D-MATH Algebraic Number Theory FS 2018
Prof. Richard Pink

Solutions 6

Decomposition Of Prime Ideals, Different

1. Let $R := \mathbb{F}_p(t)[x]$ for a rational prime p and algebraically independent t and x. Let A be the localization of R at the prime ideal Rx, and let $\mathfrak{p} := Ax$ denote its maximal ideal. Let K be the quotient field of A.

   (a) Show that the polynomial $f(Y) := Y^p - x^{p-1}Y - t \in A[Y]$ is separable and irreducible over K.

   (b) Consider a field extension $L = K(y)$ with $f(y) = 0$. Show that L/K is galois with Galois group isomorphic to $\mathbb{F}_p$, acting by $y \mapsto y + \alpha x$ for all $\alpha \in \mathbb{F}_p$.

   (c) Show that $B := A[y]$ is the integral closure of A in L and that $\mathfrak{P} := B\mathfrak{p}$ is the unique prime ideal of B above $\mathfrak{p}$.

   (d) Show that the extension of residue fields $k(\mathfrak{P})/k(\mathfrak{p})$ is inseparable.

   *(e) Repeat the constructions of $R, A, \mathfrak{p}, K, L$ after replacing the field $\mathbb{F}_p(t)$ by its inseparable extension $\mathbb{F}_p(s)$ with $s^p = t$, so that $f(Y) = Y^p - x^{p-1}Y - s^p$. Show that (a) and (b) are still true for the resulting items by $R', A', \mathfrak{p}', K', L'$. But in (c) define B' instead as the integral closure of A' in L' and prove that $B'\mathfrak{p}' = \mathfrak{Q}'^p$ for a prime ideal $\mathfrak{Q}'$.

   Note: The correct definition of an unramified prime $\mathfrak{P}/\mathfrak{p}$ requires not only that $e_{\mathfrak{P}/\mathfrak{p}} = 1$ but also that the residue field extension is separable. If one left out the second condition, the above example would be an unramified extension which becomes ramified after the base change from $\mathbb{F}_p(t)$ to $\mathbb{F}_p(s)$, which is just one of the things that would go wrong.

Solution:

(a) The polynomial $Y^p - x^{p-1}Y - t \in \mathbb{F}_p[x, Y, t]$ is monic of degree 1 with respect to the variable t, hence it is irreducible in $\mathbb{F}_p(x, Y)[t]$. Being monic, by the Gauss lemma it is therefore also irreducible in $\mathbb{F}_p[x, Y, t]$ and hence in $A[Y]$. Furthermore the formal derivative $\frac{\mathrm{d}f}{\mathrm{d}Y} = -x^{p-1}$ is nonzero, so f is separable.

(b) For any $\alpha \in \mathbb{F}_p$ we have $\alpha^p = \alpha$ and hence

$$f(y+\alpha x) = (y+\alpha x)^p - x^{p-1}(y+\alpha x) - t = y^p + \alpha x^p - x^{p-1}y - \alpha x^p - t = f(y) = 0.$$

Since the $y + \alpha x$ are all distinct, it follows that $f(Y) = \prod_{\alpha \in \mathbb{F}_p}(Y - y - \alpha x)$ in $L[Y]$. Thus L/K is already a splitting field of f and hence galois with Galois group in bijection with $\mathbb{F}_p$. Direct computation shows that this bijection is a group isomorphism.

(c) Since $B \cong A[Y]/(f)$, we have

$$(*) \quad B/\mathfrak{P} \;\cong\; A[Y]/(f,x) \;\cong\; (A/\mathfrak{p})[Y]/(Y^p - t) \;\cong\; \mathbb{F}_p(t)[Y]/(Y^p - t).$$

The latter is a field, because, like in (a), the polynomial $Y^p - t$ is irreducible over $\mathbb{F}_p(t)$. Thus $\mathfrak{P}$ is a maximal ideal of B. Since $\mathfrak{p} \subset \mathfrak{P} \cap A$ and the former is a maximal ideal of A, it follows that $\mathfrak{p} = \mathfrak{P} \cap A$. Thus $\mathfrak{P} = B\mathfrak{p}$ is the unique prime ideal of B above $\mathfrak{p}$.

