Solutions to Sheet 8

Exercise 1

Let $K = \mathbb{Q}[\sqrt{7}, \sqrt{10}]$. The extension $K/\mathbb{Q}$ is Galois (the extension is normal since K is a splitting field of the polynomial $(T^2 - 7)(T^2 - 10) \in \mathbb{Q}[T]$).

1. Show that there exist pairwise distinct prime ideals $\mathfrak{P}_1, \dots \mathfrak{P}_4$ of $\mathcal{O}_K$ such that $3\mathcal{O}_K = \mathfrak{P}_1 \cdots \mathfrak{P}_4$. *Hint: Consider $D(\mathfrak{P}|3\mathbb{Z})$ for a prime ideal $\mathfrak{P}$ of $\mathcal{O}_K$ lying over 3.*
2. Deduce that $3 \mid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$ for every $\alpha \in \mathcal{O}_K$. In particular, $\mathcal{O}_K$ is not monogenic.

Solution.

1. As in the hint we will show that

$$D(\mathfrak{P}|3\mathbb{Z}) = \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) \mid \sigma(\mathfrak{P}) = \mathfrak{P}\} = \{1\}$$

for any prime ideal $\mathfrak{P} \subset \mathcal{O}_K$ dividing (3). This finishes the exercise, as we know from the lecture that $1 = \#D(\mathfrak{P}|3\mathbb{Z}) = e(\mathfrak{P}|3)f(\mathfrak{P}|3)$. Now (the very useful) Lemma 3.10 implies that

$$4 = [K : \mathbb{Q}] = \sum_{\mathfrak{P}|3\mathcal{O}_K} e(\mathfrak{P}|3\mathbb{Z})f(\mathfrak{P}|3\mathbb{Z}) = \sum_{\mathfrak{P}|3\mathcal{O}_K} 1.$$

Hence there are four distinct prime divisors of $3\mathcal{O}_K$.

The Galois group of L/K is given by $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, which acts by switching the sign of $\sqrt{7}$ and $\sqrt{10}$. Note that $(\sqrt{10}+1)(\sqrt{10}-1) = 9 \in \mathfrak{P}$ and $(\sqrt{7}+1)(\sqrt{7}-1) = 6 \in \mathfrak{P}$; in both cases we find that one of the factors must lie in $\mathfrak{P}$. If now σ switched the sign of $\sqrt{\alpha}$ for $\alpha \in \{7, 10\}$, we'd find that $(\sqrt{\alpha} \pm 1) + \sigma(\sqrt{\alpha} \pm 1) = \pm 2 \in \mathfrak{P}$. But we have $3 \in \mathfrak{P}$, so now we find $3 - 2 = 1 \in \mathfrak{P}$, Contradiction. So there cannot be non-trivial elements in $D(\mathfrak{P}|3)$.

2. Assume for sake of contradiction that $3 \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$ but $K = \mathbb{Q}(\alpha)$. Let $m_\alpha(X)$ be the minimal polynomial of α. Then theorem 3.11 yields

$$m_\alpha(X) \cong P_1(X)P_2(X)P_3(X)P_4(X)$$

for four distinct (irreducible) polynomials $P_i(X) \in \mathbb{F}_3[X]$ of degree $f(\mathfrak{P}|3) = 1$. But the only degree 1 polynomials in $\mathbb{F}_3[X]$ are $X, X-1, X-2$. Contradiction.

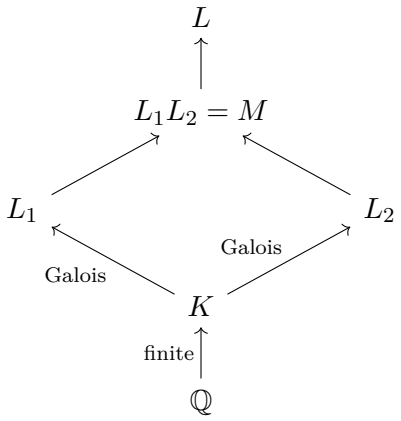
Exercise 2

Let K be a number field, let L/K be an algebraic extension, and let L_1 and L_2 be two subfields of L containing K such that the extensions L_1/K and L_2/K are Galois (in particular finite). Let M denote the compositum L_1L_2 of L_1 and L_2 inside L., i.e., the intersection of all subfields of L that contain $L_1 \cup L_2$. Let $\mathfrak{p}$ denote a non-zero prime ideal of $\mathcal{O}_K$.

1. Show that the extension M/K is Galois.
2. Show with an example that the implication "$\mathfrak{p}$ is totally ramified in both L_1/K and L_2/K, so $\mathfrak{p}$ is totally ramified in M/K" is false in general.

3. Show with an example that the implication "$\mathfrak{p}$ is inert in both L_1/K and L_2/K, so $\mathfrak{p}$ is inert in M/K" is false in general.

