---

1. Let K/Q be an extension of the number field Q, L/K a finite extension, and $\mathfrak{p} \lhd \mathcal{O}_Q$ a non-zero prime ideal, $\mathfrak{P} \in \mathrm{Spec}_{\mathfrak{p}}(\mathcal{O}_K)$, and $\mathfrak{Q} \in \mathrm{Spec}(\mathcal{O}_L)$.
   a) Show that $\mathfrak{Q} \in \mathrm{Spec}_{\mathfrak{p}}(\mathcal{O}_L)$ if and only if $\mathfrak{Q} \cap \mathcal{O}_K \in \mathrm{Spec}_{\mathfrak{p}}(\mathcal{O}_K)$.
   b) Show that

$$e_{\mathfrak{Q}|\mathfrak{p}} = e_{\mathfrak{Q}|\mathfrak{P}} \cdot e_{\mathfrak{P}|\mathfrak{p}} \quad \text{and} \quad f_{\mathfrak{Q}|\mathfrak{p}} = f_{\mathfrak{Q}|\mathfrak{P}} \cdot f_{\mathfrak{P}|\mathfrak{p}}.$$

2. Let K/Q be an extension of number fields and let $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_Q)$ a non-zero prime unramified in K. Let $\mathfrak{P} \in \mathrm{Spec}_{\mathfrak{p}}(\mathcal{O}_K)$. Recall that the Frobenius element $\left(\frac{K/Q}{\mathfrak{P}}\right) \in D_{\mathfrak{P}}$ denotes the preimage of the Forbenius $\mathrm{frob}_{|k_{\mathfrak{p}}|} \in \mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}})$.
   a) Show that $\left(\frac{K/Q}{\mathfrak{P}}\right)$ is the unique element $\sigma \in D_{\mathfrak{P}}$ such that

$$\forall z \in \mathcal{O}_K \quad \sigma(z) = z^{|k_{\mathfrak{p}}|} \mod \mathfrak{P}.$$

   b) Let $\sigma \in \mathrm{Gal}(K/Q)$, show that

$$\sigma \circ \left(\frac{K/Q}{\mathfrak{P}}\right) \circ \sigma^{-1} = \left(\frac{K/Q}{\sigma(\mathfrak{P})}\right).$$

   c) Show that the set of Frobenius elements at primes above $\mathfrak{p}$ is a single conjugacy class in $\mathrm{Gal}(K/Q)$.
3. *The following exercise is an exercise in Galois Theory. If time is scarce, we encourage you to just use the results and focus on the other exercises instead.*

   Let K be a field, let $L_1, L_2 \subset \overline{K}$ be finite Galois extensions of K. Let L_1L_2 denote their composite field, i.e., L_1L_2 is the smallest subfield of $\overline{K}$ containing the union $L_1 \cup L_2$.
   a) Show that L_1L_2/K is Galois.
   b) Consider the map given by

$$\begin{aligned} \Psi\colon\ \mathrm{Gal}(L_1L_2/K) &\longrightarrow \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K), \\ \sigma &\longmapsto (\sigma|_{L_1}, \sigma|_{L_2}), \end{aligned}$$

   where $\sigma|_{L_i}$ denotes the restriction of σ to L_i. Show that Ψ is an injective group homomorphism.
   c) Show that the group homomorphism

$$\begin{aligned} \Phi\colon\ \mathrm{Gal}(L_1L_2/L_1) &\longrightarrow \mathrm{Gal}(L_2/L_1 \cap L_2), \\ \sigma &\longmapsto \sigma|_{L_2}, \end{aligned}.$$

   is a well defined isomorphism of groups.
   Hint: For surjectivity, show that the fixed field of $\mathrm{im}(\Phi)$ equals $L_1 \cap L_2$, i.e.,

$$\{x \in L_2 \colon \forall \sigma \in \mathrm{im}(\Phi)\, \sigma(x) = x\} = L_1 \cap L_2.$$

   d) Prove that if $L_1 \cap L_2 = K$, then Ψ is an isomorphism and hence

$$\mathrm{Gal}(L_1L_2/K) \cong \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K).$$