Now observe that B is an integral domain and an integral ring extension of A, because y is integral over A. Thus for any prime ideal $(0) \neq \mathfrak{P}' \subset B$ we have $(0) \neq \mathfrak{P}' \cap A$. As A is a discrete valuation ring with maximal ideal $\mathfrak{p}$, it follows that $\mathfrak{P}' \cap A = \mathfrak{p}$. By what we proved above, this implies that $\mathfrak{P}' = \mathfrak{P}$. Thus $\mathfrak{P}$ is the only non-zero prime ideal of B.

Together we now know that B is a noetherian local integral domain of Krull dimension 1 whose maximal ideal $\mathfrak{P} = Bx$ is principal. It is thus a discrete valuation ring and therefore normal, i.e., its own integral closure in L. Since it is integral over A, it is therefore the integral closure of A in L, as desired.

(d) The isomorphism $(*)$ in (c) and the fact that the polynomial $Y^p - t$ is inseparable over $\mathbb{F}_p(t)$ together imply that $k(\mathfrak{P})/k(\mathfrak{p})$ is inseparable of degree p.

*(e) After substituting $t = s^p$ we have $K' = \mathbb{F}_p(s,x)$ and $f = Y^p - x^{p-1}Y - s^p = (Y-s)^p - x^{p-1}Y$. To show that this is irreducible in $\mathbb{F}_p(s,x)[Y]$, it suffices to show that it is irreducible in $\mathbb{F}_p[s,x,Y]$. Since s, x, Y are algebraically independent over $\mathbb{F}_p$, after substituting $Y - s = Z$ it suffices to show that $Z^p - X^{p-1}Y$ is irreducible in $\mathbb{F}_p[Z,X,Y]$. As this polynomial has degree 1 with respect to the variable Y, it is irreducible in $\mathbb{F}_p(Z,X)[Y]$. Since its coefficients $Z^p, -X^{p-1} \in \mathbb{F}_p[Z,X]$ have no common divisor, by the Gauss lemma it is therefore also irreducible in $\mathbb{F}_p[Z,X,Y]$, as desired.

The same arguments as above imply that f is still separable and that $L' = K'(y)/K'$ is galois with Galois group $\mathbb{F}_p$. Thus (a) and (b) still hold for the new objects.

To obtain the analogue of (c) we substitute $y = s + \frac{x}{z}$. Then $L' = K'(z)$ and the equation $(y-s)^p = x^{p-1}y$ implies that $(\frac{x}{z})^p = x^{p-1}(s + \frac{x}{z})$ and hence $z^p + \frac{x}{s}z^{p-1} - \frac{x}{s} = 0$. Here the polynomial $Z^p + \frac{x}{s}Z^{p-1} - \frac{x}{s} \in A'[Z]$ satisfies the Eisenstein criterion for the prime $\mathfrak{p}' = (x)$. The desired statement $B'\mathfrak{p}' = \mathfrak{Q}'^p$ thus follows from exercise 3 below.

2. Consider a Dedekind ring A with quotient field K, a finite Galois extension L/K, and let B denote the integral closure of A in L. Consider a subextension K'/K which is also Galois and let A' denote the integral closure of A in K'. Consider a prime $\mathfrak{p}$ of A and a prime $\mathfrak{P} \subset B$ above $\mathfrak{p}$, such that $k(\mathfrak{P})/k(\mathfrak{p})$ is separable. Determine the decomposition of $\mathfrak{p}$ in A' with its numerical invariants r, e, f and its decomposition and inertia groups from the corresponding data in B.

Solution: Write $G' := \mathrm{Gal}(L/K')$ and $G'' := \mathrm{Gal}(K'/K) \cong G/G'$. Let $I_{\mathfrak{P}} \triangleleft G_{\mathfrak{P}} < G$ be the inertia group and the decomposition group for $\mathfrak{P}/\mathfrak{p}$. We will show how these groups determine all the desired data.