Solution. We are in the following situation:



1. For us, Galois means separable, finite and normal. Separability follows from the fact that every extension of fields in characteristic 0 is separable. For normality and finiteness, observe that L_1 and L_2 are the splitting fields of (finite) families of polynomials. But now L_1L_2 is the splitting field of the union of these families. Hence it is normal and finite.

2. Remember that a prime $\mathfrak{p} \subset \mathcal{O}_K$ is said to be totally ramified in M iff $\mathfrak{p}\mathcal{O}_M = \mathfrak{P}^{e(\mathfrak{P}|\mathfrak{p})}$ in $\mathcal{O}_M$, i.e., iff $e(\mathfrak{P}|\mathfrak{p}) = [M : K]$. Let's just try to create easy example of totally ramified prime ideals. Here remark 3.14 (ii) is of help. For the desired counterexample, set $L_1 = \mathbb{Q}(\sqrt{3})$ and $L_2 = \mathbb{Q}(\sqrt{-1})$. Now take the ideal $(2) \subset \mathbb{Z}$. One can also see that this is ramified in both extensions because $2 \mid \Delta_{L_i/\mathbb{Q}}$ this is theorem 3.22, and this can also quickly be verified using 3.11). Thereby it is automatically totally ramified, because $[L_i : \mathbb{Q}] = 2$. Now the composite field extension $L_1L_2 = M$ contains the field $L_1' = \mathbb{Q}[\sqrt{-3}]$, where (2) is inert (this is a routine consequence of 3.11). Now $[L_1' : M]$, and we find that for any prime $\mathfrak{P} \subset M$ above $(2) \subset \mathbb{Z}$,

$$e(\mathfrak{P}|2\mathbb{Z}) = e(\mathfrak{P}|2\mathcal{O}_{L_1'})e(2\mathcal{O}_{L_1'}|2\mathbb{Z}) \leq [M : L_1'] \cdot 1 = 2$$

. In particular, $e(\mathfrak{P}|2\mathbb{Z}) < 4$, so (2) cannot be totally ramified in M.

3. Same idea. Inert means that $f(\mathfrak{P}|\mathfrak{p}) = [L : K]$. This time, take $L_1 = \mathbb{Q}(\sqrt{5})$ and $L_2 = \mathbb{Q}(\sqrt{13})$, and the ideal (2) again, which is inert in both extensions (the discriminants are given by 5 and 13, respectively). Now the composite contains $\mathbb{Q}(\sqrt{65})$, which has discriminant 65. But $\left(\frac{65}{2}\right) = 1$, so it is ramified there. In particular it cannot be inert, because now for a prime ideal $\mathfrak{P}$ of $\mathcal{O}_M$ over (2) we have $e(\mathfrak{P}|2\mathbb{Z})f(\mathfrak{P}|2\mathbb{Z}) \leq [L : K]$ and $e(\mathfrak{P}|2\mathbb{Z}) \geq 2$.

Exercise 3

Let K be a number field. For $n \in \mathbb{N} = \{1, 2, 3, \dots\}$, set $a_n(K) = \#\{I \subset \mathcal{O}_K \mid \mathrm{N}(I) = n\}$. Let m, n be coprime natural numbers. Show that $a_{mn}(K) = a_m(K)a_n(K)$.

Solution. Define $A_n(K) = \{I \subset \mathcal{O}_K \mid \mathrm{N}(I) = n\}$. Then one can see that if $(n, m) = 1$,

$$A_n(K)A_m(K) = \{IJ \mid I \subset A_n(K), J \subset A_m(K)\} = A_{nm}(K).$$

Here we used again that Ideals decompose uniquely into prime factors, and that for any $I \in A_{nm}(K)$, the set of prime ideal factors of I that divide n and the set of prime ideal factors that divide m are disjoint.

Remark. In particular, this shows that it is enough to understand $a_n(K)$ for prime powers n. In analytic number theory, this has some nice consequences. There one can define the *Dedekind zeta function*

$$\zeta_K(s) = \sum_{n=1}^{\infty} a_n(K) n^{-s},$$

which can be shows to define a holomorphic function for $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$. This function has a meromorphic continuation to all of $\mathbb{C}$, and it encodes many invariants of the number field. For example, by the *analytic class number formula*, the residue of $\zeta_K(s)$ of the pole at $s = 1$ provides information about the class number of K. The multiplicativity of the coefficients relates directly to there being a *Euler product expansion*

$$\zeta_K(s) = \prod_{p \in \mathbb{N}} \left(1 + a_p(K) p^{-s} + a_{p^2}(K) p^{-2s} + \dots\right).$$

We will encounter the Dedekind zeta function in upcoming lectures.

Max von Consbruch, email: mvconsbruch@uni-bonn.de. Date: December 4, 2023