigma_a) = Id_{\mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})}$$

In particular, this is equivalent to $\overline{\zeta^a} = \overline{\zeta}$ in $\mathbb{F}_\mathfrak{P}$

If $p \nmid m$, then by part (b) the reduction map on the set of m-th roots of unity is injective modulo $\mathfrak{P}$. Therefore $\overline{\zeta^a} = \overline{\zeta}$ implies $\zeta^a = \zeta$, hence $a \equiv 1 \pmod m$. Therefore $\sigma_a = \mathrm{id}$, so T is trivial and $\mathfrak{p}$ is unramified.

If $p \mid m$, write $m = p^r m'$ with $r \geq 1$ and $p \nmid m'$.
By the chinese remainder theorem we have

$$(\mathbb{Z}/m\mathbb{Z})^\times \simeq (\mathbb{Z}/p^r\mathbb{Z})^\times \times (\mathbb{Z}/m'\mathbb{Z})^\times.$$

Consider $a \in (\mathbb{Z}/m\mathbb{Z})^\times$ such that

$$a \equiv 1 \pmod{m'} \quad \text{but} \quad a \not\equiv 1 \pmod{p^r}.$$

Such an a exists since $(\mathbb{Z}/p^r\mathbb{Z})^\times$ contains nontrivial units. Then ζ^{a-1} is a p^r-th root of unity, in particular

$$\overline{\zeta^{a-1}} = 1 \quad \Rightarrow \quad \overline{\zeta^a} = \overline{\zeta}.$$

Therefore $\sigma_a \in T$. But since $a \not\equiv 1 \pmod m$, we have $\sigma_a \neq \mathrm{id}$, hence T is nontrivial and $\mathfrak{p}$ ramifies in K.

(b) Let $p \nmid m$ and $\mathfrak{P} \subset \mathcal{O}_K$ a prime above $\mathfrak{p} = p\mathbb{Z}$. Suppose $\zeta, \zeta' \in \mu_m := \{x \in K : x^m = 1\}$ satisfy

$$\overline{\zeta} = \overline{\zeta'} \quad \text{in } \mathbb{F}_\mathfrak{P}.$$

Note that $\overline{\zeta}^m = \overline{\zeta'}^m = 1$ in $\mathbb{F}_\mathfrak{P}$, i.e. the common reduction is a root of $X^m - 1$ over $\mathbb{F}_\mathfrak{P}$. Since $p \nmid m$ we have

$$\frac{d}{dX}(X^m - 1) = mX^{m-1} \not\equiv 0 \pmod p,$$

so the polynomial $X^m - 1$ is separable modulo p and therefore has exactly m distinct roots in $\overline{\mathbb{F}_\mathfrak{p}}$.

The elements of μ_m are m distinct roots of $X^m - 1$ in K, and their reductions (viewed in $\overline{\mathbb{F}_\mathfrak{P}}$) must therefore be m distinct roots of $X^m - 1$ as well. If two distinct m-th roots of unity in K had the same reduction, this would yield fewer than m distinct roots after reduction, contradicting separability. Hence no two distinct elements of μ_m can have the same reduction, and $\overline{\zeta} = \overline{\zeta'}$ implies $\zeta = \zeta'$.

(c) For $p \nmid m$, the Frobenius automorphism $\left(\frac{\mathfrak{P}}{K/F}\right)$ satisfies $\left(\frac{\mathfrak{P}}{K/F}\right)(\zeta) \equiv \zeta^p \ mod\ \mathfrak{P}$ for all $\zeta \in \mathcal{O}_K$ by 1(a). By 2(b), reduction modulo $\mathfrak{P}$ is injective on m-th roots of unity, hence $\left(\frac{\mathfrak{P}}{K/F}\right)(\zeta) = \zeta^p$. Identifying $\mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^\times$ via $\zeta \mapsto \zeta^a$, the Artin automorphism corresponds to $[p] \in (\mathbb{Z}/m\mathbb{Z})^\times$.

3. First, let us clarify the exercise statement. As seen in class, the absolute discriminant of $K = \mathbb{Q}(\zeta_p)$ is a module (ideal) in the principal ring $\mathbb{Z}$ with generator $d(v_1, \ldots, v_n)$ where $\{v_1, \ldots, v_n\}$ is any integral basis of $\mathcal{O}_K$ (a change in $\mathbb{Z}$-basis equates to multiplying by a matrix A with $det(A)^2 = 1$ hence all basis here have the same discriminant). Our goal rather than to compute the module d_K is to compute the discriminant of any integral basis of $\mathcal{O}_K$.