Set $\mathfrak{p}' := \mathfrak{P} \cap A'$, which is a prime of A' above $\mathfrak{p}$. Then by §6 Proposition 11 the inertia and decomposition groups for $\mathfrak{P}/\mathfrak{p}'$ are $I'_{\mathfrak{P}} := G' \cap I_{\mathfrak{P}} \triangleleft G'_{\mathfrak{P}} := G' \cap G_{\mathfrak{P}} < G'$. Let $I''_{\mathfrak{p}'} \triangleleft G''_{\mathfrak{p}'} < G''$ denote the inertia and decomposition groups for $\mathfrak{p}'/\mathfrak{p}$. Since $k(\mathfrak{P})/k(\mathfrak{p}')/k(\mathfrak{p})$ are separable field extensions, we have

$e := e_{\mathfrak{P}/\mathfrak{p}} = \lvert I_{\mathfrak{P}}\rvert$	$f := f_{\mathfrak{P}/\mathfrak{p}} = [G_{\mathfrak{P}} : I_{\mathfrak{P}}]$	$r := r_{B/\mathfrak{p}} = [G : G_{\mathfrak{P}}]$
$e' := e_{\mathfrak{P}/\mathfrak{p}'} = \lvert I'_{\mathfrak{P}}\rvert$	$f' := f_{\mathfrak{P}/\mathfrak{p}'} = [G'_{\mathfrak{P}} : I'_{\mathfrak{P}}]$	$r' := r_{B/\mathfrak{p}'} = [G' : G'_{\mathfrak{P}}]$
$e'' := e_{\mathfrak{p}'/\mathfrak{p}} = \lvert I''_{\mathfrak{p}'}\rvert$	$f'' := f_{\mathfrak{p}'/\mathfrak{p}} = [G''_{\mathfrak{p}'} : I''_{\mathfrak{p}'}]$	$r'' := r_{A'/\mathfrak{p}} = [G'' : G''_{\mathfrak{p}'}]$

where $r_{../..}$ denotes the number of primes of .. above ... Since $I'_{\mathfrak{P}}$ and $G'_{\mathfrak{P}}$ are already given by explicit formulas, a complete answer follows from the descriptions:

(a) $G''_{\mathfrak{p}'} = G_{\mathfrak{P}}G'/G' \cong G_{\mathfrak{P}}/G'_{\mathfrak{P}}$.

(b) $I''_{\mathfrak{p}'} = I_{\mathfrak{P}}G'/G' \cong I_{\mathfrak{P}}/I'_{\mathfrak{P}}$.

In both statements the last isomorphism results from the first isomorphism theorem. To prove (a) note that $G_{\mathfrak{P}}$ stabilizes $\mathfrak{P}$ and A' and hence also $\mathfrak{p}' := \mathfrak{P} \cap A'$. Thus its image $G_{\mathfrak{P}}G'/G'$ in $G/G' \cong \mathrm{Gal}(K'/K)$ is contained in $G''_{\mathfrak{p}'}$. It follows that

$$e''f'' \;=\; |G''_{\mathfrak{p}'}| \;\geqslant\; |G_{\mathfrak{P}}G'/G'| \;=\; |G_{\mathfrak{P}}/G'_{\mathfrak{P}}| \;=\; \frac{|G_{\mathfrak{P}}|}{|G'_{\mathfrak{P}}|} \;=\; \frac{ef}{e'f'}.$$

Since $e = e'e''$ and $f = f'f''$, this inequality must be an equality; hence so is the inclusion $G_{\mathfrak{P}}G'/G' \subset G''_{\mathfrak{p}'}$, proving (a).

Likewise, for (b) observe that $I_{\mathfrak{P}}$ acts trivially on the residue field $k(\mathfrak{P})$ and hence also on the subfield $k(\mathfrak{p}')$. Thus its image $I_{\mathfrak{P}}G'/G'$ in $G/G' \cong \mathrm{Gal}(K'/K)$ is contained in $I''_{\mathfrak{p}'}$. It follows that

$$e'' \;=\; |I''_{\mathfrak{p}'}| \;\geqslant\; |I_{\mathfrak{P}}G'/G'| \;=\; |I_{\mathfrak{P}}/I'_{\mathfrak{P}}| \;=\; \frac{|I_{\mathfrak{P}}|}{|I'_{\mathfrak{P}}|} \;=\; \frac{e}{e'}.$$

Since again $e = e'e''$, the inclusion $I_{\mathfrak{P}}G'/G' \subset I''_{\mathfrak{p}'}$ must be an equality, proving (b).

