Homework 4

Songyu Ye

September 27, 2025

Problem 1 Let p be a prime number, and n a positive integer greater than 1. Find an example for each of the following with brief justifications.

(1) A degree n extension of $\mathbb{Q}$ in which p is inert (i.e. the ring of integers in the extension possesses a unique prime $\mathfrak{q}$ above p, and the inertial degree $f_{\mathfrak{q}/p}$ is equal to n).

(2) A degree n extension of $\mathbb{Q}$ in which p is totally ramified.

Hint: You can apply results of Serre, I.6 after localizing at p.

Remark: There's nothing special about $\mathbb{Q}$. The same question can be answered similarly with any global field in place of $\mathbb{Q}$.

Solution:

(1) Pick any monic irreducible polynomial $m(x) \in \mathbb{F}_p[x]$ of degree n. Lift its coefficients to $\mathbb{Z}$ to get $f(x) \in \mathbb{Z}[x]$ with the same degree and reduction $\overline{f} = m$. Let $K = \mathbb{Q}(\alpha)$ with $f(\alpha) = 0$.

Since $\overline{f}$ is irreducible over $\mathbb{F}_p$, Gauss's lemma gives that f is irreducible over $\mathbb{Q}$, so $[K : \mathbb{Q}] = n$. Over a finite field, every irreducible polynomial is separable; hence $\gcd(\overline{f}, \overline{f}') = 1$. In particular, $\overline{f}$ has distinct roots and so the discriminant $\operatorname{disc}(\overline{f}) \neq 0$ in $\mathbb{F}_p$ (If one computes the discriminant over $\mathbb{Z}$ and then reduce mod p, one gets the discriminant of the reduced polynomial $\overline{f}$). This means $p \nmid \operatorname{disc}(f)$.

The relationship between the discriminant of f and that of K is given by

$$\operatorname{disc}(f) \ = \ \operatorname{disc}(K) \cdot [\mathcal{O}_K : \mathbb{Z}[\alpha]]^2.$$

which implies that $p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$. Therefore, Dedekind's theorem applies to f and p. By Dedekind's theorem, the factorization of (p) in $\mathcal{O}_K$ matches the factorization of $\overline{f}$ in $\mathbb{F}_p[x]$. Since $\overline{f}$ is irreducible of degree n, we get a single prime $\mathfrak{q}$ above p with residue degree $f_{\mathfrak{q}/p} = n$. Hence p is inert.

(2) Recall the following proposition from Serre's Local Fields.

Proposition 0.1 (Serre Proposition 1.6.17)**.** *Let A be a local ring with residue field k. Let $f \in A[x]$ be a monic polynomial. Let $B_f = A[x]/(f)$ free and finite type A-algebra. Suppose A is a DVR and f has the form*

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \quad a_i \in \mathfrak{m}_A \textit{ for all } i, \quad a_0 \notin \mathfrak{m}_A^2.$$

i.e. f is Eisenstein. Then B_f is a DVR with uniformizer the class of x in B_f, and residue field of B_f is k.

Apply this proposition to $A = \mathbb{Z}_{(p)}$, the localization of $\mathbb{Z}$ at the prime ideal (p), with $f(x) = x^n - p$. Then $B_f = \mathbb{Z}_{(p)}[x]/(x^n - p)$ is a DVR with residue field $\mathbb{F}_p$. The corresponding field extension is $K = \mathrm{Frac}(B_f) = \mathbb{Q}(\sqrt[n]{p})$. The minimal polynomial $f(x) = x^n - p$ is Eisenstein at p, so $[K : \mathbb{Q}] = n$. Eisenstein at p implies that p is totally ramified in K because the residue field extension is trivial and therefore the ramification index must be n.

Problem 2 Let A be a Dedekind domain, $K = \mathrm{Frac}(A)$. Let L/K be a finite separable extension with normal closure M of L so that M is Galois over K. Let $\mathfrak{p}$ be a prime ideal of A. Fix a prime ideal $\mathfrak{t}$ of M above $\mathfrak{p}$. (By convention, this means $\mathfrak{t}$ is a nonzero prime in the integral closure of A in M such that $\mathfrak{t}$ divides $\mathfrak{p}$.) Denote by $D_{\mathfrak{t}}(M/K)$ the decomposition group of $\mathfrak{t}$ in M/K.

