June 16th, 2016

Number Theory II

Prof. H. Esnault, Dr. V. Di Proietto

Exercise sheet 9[1]

Exercise 1. Let L, K be two fields both contained in a field Ω.

(i) Show that $L \cap K$ is again a field contained in Ω.

(ii) Deduce that there exists a field LK, called the *compositum* of L and K, defined as the smallest subfield of Ω containing both K and L. Does it coincide with the smallest *subring* of Ω containing both K and L?

(iii) Let F be any perfect field, and suppose that Ω is an algebraic closure of F and that both L and K are finite algebraic extensions of F. Prove that LK is again algebraic and that it coincides with the smallest subring of Ω containing both L and K.

(iv) Let F be any perfect field, and suppose that Ω is an algebraic closure of F and that both L and K are finite algebraic extensions of F. The field L is said to be *F-linearly disjoint* from K if every family $x_1, \dots, x_n$ of elements in L which are linearly independent over F are also linearly independent over K. Prove that being "linearly disjoint over F" is a symmetric relation, and that the following conditions are equivalent:
   (i) L and K are F-linearly disjoint
   (ii) $[LK : K] = [L : F]$
   (iii) $[LK : L] = [K : F]$
   (iv) $[LK : F] = [L : F] \cdot [K : F]$
   (*Hint: For the equivalences, consider the ring $K \otimes F$*).

(v) Provide an example of two number fields L_1, L_2 such that $L_1 \cap L_2 = \mathbb{Q}$ but L_1, L_2 are not linearly disjoint.
   Hint: Chose L_1, L_2 of degree 3 over $\mathbb{Q}$.

Exercise 2. Let L and K be two number fields, and suppose that they are linearly disjoint (over $\mathbb{Q}$).

(i) Show that every pair of embeddings $\sigma\colon L \hookrightarrow \mathbb{C}$ and $\tau\colon K \hookrightarrow \mathbb{C}$ can be extended to an embedding $\widetilde{\sigma\tau}\colon LK \hookrightarrow \mathbb{C}$ such that $\widetilde{\sigma\tau}|_L = \sigma$ and $\widetilde{\sigma\tau}|_L = \tau$

[1]If you want your solutions of this exercises to be corrected, please hand them in before the exercise class on June 24^{th}.

(ii) Show that if $L/\mathbb{Q}$ and $K/\mathbb{Q}$ are Galois extensions, then LK is Galois and

$$\mathrm{Gal}(LK/Q) = \mathrm{Gal}(L/Q) \times \mathrm{Gal}(K/\mathbb{Q})$$

(iii) Show that the ring of integers $\mathcal{O}_{LK}$ verifies

$$\mathcal{O}_L\mathcal{O}_K \subseteq \mathcal{O}_{LK} \subseteq \frac{1}{\big(\mathrm{disc}(\mathcal{O}_L/\mathbb{Z}), \mathrm{disc}(\mathcal{O}_K/\mathbb{Z})\big)}\mathcal{O}_L\mathcal{O}_K$$

(iv) Generalize point (ii) above in the following sense: let L/F be a finite Galois extension with Galois group $\mathrm{Gal}(L/F) = G$ and let K_1, K_2 be two subfields of L/K, *not supposed linearly disjoint anymore*. Writing $H_i = \mathrm{Gal}(L/K_i)$ for $i = 1, 2$. Show that

$$L^{H_1 \cap H_2} = K_1K_2.$$

Exercise 3. Let L/K be an extension of number fields with ring of integers $\mathcal{O}_L$ and $\mathcal{O}_K$, respectively. Let

$$\mathrm{disc}(\mathcal{O}_L/\mathcal{O}_K) = (\mathrm{disc}(\underline{e})) \subseteq \mathcal{O}_K$$

be the ideal generated the discriminants of all K-basis of L contained in $\mathcal{O}_L$.

(i) Show that if $\mathcal{O}_L$ is free as $\mathcal{O}_K$-module, this definition coincides with the usual one.

(ii) Show that a prime $P \subseteq \mathcal{O}_K$ is ramified in L/K if and only if P contains $\mathrm{disc}(\mathcal{O}_L/\mathcal{O}_K)$.
Hint: recall that the localization at a prime ideal of a Dedekind domain is a PID.

Exercise 4. Using that for every number field $K/\mathbb{Q}$ there exist one prime (actually, infinitely many primes) p such that

$$p\mathcal{O}_K = P_1P_2 \cdots P_{[K:\mathbb{Q}]},$$

show that there exists $\alpha \in K \setminus \mathcal{O}_K$ such that $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha) = \pm 1$.