3. Consider a Dedekind ring A with quotient field K, a finite separable extension L/K, and let B denote the integral closure of A in L. Assume that $L = K(\alpha)$, where the minimal polynomial $f(X) = X^n + \sum_{i=0}^{n-1} a_i X^i$ of α over K lies in $A[X]$ and is *Eisenstein at* a prime ideal $\mathfrak{p}$ of A, that is, all $a_i \in \mathfrak{p}$ and $a_0 \notin \mathfrak{p}^2$. Show that $\mathfrak{p}B = \mathfrak{P}^n$ with $\mathfrak{P} := \mathfrak{p}B + \alpha B$ prime, so that $\mathfrak{p}$ is totally ramified in B.

(*Hint:* Prove that $\mathfrak{p}B \subset \mathfrak{P}^j$ for all $j \leqslant n$ by induction on j.)

Solution: Since $f(\alpha) = 0$, the element α is integral over A and hence lies in B. Thus $\mathfrak{P}$ is an ideal of B.

We first claim that $\mathfrak{p}B \subset \mathfrak{P}^n$. For this note that $\mathfrak{p}B \subset \mathfrak{P}$ by construction. Suppose that $\mathfrak{p}B \subset \mathfrak{P}^j$ for some integer $1 \leqslant j < n$. Then we have $\alpha^n \in \mathfrak{P}^n \subset \mathfrak{P}^{j+1}$, and for all $0 < i < n$ we have $a_i\alpha^i \in \mathfrak{p}\mathfrak{P}^i \subset \mathfrak{P}^{j+1}$. The equation $f(\alpha) = 0$ thus implies that $a_0 \in \mathfrak{P}^{j+1}$. But since $a_0 \in \mathfrak{p} \setminus \mathfrak{p}^2$, we have $\mathfrak{p} = a_0A + \mathfrak{p}^2$; hence $\mathfrak{p}B = a_0B + \mathfrak{p}^2B \subset \mathfrak{P}^{j+1} + (\mathfrak{P}^j)^2 = \mathfrak{P}^{j+1}$. By induction on j this proves the claim.

In particular, the claim implies that $\mathfrak{P}^n \neq B$ and hence $\mathfrak{P} \neq B$. Thus $\mathfrak{P}$ is contained in some prime ideal $\mathfrak{P}' \subset B$. Write $\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ with distinct prime ideals $\mathfrak{P}_i$, exponents $e_i > 0$, and residue degrees f_i. Then $\sum_{i=1}^r e_i f_i = n$. Since $\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r} = \mathfrak{p}B \subset \mathfrak{P}^n \subset \mathfrak{P}'^n$ and $\mathfrak{P}'$ is prime, this leaves only the possibility that $r = 1$ and $e_1 = n$ and $\mathfrak{P}_1^n = \mathfrak{p}B = \mathfrak{P}^n = \mathfrak{P}'^n$. Therefore $\mathfrak{P} = \mathfrak{P}'$ and this ideal is prime.

Remark: If we knew that $B = A[\alpha]$, we could directly compute that $B \cong A[X]/(f)$ and hence $B/\mathfrak{p}B \cong (A/\mathfrak{p})[X]/(X^n)$, whence the prime decomposition $\mathfrak{p}B = \mathfrak{P}^n$. But in general we do not have $B = A[\alpha]$, for instance, because the assumptions do not change on replacing α by $a\alpha$ for an arbitrary $a \in A \setminus \mathfrak{p}$. However, one can prove that $B_\mathfrak{p} = A_\mathfrak{p}[\alpha]$ in this case.

4. Let L/K be a Galois extension of number fields with noncyclic Galois group.

   (a) Show that any prime ideal of $\mathcal{O}_K$ over which lies only one prime ideal of $\mathcal{O}_L$ is ramified in $\mathcal{O}_L$.