(i) Define a map

$$\mathrm{Gal}(M/K) \to \{\text{primes of } L \text{ above } \mathfrak{p}\}, \qquad \sigma \mapsto \sigma(\mathfrak{t}) \cap L.$$

Show that this map induces a bijection

$$\mathrm{Gal}(M/L)\backslash\mathrm{Gal}(M/K)/D_{\mathfrak{t}}(M/K) \xrightarrow{\sim} \{\text{primes of } L \text{ above } \mathfrak{p}\}.$$

(ii) Assume that $\mathrm{Gal}(M/K) \simeq S_3$, the symmetric group in 3 variables, that $D_{\mathfrak{t}}(M/K)$ and $\mathrm{Gal}(M/L)$ are order 2 subgroups of $\mathrm{Gal}(M/K)$ which are equal (not just isomorphic). Use part (i) to verify that $\mathfrak{p}$ does *not* split completely in L.

Remark: The point of (ii) is that when the decomposition group of $\mathfrak{t}$ is not normal in $\mathrm{Gal}(M/K)$, the prime $\mathfrak{t}$ need not split completely in the decomposition field, which is L here. A concrete example for (ii) can be given when

$$K = \mathbb{Q}, \quad L = \mathbb{Q}(\sqrt[3]{2}), \quad M = \mathbb{Q}(\sqrt[3]{2}, \zeta_3).$$

By the Chebotarev density theorem, or by explicit computation, you can find $\mathfrak{t}$ such that $(\mathfrak{t}, M/K)$ is the unique nontrivial element of $\mathrm{Gal}(M/L)$. Then all the conditions of (ii) are satisfied.

Solution:

(i) Let $G = \mathrm{Gal}(M/K)$, $H = \mathrm{Gal}(M/L)$, and fix a prime $\mathfrak{t}$ of M above $\mathfrak{p} \subset A$. Define

$$\Phi : G \longrightarrow \{\text{primes of } L \text{ above } \mathfrak{p}\}, \qquad \sigma \longmapsto \big(\sigma\mathfrak{t}\big) \cap L.$$

Since σ is a K-automorphism, it fixes $\mathfrak{p}$ and therefore the contraction of $\sigma\mathfrak{t}$ to L is a prime of L above $\mathfrak{p}$. In particular, the target of Φ is correct.

Moreover, the map Φ is right $D_{\mathfrak{t}}$-invariant and left H-invariant:

If $d \in D_{\mathfrak{t}}(M/K) = \{g \in G : g\mathfrak{t} = \mathfrak{t}\}$, then

$$\Phi(\sigma d) = \big(\sigma d\,\mathfrak{t}\big) \cap L = \big(\sigma\mathfrak{t}\big) \cap L = \Phi(\sigma)$$

If $h \in H$ (so h fixes L), then

$$\Phi(h\sigma) = \big(h\sigma\mathfrak{t}\big) \cap L = h\big((\sigma\mathfrak{t}) \cap L\big) = (\sigma\mathfrak{t}) \cap L = \Phi(\sigma)$$

Thus Φ is constant on double cosets $H\sigma D_{\mathfrak{t}}$.

So Φ descends to a map

$$\overline{\Phi} : \ H\backslash G/D_{\mathfrak{t}} \ \longrightarrow \ \{\text{primes of } L \text{ above } \mathfrak{p}\}.$$

Now I claim that $\overline{\Phi}$ is surjective and injective.

Let $\mathfrak{q}$ be a prime of L above $\mathfrak{p}$. Choose a prime $\mathfrak{t}'$ of M above $\mathfrak{q}$. Because M/K is Galois, there exists $\sigma \in G$ with $\sigma\mathfrak{t} = \mathfrak{t}'$. Then $\overline{\Phi}(H\sigma D_{\mathfrak{t}}) = (\sigma\mathfrak{t}) \cap L = \mathfrak{q}$.