Let $n = [K : \mathbb{Q}] = p - 1$, and consider the integral basis $\{1, \zeta_p, \ldots, \zeta_p^{n-1}\}$ of $\mathcal{O}_K$. As seen in class, the discriminant of this basis is

$$d(1, \zeta_p, \ldots, \zeta_p^{n-1}) = \prod_{1 \le i < j \le n} (\sigma_i(\zeta_p) - \sigma_j(\zeta_p))^2,$$

where σ_k are the embeddings $K \hookrightarrow \mathbb{C}$ given by $\sigma_k(\zeta_p) = \zeta_p^k$. Hence,

$$d(1, \zeta_p, \ldots, \zeta_p^{n-1}) = \prod_{1 \le i < j \le n} (\zeta_p^i - \zeta_p^j)^2.$$

Factor ζ_p^i from each term: $\zeta_p^i - \zeta_p^j = \zeta_p^i(1 - \zeta_p^{j-i})$, so

$$\prod_{1 \le i < j \le n} (\zeta_p^i - \zeta_p^j)^2 = \left(\prod_{1 \le i < j \le n} \zeta_p^i \right)^2 \left(\prod_{1 \le i < j \le n} (1 - \zeta_p^{j-i}) \right)^2$$

Let us compute these products. For the first product:

$$\left(\prod_{1 \le i < j \le n} \zeta_p^i \right)^2 = \zeta_p^{2\sum_{1 \le i < j \le n} i} = \zeta_p^{2\sum_{i=1}^{n-1} i(n-i)} = \zeta_p^{\frac{n(n-1)(n+1)}{3}} = \zeta_p^{\frac{p(p-1)(p-2)}{3}}$$

If $p > 3$, then $\frac{(p-1)(p-2)}{3} \in \mathbb{Z}$ and $p | \frac{p(p-1)(p-2)}{3}$, meaning that $\left(\prod_{1 \le i < j \le n} \zeta_p^i \right)^2 = 1$.

For $p = 3$ then $\left(\prod_{1\le i<j\le n} \zeta_p^i\right)^2 = \zeta_3^2$.

For the second product, consider the pairs $1 \le i < j \le n$. For each $k = j - i$, the number of pairs with difference k is $n - k = p - 1 - k$, so

$$\left(\prod_{1\le i<j\le n} (1-\zeta_p^{j-i})\right)^2 = \left(\prod_{k=1}^{p-2}(1-\zeta_p^k)^{p-1-k}\right)^2 = (1-\zeta_p)^{2(p-2)}\left(\prod_{k=2}^{p-2}(1-\zeta_p^k)^{p-1-k}\right)^2$$

Using the equality $1 - \zeta_p^{p-k} = -\zeta_p^{-k}(1 - \zeta_p^k)$ and pairing k with $p - k$ for $k \in \{2, \dots, \frac{p-1}{2}\}$:

$$\begin{aligned}
&(1 - \zeta_p^k)^{2(p-1-k)}(1 - \zeta_p^{p-k})^{2(p-1-(p-k))} \\
&= (-1)^{2(k-1)}\zeta_p^{-2k(k-1)}(1 - \zeta_p^k)^{2(p-1-k)}(1 - \zeta_p^k)^{2(k-1)} \\
&= \zeta_p^{-2k(k-1)}(1 - \zeta_p^k)^{2(p-2)} \\
&= \zeta_p^{-2k(k-1)}\big(-\zeta_p^k(1 - \zeta_p^k)(1 - \zeta_p^{p-k})\big)^{p-2} \\
&= (-1)^{p-2}\zeta_p^{-2k^2}\big((1 - \zeta_p^k)(1 - \zeta_p^{p-k})\big)^{p-2}
\end{aligned}$$

Which allows us to write

$$\begin{aligned}
\left(\prod_{k=1}^{p-2}(1 - \zeta_p^k)^{p-1-k}\right)^2 &= (1 - \zeta_p)^{2(p-2)}\left(\prod_{k=2}^{(p-1)/2}(-1)^{p-2}\zeta_p^{-2k^2}\big((1 - \zeta_p^k)(1 - \zeta_p^{p-k})\big)^{p-2}\right) \\
&= (1 - \zeta_p)^{p-2}\left(\prod_{k=2}^{(p-1)/2}(-1)^{p-2}\zeta_p^{-2k^2}\right)\left(\prod_{k=1}^{p-2}(1 - \zeta_p^k)\right)^{p-2} \\
&= -\zeta_p^{p-2}(1 - \zeta_p^{p-1})^{p-2}\left(\prod_{k=2}^{(p-1)/2}(-1)^{p-2}\zeta_p^{-2k^2}\right)\left(\prod_{k=1}^{p-2}(1 - \zeta_p^k)\right)^{p-2} \\
&= \zeta_p^{-2}\left(\prod_{k=1}^{(p-1)/2}(-1)^{p-2}\right)\left(\prod_{k=2}^{(p-1)/2}\zeta_p^{-2k^2}\right)\left(\prod_{k=1}^{p-1}(1 - \zeta_p^k)\right)^{p-2} \\
&= \left(\prod_{k=1}^{(p-1)/2}(-1)\right)\left(\prod_{k=1}^{(p-1)/2}\zeta_p^{-2k^2}\right)\left(\prod_{k=1}^{p-1}(1 - \zeta_p^k)\right)^{p-2} \\
&= (-1)^{\frac{p-1}{2}}\zeta_p^{-\frac{p(p-1)(p+1)}{12}}\left(\prod_{k=1}^{p-1}(1 - \zeta_p^k)\right)^{p-2}
\end{aligned}$$