   (b) Deduce that there are at most finitely many prime ideals with the property in (a), and in particular no prime ideals of $\mathcal{O}_K$ that are totally inert in $\mathcal{O}_L$.

   Solution:

   (a) Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ over which lies only one prime ideal $\mathfrak{P}$ of $\mathcal{O}_L$. Then the decomposition group at $\mathfrak{P}$ is equal to $\mathrm{Gal}(L/K)$, so we have a short exact sequence

   $$1 \to I_\mathfrak{P} \to \mathrm{Gal}(L/K) \to \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p})) \to 1.$$

   Since $k(\mathfrak{p})$ is a finite field, the group $\mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$ is cyclic; hence it is not isomorphic to $\mathrm{Gal}(L/K)$. Thus the inertia group $I_\mathfrak{P}$ is not trivial. By §6 Proposition 10, it follows that $e = |I_\mathfrak{P}| > 1$, as desired.

   (b) By (a), every such prime is ramified. Hence, there are no totally inert primes. Since, by §7 Corollary 14, there are only finitely many ramified primes, there are only finitely many primes with the property from (a).

   Note: The Cebotarev density theorem implies that for any finite Galois extension $K/\mathbb{Q}$ with group G and any element $g \in G$, there exist infinitely many rational

primes p such that the Frobenius element associated to some prime above p is equal to g. In fact, the theorem says specifically that for any real number x, the proportion of primes $p \leqslant x$ with the above property tends to $|\operatorname{Cent}_G(g)|^{-1}$ for $x \to \infty$.

5. For $K := \mathbb{Q}(\sqrt[3]{2})$ compute the prime factorization of the different $\operatorname{diff}_{\mathcal{O}_K/\mathbb{Z}}$ and verify that a prime ideal of $\mathcal{O}_K$ divides $\operatorname{diff}_{\mathcal{O}_K/\mathbb{Z}}$ if and only if it is ramified over $\mathbb{Z}$.

   Solution: By the solution of exercise 3 on sheet 1 we have $\mathcal{O}_K = \mathbb{Z}[\alpha]$ with $\alpha := \sqrt[3]{2}$. The minimal polynomial of α over $\mathbb{Q}$ is $f(X) := X^3 - 2$; hence by §7 Proposition 3 we have

$$\operatorname{diff}_{\mathcal{O}_K/\mathbb{Z}} = \left(\tfrac{df}{dX}(\alpha)\right) = \left(3\alpha^2\right).$$

   In the solution of exercise 5 on sheet 5, we calculated that $\mathcal{O}_K/2\mathcal{O}_K \cong \mathbb{F}_2[X]/(X)^3$ and $\mathcal{O}_K/3\mathcal{O}_K \cong \mathbb{F}_3[X]/(X-2)^3$. Therefore $2\mathcal{O}_K = \mathfrak{p}_2^3$ and $3\mathcal{O}_K = \mathfrak{p}_3^3$ for the prime ideals $\mathfrak{p}_2 := (2, \alpha) = (\alpha)$ and $\mathfrak{p}_3 := (3, \alpha - 2)$. The prime factorization of the different is therefore $\operatorname{diff}_{\mathcal{O}_K/\mathbb{Z}} = \mathfrak{p}_3^3\mathfrak{p}_2^2$.

   In particular, the primes $\mathfrak{p}_2$ and $\mathfrak{p}_3$ are totally ramified over $\mathbb{Z}$ and divide the different. Any other prime $\mathfrak{p}$ of $\mathcal{O}_K$ lies over a rational prime $p \neq 2, 3$. The polynomial $f(X) = X^3 - 2$ is then separable modulo p. Thus its decomposition in $\mathbb{F}_p[X]$ has no multiple factors, and so all exponents in the prime factorization of $p\mathcal{O}_K$ are 1. (Compare again the solution of exercise 5 on sheet 5). Thus $\mathfrak{p}$ is unramified over $\mathbb{Z}$ and does not divide the different. Together this shows that a prime of $\mathcal{O}_K$ is ramified over $\mathbb{Z}$ if and only if it divides $\operatorname{diff}_{\mathcal{O}_K/\mathbb{Z}}$.