Suppose $\overline{\Phi}(H\sigma_1 D_{\mathfrak{t}}) = \overline{\Phi}(H\sigma_2 D_{\mathfrak{t}})$. Then $(\sigma_1\mathfrak{t}) \cap L = (\sigma_2\mathfrak{t}) \cap L =: \mathfrak{q}$. Primes of M above the same $\mathfrak{q}$ form a single H-orbit (see remark), so there is $\tau \in H$ with $\tau\sigma_1\mathfrak{t} = \sigma_2\mathfrak{t}$. Hence $\sigma_2^{-1}\tau\sigma_1 \in D_{\mathfrak{t}}$, i.e. $\sigma_2 \in H\sigma_1 D_{\mathfrak{t}}$. Thus the double cosets coincide.

Therefore $\overline{\Phi}$ is a bijection:

$$H\backslash G/D_{\mathfrak{t}} \ \xrightarrow{\sim} \ \{\text{primes of } L \text{ above } \mathfrak{p}\}.$$

(ii) Assume $G \simeq S_3$, $|G| = 6$, and that both $H = \mathrm{Gal}(M/L)$ and $D_{\mathfrak{t}}(M/K)$ are order 2 subgroups and are equal. Then $[L : K] = |G|/|H| = 3$.

By (i), the primes of L above $\mathfrak{p}$ are in bijection with the double cosets $H\backslash G/H$. Take $H = \langle (12) \rangle \le S_3$ for concreteness. There are two double cosets, H and $H(13)H$. One can check that the latter has size 4. Thus there are exactly two primes of L above $\mathfrak{p}$. If $\mathfrak{p}$ split completely in L, there would be $[L : K] = 3$ distinct primes over $\mathfrak{p}$. Therefore $\mathfrak{p}$ does not split completely in L.

Remark 0.2 (This remark is just for myself)**.** *Suppose M/K is finite Galois (i.e. finite, separable, normal). For any intermediate field $K \subseteq L \subseteq M$:*

M/L is separable: Take any $\alpha \in M$. Its minimal polynomial over K, say $m_\alpha(x)$, is separable (no repeated roots). The minimal polynomial of α over L divides $m_\alpha(x)$ in $L[x]$. A factor of a separable polynomial is still separable, so the minimal polynomial of α over L is separable.

M/L is normal: Recall that for finite extensions, normal means that the minimal polynomial of any element in the extension splits completely in the extension. Take any $\alpha \in M$. Its minimal polynomial over K, say $m_\alpha(x)$, splits completely in M since M/K is normal. The

minimal polynomial of α over L divides $m_\alpha(x)$ in $L[x]$. Since $m_\alpha(x)$ splits completely in M, so does its factor, the minimal polynomial of α over L. Hence M/L is normal.

So M/L is both separable and normal $\Rightarrow$ Galois. Thus $H = \mathrm{Gal}(M/L)$ is indeed the full automorphism group of M over L.

Neukirch Ch. I.9, Exercise 3 Continue the general setup from Problem 2. Assume the following:

(i) L/K is solvable, meaning that $\mathrm{Gal}(M/K)$ is a solvable group. (We are not assuming $M = L$.) Recall that a group G is solvable if there is a chain of subgroups

$$\{1\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G$$

such that each G_i is normal in G_{i+1} and the quotient G_{i+1}/G_i is abelian.

(ii) $p = [L : K]$ is a prime number.

Now let $\mathfrak{p}$ be a prime of K unramified in L. If there are two primes $\mathfrak{q}$ and $\mathfrak{q}'$ of L above $\mathfrak{p}$ such that the inertial degrees $f_\mathfrak{q}$ and $f_{\mathfrak{q}'}$ are equal to 1, then show that $\mathfrak{p}$ splits completely in L/K.

Caveat: The extension degree p has nothing to do with the prime ideal $\mathfrak{p}$ in the problem.

Hint: Let S_p denote the symmetric group in p letters acting on $\{1, 2, \dots, p\}$. If G is a solvable subgroup of S_p acting transitively on $\{1, 2, \dots, p\}$ then every nontrivial element of G fixes at most one element in $\{1, 2, \dots, p\}$. (A reference for this fact is given in Neukirch.)