4. Let $L_1, L_2 \subset \overline{\mathbb{Q}}$ be finite Galois extensions of $\mathbb{Q}$ such that $L_1 \cap L_2 = \mathbb{Q}$. We denote $n_1 = [L_1 \colon \mathbb{Q}]$ and $n_2 = [L_2 \colon \mathbb{Q}]$. Furthermore, for $i = 1, 2$, let $\mathcal{O}_i$ be the ring of integers in L_i and
$$\left(z_1^{(i)}, \dots, z_{n_i}^{(i)}\right) \in \mathcal{O}_i^{n_i}$$
be $\mathbb{Z}$-bases of $\mathcal{O}_i$. Finally, set
$$d_i = \operatorname{disc}_{L_i/\mathbb{Q}}\left(z_1^{(i)}, \dots, z_{n_i}^{(i)}\right) \in \mathbb{Z},$$
and assume that d_1 and d_2 are relatively prime, i.e., $(d_1, d_2) = (1)$ as ideals in $\mathbb{Z}$.
   a) Show that L_1L_2 is a number field of degree n_1n_2.
   b) Let $\beta_1, \dots, \beta_{n_2} \in L_1$ be such that
   $$\alpha := \beta_1 z_1^{(2)} + \dots + \beta_{n_2} z_{n_2}^{(2)} \in \mathcal{O}_{L_1L_2}.$$
   Prove that the elements $d_2\beta_1, \dots, d_2\beta_{n_2}$ are integral.
   Hint: Let $\mathrm{Gal}(L_1L_2/L_1) = \{\sigma_1^{(2)}, \dots, \sigma_{n_2}^{(2)}\}$ and $T_2 = \left(\sigma_j^{(2)}(z_i)\right) \in \overline{\mathbb{Q}}^{n_2 \times n_2}$. Note that
   $$\left(\sigma_1^{(2)}(\alpha), \dots, \sigma_{n_2}^{(2)}(\alpha)\right) = (\beta_1, \dots, \beta_{n_2})T_2.$$
   c) Deduce that the tuple
   $$\mathcal{B} = \left(z_{j_1}^{(1)} z_{j_2}^{(2)} : 1 \leqslant j_i \leqslant n_i\right)$$
   forms a $\mathbb{Z}$-basis for the ring of integers in L_1L_2.
   Hint: $\mathcal{B}$ is a $\mathbb{Q}$-basis of L_1L_2.
   d) Prove that
   $$\operatorname{disc}_{L_1L_2/\mathbb{Q}}(\mathcal{B}) = {d_1}^{n_2} {d_2}^{n_1}.$$
   Hint: This is a rather long computation in rearranging the matrix defining the discriminant; cf. §3 of Lecture 4.
5. For each positive integer $n \geqslant 1$, let ζ_n be a primitive n-th root of unity. The aim of this exercise is to show that the ring of integers of the cyclotomic field $\mathbb{Q}(\zeta_n)$ is given by
$$\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n].$$
   a) Let $[n_1, n_2]$ denote the least common multiple of n_1 and n_2. Prove that
   $$\mathbb{Q}(\zeta_{n_1}, \zeta_{n_2}) = \mathbb{Q}(\zeta_{[n_1,n_2]}) \quad \text{and} \quad \mathbb{Z}[\zeta_{n_1}, \zeta_{n_2}] = \mathbb{Z}[\zeta_{[n_1,n_2]}].$$
   Hint: You can choose the roots ζ_1 and ζ_2 such that, for example,
   $${\zeta_{[n_1,n_2]}}^{\frac{n_2}{(n_1,n_2)}} = \zeta_{n_1},$$
   where (n_1, n_2) denotes the greatest common divisor of n_1 and n_2 respectively.
   b) Prove that $\mathbb{Q}(\zeta_{n_1}) \cap \mathbb{Q}(\zeta_{n_2}) = \mathbb{Q}(\zeta_{(n_1,n_2)})$.
   Hint: First, show that $\mathbb{Q}(\zeta_{(n_1,n_2)}) \subset \mathbb{Q}(\zeta_{n_1}) \cap \mathbb{Q}(\zeta_{n_2})$. Then use Exercise 3c together with $[\mathbb{Q}(\zeta_n) \colon \mathbb{Q}] = \phi(n)$ to show that
   $$[\mathbb{Q}(\zeta_{n_2}) \colon \mathbb{Q}(\zeta_{n_1}) \cap \mathbb{Q}(\zeta_{n_2})] = \frac{[\mathbb{Q}(\zeta_{[n_1,n_2]}) \colon \mathbb{Q}]}{[\mathbb{Q}(\zeta_{n_1}) \colon \mathbb{Q}]} = [\mathbb{Q}(\zeta_{n_2}) \colon \mathbb{Q}(\zeta_{(n_1,n_2)})].$$
   c) Conclude that $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$ and that all the divisors of the discriminant of $\mathcal{O}_{\mathbb{Q}(\zeta_n)}$ divide n.
   Hint: Use induction on the number of prime divisors of n.
   d) Prove that a non-zero prime $(p) \in \operatorname{Spec}(\mathbb{Z})$ is ramified in $\mathbb{Q}(\zeta_n)$ if and only if $p|n$.