Solutions 9

Decomposition of primes

1. Let A be a Dedekind ring with quotient field K. Let K'/K be a finite separable extension and L/K its Galois closure over K. Set $\Gamma := \mathrm{Gal}(L/K)$ and $\Gamma' := \mathrm{Gal}(L/K')$. Let A' be the integral closure of A in K' and B that in L. Consider a maximal ideal $\mathfrak{p} \subset A$ with $k(\mathfrak{p})$ perfect and a prime ideal $\mathfrak{q} \subset B$ above $\mathfrak{p}$.

   (a) Show that $\bigcap_{\gamma\in\Gamma} \gamma^{-1}\Gamma'\gamma = \{1\}$.

   (b) Construct a natural bijection between the set $S_\mathfrak{p}$ of prime ideals of A' above $\mathfrak{p}$ and the set of double cosets $\Gamma'\backslash\Gamma/\Gamma_\mathfrak{q}$.

   (c) Prove that $\mathfrak{p}$ is totally split in K' if and only if it is totally split in L.

   (d) Prove that $\mathfrak{p}$ is unramified in K' if and only if it is unramified in L.

   Solution:

   (a) The group in question is the unique largest subgroup of Γ' that is normal in Γ. By the Galois correspondence it therefore corresponds to the unique smallest subfield of L containing K' that is galois over K. By assumption that is L itself, so the subgroup is trivial.

   (b) For any $\gamma \in \Gamma$ we first note that ${}^\gamma\mathfrak{q} \subset B$ is a prime ideal with ${}^\gamma\mathfrak{q} \cap A = \mathfrak{p}$. Its intersection ${}^\gamma\mathfrak{q} \cap A'$ is then a prime ideal of A', whose intersection with A is again $\mathfrak{p}$. Thus we have a natural map

   $$\Gamma \longrightarrow S_\mathfrak{p}, \quad \gamma \mapsto {}^\gamma\mathfrak{q} \cap A'. \tag{$*$}$$

   For any $\mathfrak{p}' \in S_\mathfrak{p}$ there exists a prime ideal of B above $\mathfrak{p}'$. Since Γ transitively permutes the prime ideals of B above $\mathfrak{p}$, this prime ideal has the form ${}^\gamma\mathfrak{q}$ for some $\gamma \in \Gamma$. Thus $\mathfrak{p}' = {}^\gamma\mathfrak{q} \cap A'$, proving that the map $(*)$ is surjective.

   Now consider another element $\delta \in \Gamma$. Then we have ${}^\delta\mathfrak{q} \cap A' = {}^\gamma\mathfrak{q} \cap A'$ if and only if both ${}^\delta\mathfrak{q}$ and ${}^\gamma\mathfrak{q}$ are prime ideals of B above the prime ideal ${}^\gamma\mathfrak{q} \cap A'$ of A'. As the Galois group Γ' transitively permutes the prime ideals of B above ${}^\gamma\mathfrak{q} \cap A'$, this is equivalent to ${}^\delta\mathfrak{q} = {}^{\gamma'\gamma}\mathfrak{q}$ for some $\gamma' \in \Gamma'$. That in turn is equivalent to $\mathfrak{q} = {}^{\delta^{-1}\gamma'\gamma}\mathfrak{q}$ and hence to $\delta^{-1}\gamma'\gamma \in \Gamma_\mathfrak{q}$, or again to $\gamma'\gamma\Gamma_\mathfrak{q} = \delta\Gamma_\mathfrak{q}$. Thus ${}^\delta\mathfrak{q} \cap A' = {}^\gamma\mathfrak{q} \cap A'$ if and only if there exists $\gamma' \in \Gamma'$ with $\gamma'\gamma\Gamma_\mathfrak{q} = \delta\Gamma_\mathfrak{q}$, that is, if and only if $\Gamma'\gamma\Gamma_\mathfrak{q} = \Gamma'\delta\Gamma_\mathfrak{q}$. Thus the map $(*)$ induces the desired bijection.