Differentiating the equality $X^p - 1 = (X - 1)\prod_{k=1}^{p-1}(X - \zeta_p^k)$ and evaluating at $X = 1$ gives $\prod_{k=1}^{p-1}(1 - \zeta_p^k) = p$. Hence

$$\left(\prod_{k=1}^{p-2}(1 - \zeta_p^k)^{p-1-k}\right)^2 = (-1)^{\frac{p-1}{2}}\zeta_p^{-\frac{p(p-1)(p+1)}{12}}p^{p-2}.$$

If $p > 3$, then $\frac{(p-1)(p+1)}{12} \in \mathbb{Z}$ hence $\zeta_p^{-\frac{p(p-1)(p+1)}{12}} = 1$.

For $p = 3$, $\zeta_p^{-\frac{p(p-1)(p+1)}{12}} = \zeta_3$. Remember the equality $\left(\prod_{1\leq i<j\leq n} \zeta_p^i\right)^2 = \zeta_3^2$ for $p = 3$, the multiplication of those terms gives us 1, and indeed for any odd prime p, we obtain

$$d(1, \zeta_p, \ldots, \zeta_p^{n-1}) = (-1)^{\frac{p-1}{2}} p^{p-2}.$$

4. (a) As in ex. 3, we are looking to compute the discriminant of an integral basis of $K = \mathbb{Q}(\sqrt{d})$. It is clear the the embeddings $\sigma : \mathbb{K} \hookrightarrow \overline{\mathbb{Q}}$ are entirely determined by the image of $\sqrt{d}$. In particular, the image $\sigma(\sqrt{d})$ must also be a zero of the quadratic polynomial $x^2 - d$. This implies that the unique non trivial embedding $\mathbb{K} \hookrightarrow \overline{\mathbb{Q}}$ sends $\sqrt{d}$ to $-\sqrt{d}$. Characterising these embeddings justifies the computations of d_K that we are about to do.

   If $d \equiv 1 \pmod 4$, then $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ with integral basis $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$. By definition, the discriminant is

$$d_K = \det \begin{pmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2} \end{pmatrix}^2 = d.$$

   If $d \equiv 2, 3 \pmod 4$, then $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ with integral basis $\{1, \sqrt{d}\}$. As justified above, the discriminant is

$$d_K = \det \begin{pmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{pmatrix}^2 = 4d.$$

   (b) Write $\mathfrak{p} = p\mathbb{Z}$ and let $\mathfrak{P} \subset \mathcal{O}_K$ be a prime lying above $\mathfrak{p}$. By definition, p being unramified in $K/\mathbb{Q}$ means $p \nmid d_K$. By part (a) it follows in particular that $p \nmid d$.

   By definition, the Frobenius element $\left(\frac{\mathfrak{p}}{K/\mathbb{Q}}\right) \in \mathrm{Gal}(K/\mathbb{Q})$ satisfies

$$\left(\frac{\mathfrak{p}}{K/\mathbb{Q}}\right)(\alpha) \equiv \alpha^p \pmod{\mathfrak{P}} \qquad \text{for all } \alpha \in \mathcal{O}_K.$$

   We apply this to $\alpha = \sqrt{d}$. Euler's criterion in the residue field $\mathbb{F}_{\mathfrak{P}}$ gives

$$\sqrt{d}^{\,p-1} = d^{\frac{p-1}{2}} \equiv \left(\frac{d}{p}\right) \pmod{\mathfrak{P}},$$

   so multiplying by $\sqrt{d}$ yields

$$\left(\frac{\mathfrak{p}}{K/\mathbb{Q}}\right)(\sqrt{d}) \equiv \left(\frac{d}{p}\right)\sqrt{d} \pmod{\mathfrak{P}}.$$

The reductions of $\sqrt{d}$ and $-\sqrt{d}$ are distinct: if $\sqrt{d} \equiv -\sqrt{d} \pmod{\mathfrak{P}}$ then $2\sqrt{d} \in \mathfrak{P}$, which cannot happen because p is odd and $p \nmid d$. Thus reduction modulo $\mathfrak{P}$ distinguishes the two galois images, so the congruence above implies the following equality for the Frobenius element

$$\left(\frac{\mathfrak{p}}{K/\mathbb{Q}}\right) = \left(\frac{d}{p}\right) \in \mathrm{Gal}(K/\mathbb{Q}) \cong \{\pm 1\}$$

Finally, since p is odd and $p \nmid d_K$, we have $(\frac{4}{p}) = 1$, so $(\frac{d_K}{p}) = (\frac{d}{p})$ and we get the desired result.