Solution: Let $G = \mathrm{Gal}(M/K)$, $H = \mathrm{Gal}(M/L)$. Then $[L : K] = [G : H] = p$ is prime. Let $\mathfrak{p}$ be a prime of K unramified in L. Fix $\mathfrak{t} \mid \mathfrak{p}$ in M. Let $D = D_\mathfrak{t}(M/K)$, $I = I_\mathfrak{t}(M/K)$.

Let $X = H\backslash G$. The set X has size p and there is a transitive action of G on X by right multiplication. Right multiplication gives a homomorphism $\pi : G \hookrightarrow S_X \cong S_p$, whose image $G^* := \pi(G)$ is transitive and solvable.

Recall by the previous problem that $X/D_\mathfrak{t}$ is in bijection with the primes of L above $\mathfrak{p}$. For the base point $\bar{e} \in X$, $\mathrm{Stab}_D(\bar{e}) = \{d \in D : Hd = H\} = D \cap H$. Hence $|\text{orbit of } \bar{e}| = [D : D \cap H]$. Moreover, we have that

$$D/I \cong \mathrm{Gal}\big(\kappa(\mathfrak{t})/\kappa(\mathfrak{p})\big)$$

so

$$|D/I| = f_{\mathfrak{t}/\mathfrak{p}}$$

$$(D \cap H)/(I \cap H) \cong \mathrm{Gal}\big(\kappa(\mathfrak{t})/\kappa(\mathfrak{q})\big)$$

so $|(D \cap H)/(I \cap H)| = f_{\mathfrak{t}/\mathfrak{q}}$.

Therefore

$$[D : D \cap H] = \frac{|D|}{|D \cap H|} = \frac{|D/I|}{|(D \cap H)/(I \cap H)|} = \frac{f_{\mathfrak{t}/\mathfrak{p}}}{f_{\mathfrak{t}/\mathfrak{q}}} = f_{\mathfrak{q}/\mathfrak{p}}$$

Thus we see that the D-orbit size on X for $\mathfrak{q}$ equals $f_{\mathfrak{q}/\mathfrak{p}}$.

Restriction and reduction give a surjection $D \xrightarrow{\text{res}} D_{\mathfrak{q}}(L/K) \twoheadrightarrow \operatorname{Gal}\big(\kappa(\mathfrak{q})/\kappa(\mathfrak{p})\big)$ and since $\mathfrak{p}$ is unramified in L, the kernel of $D \to \operatorname{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p}))$ is precisely $D \cap H$. In particular the size of the orbit through $\bar{e}$ is $f_{\mathfrak{q}/\mathfrak{p}} = \operatorname{ord} \operatorname{Frob}_{\mathfrak{p}}$, where $\operatorname{Frob}_{\mathfrak{p}}$ is the Frobenius element in $\operatorname{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p}))$.

In particular, $f = 1$ if and only if the corresponding point of X is fixed by $\operatorname{Frob}_{\mathfrak{p}}$. We know there exist two primes $\mathfrak{q}, \mathfrak{q}'$ of L above $\mathfrak{p}$ with $f_{\mathfrak{q}/\mathfrak{p}} = f_{\mathfrak{q}'/\mathfrak{p}} = 1$. Equivalently, the permutation $\operatorname{Frob}_{\mathfrak{p}} \in G^* \leq S_p$ fixes two distinct points of X. Therefore, the hint implies that $\operatorname{Frob}_{\mathfrak{p}}$ must be the identity permutation.

If the Frobenius permutation is the identity, all its cycles have length 1; hence $f_{\mathfrak{q}/\mathfrak{p}} = 1$ for every prime $\mathfrak{q}$ of L over $\mathfrak{p}$. Since $\mathfrak{p}$ is unramified in L, also $e_{\mathfrak{q}/\mathfrak{p}} = 1$ for all $\mathfrak{q}$. Now we use the identity

$$[L : K] = \sum_{\mathfrak{q}|\mathfrak{p}} e_{\mathfrak{q}/\mathfrak{p}} f_{\mathfrak{q}/\mathfrak{p}} = \#\{\mathfrak{q} \mid \mathfrak{p}\}$$

Because $[L : K] = p$, there are p distinct primes above $\mathfrak{p}$, as desired.