(c) The prime $\mathfrak{p}$ is totally split in K' if and only if $|S_{\mathfrak{p}}| = [K'/K]$. By (b) this is equivalent to $|\Gamma'\backslash\Gamma/\Gamma_{\mathfrak{q}}| = |\Gamma'\backslash\Gamma|$. This is so if and only if the surjective map $\Gamma'\backslash\Gamma \twoheadrightarrow \Gamma'\backslash\Gamma/\Gamma_{\mathfrak{q}}$ defined by $\Gamma'\gamma \mapsto \Gamma'\gamma\Gamma_{\mathfrak{q}}$ is bijective. That in turn is equivalent to $\Gamma'\gamma\Gamma_{\mathfrak{q}} = \Gamma'\gamma$ for all $\gamma \in \Gamma$. But

$$\Gamma'\gamma\Gamma_{\mathfrak{q}} = \Gamma'\gamma \iff \gamma\Gamma_{\mathfrak{q}} \subset \Gamma'\gamma \iff \Gamma_{\mathfrak{q}} \subset \gamma^{-1}\Gamma'\gamma.$$

Thus the condition is equivalent to $\Gamma_{\mathfrak{q}} \subset \bigcap_{\gamma\in\Gamma} \gamma^{-1}\Gamma'\gamma \overset{\text{(a)}}{=} \{1\}$. But that is equivalent to $\mathfrak{p}$ being totally split in L, as desired.

(d) By (b) the prime $\mathfrak{p}$ is unramified in K' if and only if $e_{{}^{\gamma}\mathfrak{q}\cap A'|\mathfrak{p}} = 1$ for every $\gamma \in \Gamma$. By the multiplicativity

$$e_{{}^{\gamma}\mathfrak{q}|\mathfrak{p}} \;=\; e_{{}^{\gamma}\mathfrak{q}|{}^{\gamma}\mathfrak{q}\cap A'} \cdot e_{{}^{\gamma}\mathfrak{q}\cap A'|\mathfrak{p}}$$

this is equivalent to $e_{{}^{\gamma}\mathfrak{q}|\mathfrak{p}} = e_{{}^{\gamma}\mathfrak{q}|{}^{\gamma}\mathfrak{q}\cap A'}$ for all $\gamma \in \Gamma$. To translate this into a condition on inertia groups we use the assumption that $k(\mathfrak{q})/k(\mathfrak{p})$ is separable. First note that $k({}^{\gamma}\mathfrak{q})/k(\mathfrak{p})$ is then again separable. Thus by Proposition 6.4.3 of the lecture the inertia group $I_{{}^{\gamma}\mathfrak{q}}$ satisfies $|I_{{}^{\gamma}\mathfrak{q}}| = e_{{}^{\gamma}\mathfrak{q}|\mathfrak{p}}$. Also, the subextension $k({}^{\gamma}\mathfrak{q}\cap A')/k(\mathfrak{p})$ is separable, so by the same proposition applied to the extension L/K' we have $|I_{{}^{\gamma}\mathfrak{q}} \cap \Gamma'| = e_{{}^{\gamma}\mathfrak{q}|\mathfrak{q}\cap A'}$. The condition is therefore equivalent to $I_{{}^{\gamma}\mathfrak{q}} = I_{{}^{\gamma}\mathfrak{q}} \cap \Gamma'$, or again to $I_{{}^{\gamma}\mathfrak{q}} \subset \Gamma'$, for all $\gamma \in \Gamma$. Now a direct computation shows that $I_{{}^{\gamma}\mathfrak{q}} = \gamma I_{\mathfrak{q}}\gamma^{-1}$. Thus the condition is equivalent to $I_{\mathfrak{q}} \subset \bigcap_{\gamma\in\Gamma} \gamma^{-1}\Gamma'\gamma \overset{\text{(a)}}{=} \{1\}$. But that in turn is equivalent to $e_{\mathfrak{q}|\mathfrak{p}} = |I_{\mathfrak{q}}| = 1$. This is equivalent to $e_{{}^{\gamma}\mathfrak{q}|\mathfrak{p}} = 1$ for all $\gamma \in \Gamma$, and hence to $\mathfrak{p}$ being unramified in L, as desired.

2. Let A be a Dedekind ring with quotient field K. Consider finite Galois extensions $M/L/K$ such that M/K is Galois. Let $B \subset C$ denote the integral closures of A in $L \subset M$. Consider a prime $\mathfrak{r} \subset C$ above a prime $\mathfrak{q} \subset B$ above a prime $\mathfrak{p} \subset A$.

   (a) Show that the decomposition group of $\mathfrak{r}$ in $\mathrm{Gal}(M/K)$ surjects to the decomposition group of $\mathfrak{q}$ in $\mathrm{Gal}(L/K)$.

   (b) Show that the inertia group of $\mathfrak{r}$ in $\mathrm{Gal}(M/K)$ surjects to the inertia group of $\mathfrak{q}$ in $\mathrm{Gal}(L/K)$, if $k(\mathfrak{p})$ is perfect.

   Hint: Use the multiplicativity $e_{\mathfrak{r}|\mathfrak{p}} = e_{\mathfrak{r}|\mathfrak{q}} \cdot e_{\mathfrak{q}|\mathfrak{p}}$.

Solution: Abbreviate $\Gamma := \mathrm{Gal}(M/K)$ and $\bar\Gamma := \mathrm{Gal}(L/K)$ and let $\pi\colon \Gamma \twoheadrightarrow \bar\Gamma$ denote the canonical surjection. Then $\Gamma' := \ker(\pi) = \mathrm{Gal}(M/L)$.

(a) The respective decomposition groups are

$$\begin{aligned}\Gamma_{\mathfrak{r}} &:= \big\{\gamma \in \Gamma \;\big|\; {}^{\gamma}\mathfrak{r} = \mathfrak{r}\big\},\\ \bar\Gamma_{\mathfrak{q}} &:= \big\{\bar\gamma \in \bar\Gamma \;\big|\; {}^{\bar\gamma}\mathfrak{q} = \mathfrak{q}\big\}.\end{aligned}$$

For any $\gamma \in \Gamma_{\mathfrak{r}}$ we thus have

$$^{\pi(\gamma)}\mathfrak{q} = {}^{\pi(\gamma)}(\mathfrak{r} \cap B) = {}^{\gamma}\mathfrak{r} \cap B = \mathfrak{r} \cap B = \mathfrak{q}$$

and therefore $\pi(\gamma) \in \bar{\Gamma}_{\mathfrak{q}}$. Conversely, take any $\bar{\gamma} \in \bar{\Gamma}_{\mathfrak{q}}$ and choose $\gamma \in \pi^{-1}(\bar{\gamma})$. Then ${}^{\gamma}\mathfrak{r} \cap B = {}^{\pi(\gamma)}(\mathfrak{r} \cap B) = {}^{\bar{\gamma}}\mathfrak{q} = \mathfrak{q}$ shows that ${}^{\gamma}\mathfrak{r}$ is a prime ideal of C above $\mathfrak{q}$. As $\Gamma' = \ker(\pi)$ transitively permutes the prime ideals of C above $\mathfrak{q}$, there exists $\delta \in \ker(\pi)$ with ${}^{\gamma}\mathfrak{r} = {}^{\delta}\mathfrak{r}$. Then ${}^{\delta^{-1}\gamma}\mathfrak{r} = \mathfrak{r}$ and so $\delta^{-1}\gamma \in \Gamma_{\mathfrak{r}}$ with $\pi(\delta^{-1}\gamma) = \bar{\gamma}$. Thus π induces a surjection $\Gamma_{\mathfrak{r}} \twoheadrightarrow \bar{\Gamma}_{\mathfrak{q}}$, proving (a).

(b) The respective inertia groups are

$$\begin{aligned} I_{\mathfrak{r}} &:= \{\gamma \in \Gamma \mid \forall x \in C\colon {}^{\gamma}x \equiv x \bmod \mathfrak{r}\}, \\ \bar{I}_{\mathfrak{q}} &:= \{\bar{\gamma} \in \bar{\Gamma} \mid \forall x \in B\colon {}^{\bar{\gamma}}x \equiv x \bmod \mathfrak{q}\}. \end{aligned}$$

For any $\gamma \in I_{\mathfrak{r}}$ and any $x \in B$ we thus have ${}^{\gamma}x - x \in \mathfrak{r} \cap B = \mathfrak{q}$ and therefore $\pi(\gamma) \in \bar{I}_{\mathfrak{q}}$. Thus π induces a homomorphism $I_{\mathfrak{r}} \to \bar{I}_{\mathfrak{q}}$. By construction its kernel $I'_{\mathfrak{r}} := I_{\mathfrak{r}} \cap \Gamma'$ is the inertia group of $\mathfrak{r}$ over $\mathfrak{q}$, and we obtain an injection $I_{\mathfrak{r}}/I'_{\mathfrak{r}} \hookrightarrow \bar{I}_{\mathfrak{q}}$. Next, since $k(\mathfrak{p})$ is perfect, the finite extensions $k(\mathfrak{r})/k(\mathfrak{q})/k(\mathfrak{p})$ are separable. The respective inertia groups therefore satisfy $|I_{\mathfrak{r}}| = e_{\mathfrak{r}|\mathfrak{p}}$ and $|\bar{I}'_{\mathfrak{r}}| = e_{\mathfrak{r}|\mathfrak{q}}$ and $|\bar{I}_{\mathfrak{q}}| = e_{\mathfrak{q}|\mathfrak{p}}$. By the multiplicativity $e_{\mathfrak{r}|\mathfrak{p}} = e_{\mathfrak{r}|\mathfrak{q}} \cdot e_{\mathfrak{q}|\mathfrak{p}}$ this implies that $|\bar{I}_{\mathfrak{q}}| = e_{\mathfrak{r}|\mathfrak{p}}/e_{\mathfrak{r}|\mathfrak{q}} = |I_{\mathfrak{r}}/I'_{\mathfrak{r}}|$. Thus the injection $I_{\mathfrak{r}}/I'_{\mathfrak{r}} \hookrightarrow \bar{I}_{\mathfrak{q}}$ is a bijection, proving (b).

3. Construct a number field L in which there are at least two distinct prime ideals of $\mathcal{O}_L$ over every rational prime.

Hint: Try a composite of quadratic number fields.

Solution: Choose distinct odd primes $p \equiv p' \equiv 1 \bmod (4)$ with $(\frac{p}{p'}) = (\frac{p'}{p}) = 1$, for example $(p, p') = (13, 17)$ as in the solution to problem 6 (c) of sheet 5. Setting $K := \mathbb{Q}(\sqrt{p}\,)$ and $K' := \mathbb{Q}(\sqrt{p'}\,)$, we claim that $L := KK'$ has the desired property.

First note that $(\frac{p}{p'}) = 1$ implies that p splits in $\mathcal{O}_{K'}$, so there are two distinct primes of $\mathcal{O}_{K'}$ above p. Any primes of $\mathcal{O}_L$ above these are then two distinct primes of $\mathcal{O}_L$ above p, as desired. The same argument with K and K' interchanged proves that there are at least two distinct primes of $\mathcal{O}_L$ above p'.

Now consider an arbitrary rational prime $q \neq p, p'$ and a prime $\mathfrak{q}$ of $\mathcal{O}_L$ above q. Then $d_K = p$ and $d_{K'} = p'$ implies that q is unramified in $\mathcal{O}_K$ and in $\mathcal{O}_{K'}$. By exercise 2 (b) the inertia group $I_{\mathfrak{q}}$ therefore has trivial image in $\Gamma := \mathrm{Gal}(K/\mathbb{Q})$ and in $\mathrm{Gal}(K'/\mathbb{Q})$. Since $\Gamma \xrightarrow{\sim} \mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(K'/\mathbb{Q})$, it follows that $I_{\mathfrak{q}}$ is trivial; hence p is unramified in $\mathcal{O}_L$. The decomposition group $\Gamma_{\mathfrak{q}} < \Gamma$ is thus generated by the Frobenius substitution $\mathrm{Frob}_{\mathfrak{q}|q}$. In particular it is a cyclic subgroup of $\Gamma \cong C_2^2$ and hence a proper subgroup. Thus the number of primes of $\mathcal{O}_L$ over q is $[\Gamma : \Gamma_{\mathfrak{q}}] \geqslant 2$, as desired.

Aliter: Take $L := \mathbb{Q}(\mu_n)$ for a suitable composite integer n, for instance $n = pp'$ with p, p' as above.

4. Consider a number field K and a positive integer m. Let $G_m(K) := \{x^m \mid x \in K^\times\}$ be the subgroup of m-th powers in $K^\times$ and $L_m(K)$ the group of elements $x \in K^\times$ such that, in the prime factorization of (x), all exponents are multiples of m.

   (a) Prove that for every $x \in L_m(K)$, there exists a unique fractional ideal $\mathfrak{a}_x$ such that $(x) = \mathfrak{a}_x^m$.

   (b) Define $S_m(K) := L_m(K)/G_m(K)$ and $\mathrm{Cl}(\mathcal{O}_K)[m] := \{c \in \mathrm{Cl}(\mathcal{O}_K) \mid c^m = 1\}$ and show that we get a well-defined group homomorphism

   $$f\colon S_m(K) \longrightarrow \mathrm{Cl}(\mathcal{O}_K)[m], \quad [x] \mapsto [\mathfrak{a}_x]$$

   (c) Show that f is surjective.

   (d) Identify the kernel of f.

   Solution:

   (a) For any $x \in L_m(K)$ the prime factorization of the principal ideal (x) has the form $(x) = \prod_i \mathfrak{p}_i^{ma_i}$ by assumption. Thus $\mathfrak{a}_x := \prod_i \mathfrak{p}_i^{a_i}$ has the required property, and it is unique by the uniqueness of the prime factorization.

   (b) Consider the map $\tilde{f}\colon L_m(K) \to \mathrm{Cl}(\mathcal{O}_K)$, $x \mapsto [\mathfrak{a}_x]$. For any $x, y \in L_m(K)$ we have $(\mathfrak{a}_x\mathfrak{a}_y)^m = \mathfrak{a}_x^m\mathfrak{a}_y^m = (x)(y) = (xy)$ and so $\mathfrak{a}_{xy} = \mathfrak{a}_x\mathfrak{a}_y$ by uniqueness. Thus $\tilde{f}$ is a homomorphism. Also $\tilde{f}(x)^m = [\mathfrak{a}_x]^m = [\mathfrak{a}_x^m] = [(x)] = 1$ shows that $\mathrm{Im}(\tilde{f}) \subset \mathrm{Cl}(\mathcal{O}_K)[m]$. Moreover consider any $x \in G_m(K)$ and choose $z \in K^\times$ such that $z^m = x$. Then $\mathfrak{a}_x = (z)$ and hence $\tilde{f}(x) = 1$. Therefore $G_m(K) \subset \mathrm{Ker}\,\tilde{f}$, and so $\tilde{f}$ factors through S_m, inducing the homomorphism f.

   (c) Let $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}_K)[m]$. Then $\mathfrak{a}^m$ is principal, say $\mathfrak{a}^m = (x)$. But then $x \in L_m(K)$ and $\mathfrak{a} = \mathfrak{a}_x$ by uniqueness. Thus $f([x]) = [\mathfrak{a}]$; hence f is surjective, as desired.

   (d) Take any $x \in L_m(K)$. Then $f([x]) = 1$ if and only if $\mathfrak{a}_x = (y)$ for some $y \in K^\times$. By unique factorization of ideals this is equivalent to $\mathfrak{a}_x^m = (y)^m$, and hence to $(x) = (y^m)$, or again to $x = uy^m$ for some unit $u \in \mathcal{O}_K^\times$. Thus $f([x]) = 1$ if and only if $x \in \mathcal{O}_K^\times G_m(K)$. Therefore $\mathrm{Ker}(f) = \mathcal{O}_K^\times G_m(K)/G_m(K)$. Since $\mathcal{O}_K^\times \cap G_m(K) = (\mathcal{O}_K^\times)^m$, the second isomorphism theorem for groups yields a natural isomorphism $\mathrm{Ker}(f) \cong \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^m$.

*5. (*Hilbert's Theorem 90*) Let L/K be a finite Galois extension of fields whose Galois group is cyclic and generated by σ. Show that for any element $x \in L^\times$ with $\mathrm{Norm}_{L/K}(x) = 1$ there exists an element $y \in L^\times$ with $x = \sigma(y)/y$.

Hint: Set $n := [L/K]$ and consider the map

$$h\colon L \longrightarrow L, \quad z \mapsto h(z) := \sum_{i=0}^{n-1} \sigma^i(z) \cdot \prod_{i<j<n} \sigma^j(x).$$

Solution: By Galois theory σ has finite order n and the elements $\mathrm{id}, \sigma, \ldots, \sigma^{n-1} \in \mathrm{Hom}_K(L, L)$ are L-linearly independent. Since all $\sigma^j(x)$ are non-zero, the map $h \in \mathrm{Hom}_K(L, L)$ is therefore also non-zero. Thus there exists $z \in L$ with $y := h(z) \neq 0$. Using the facts that $\sigma^n = \mathrm{id}$ and $\prod_{0<j\leqslant n} \sigma^j(x) = \mathrm{Norm}_{L/K}(x) = 1$, we compute

$$\begin{aligned}
x \cdot h(z) &= \sigma^n(x) \cdot \sum_{i=0}^{n-1} \sigma^i(z) \cdot \prod_{i<j<n} \sigma^j(x) \\
&= \sum_{i=0}^{n-1} \sigma^i(z) \cdot \prod_{i<j\leqslant n} \sigma^j(x) \\
&= z \cdot \prod_{0<j\leqslant n} \sigma^j(x) + \sum_{i=1}^{n-1} \sigma^i(z) \cdot \prod_{i<j\leqslant n} \sigma^j(x) \\
&= \sigma^n(z) \cdot 1 + \sum_{i=1}^{n-1} \sigma^i(z) \cdot \prod_{i<j\leqslant n} \sigma^j(x) \\
&= \sum_{i=1}^{n} \sigma^i(z) \cdot \prod_{i<j\leqslant n} \sigma^j(x) \\
&= \sigma(h(z)).
\end{aligned}$$

We therefore have $xy = \sigma(y)$ and hence $x = \sigma(y)/y$, as desired.