Solutions 11

Extensions of Complete Absolute Values

1. (a) Show that $X^3 - X^2 - 2X - 8$ is irreducible in $\mathbb{Q}[X]$ but splits completely in $\mathbb{Q}_2[X]$.

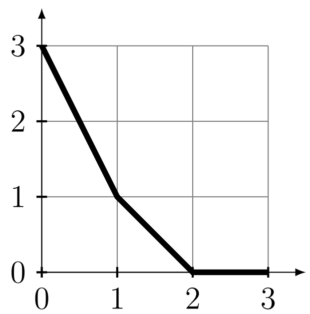
   (b) Find two monic polynomials of degree 3 in $\mathbb{Q}_5[X]$ with the same Newton polygons, but one irreducible and the other not.

   (c) Hensel's lemma concerns a polynomial f with a factorization $(f \bmod \mathfrak{p}) = \bar{g}\bar{h}$ such that $\bar{g}$ and $\bar{h}$ are coprime. Show by a counterexample that the assumption 'coprime' is necessary.

Solution:

(a) The polynomial is irreducible in $\mathbb{Z}[X]$, as any integer root would have to divide the constant coefficient 8, but $\pm 1, \pm 2, \pm 4, \pm 8$ are no roots. By the Gauss lemma the polynomial is irreducible in $\mathbb{Q}[X]$.

The Newton polygon with respect to ord_2 has the three distinct slopes $2, 1, 0$. By §12 Corollary 8 it splits completely over $\mathbb{Q}_2$. The following drawing shows the Newton polygon of the given polynomial:



(b) The Newton polygon of both polynomials $f(X) := X^3 + X^2 + X + 1$ and $g(X) := X^3 + X^2 + X - 1$ is the horizontal straight line between $(0, 0)$ and $(3, 0)$. The first polynomial is reducible as $f(-1) = 0$, while g is irreducible in $\mathbb{Q}_5[X]$, as its reduction modulo 5 has degree 3 and is irreducible in $\mathbb{F}_5[X]$.

(c) Let K be a complete non-archimedean field such that $\mathcal{O}_K$ is a discrete valuation ring, for example $K = \mathbb{Q}_p$ for any prime number $p < \infty$. Let $\pi \in \mathcal{O}_K$ be a uniformizer. Then $f(X) := X^2 - \pi$ is irreducible by the Eisenstein criterion and $\bar{g}(X) = \bar{h}(X) = X$ with $(f \bmod (\pi)) = \bar{g}\bar{h}$ is a factorization modulo (π).

2. Prove that every finite extension of $\mathbb{C}((t))$ of degree n is isomorphic to $\mathbb{C}((s))$ where $s^n = t$.

   Solution: Note that $\mathbb{C}((t))$ is a complete non-archimedean field with respect to the discrete valuation defined by $v(a_k t^k + a_{k+1} t^{k+1} + \dots) := k$ if $a_k \neq 0$ and $v(0) = +\infty$, and its valuation ring is $\mathcal{O}_{\mathbb{C}((t))} = \mathbb{C}[[t]]$. Let L be a finite extension of $\mathbb{C}((t))$ of degree n. Since the residue field $\mathbb{C}$ of $\mathbb{C}[[t]]$ is algebraically closed, the extension of residue fields is trivial. Thus L is totally ramified over $\mathbb{C}((t))$. For any uniformizer $\pi \in \mathcal{O}_L$, that is, any generator of the maximal ideal of $\mathcal{O}_L$, we therefore have $(\pi)^n = t\mathcal{O}_L$ and hence $\pi^n/t \in \mathcal{O}_L^\times$. Consider the polynomial $f(X) := X^n - \frac{\pi^n}{t} \in \mathcal{O}_L[X]$. Since π^n/t is a unit, it is nonzero $\operatorname{mod}(\pi)$. As the residue field $\mathbb{C}$ of $\mathcal{O}_L$ is algebraically closed of characteristic zero, it follows that $f \operatorname{mod}(\pi)$ has a simple root. By Hensel's lemma this root can be lifted to a root $u \in \mathcal{O}_L$ of f. This u is a unit, because $u^n = \pi^n/t$ is a unit. Setting $s := \pi/u \in \mathcal{O}_L$, we deduce that $s^n = t$. Finally observe that s is a root of the polynomial $X^n - t$ over $\mathbb{C}[[t]]$, which is irreducible by the Eisenstein criterion. Thus $\mathbb{C}((s)) \subset L$ is a subfield of degree n over $\mathbb{C}((t))$, and therefore $\mathbb{C}((s)) = L$, as desired.

3. Let K be a non-archimedean complete field such that $\mathcal{O}_K$ is a discrete valuation ring. Prove that for every finite extension L/K with separable residue field extension there exists $\alpha \in L$ such that $\mathcal{O}_L = \mathcal{O}_K[\alpha]$.

   Solution: See Lemma 10.4 in Chapter II of Neukirch (page 178) or Theorem 10.15 in the following notes by Sutherland:
   `http://math.mit.edu/classes/18.785/2016fa/LectureNotes10.pdf`

4. *(Krasner's lemma)* Let K be a field that is complete for a non-archimedean absolute value $|\ |$. Let $|\ |$ also denote the unique extension to an algebraic closure $\bar{K}$. Consider an element $\alpha \in \bar{K}$ that is separable over K, and let $\alpha = \alpha_1, \dots, \alpha_n$ be its Galois conjugates over K. Consider an element $\beta \in \bar{K}$ such that

   $$|\alpha - \beta| < |\alpha - \alpha_i|$$

   for all $2 \leqslant i \leqslant n$. Show that $K(\alpha) \subseteq K(\beta)$.

   Hint: Let M be the Galois closure of the extension $K(\alpha, \beta)/K(\beta)$ and consider the action of $\operatorname{Gal}(M/K(\beta))$ on α.

   Solution: See Lemma 8.1.6 on page 429 of [J. Neukirch, A. Schmidt, K. Wingberg: Cohomology of number fields. Second edition. Grundlehren der Mathematischen Wissenschaften. Springer-Verlag, Berlin, 2008].

*5. Consider an integer $n \geqslant 1$ and a finite set S of rational primes $p \leqslant \infty$ (allowing $\mathbb{Q}_\infty = \mathbb{R}$). For each $p \in S$ consider field extensions $L_{p,i}/\mathbb{Q}_p$ for $1 \leqslant i \leqslant r_p$ such that $\sum_{i=1}^{r_p} [L_{p,i}/\mathbb{Q}_p] = n$. Show that there exists a number field L of degree n over $\mathbb{Q}$ such that for every $p \in S$ we have $L \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong \prod_{i=1}^{r_p} L_{p,i}$.

   Hint: Use Krasner's lemma (exercise 4) or adapt it suitably.

Solution: As a preparation consider an arbitrary field K with absolute value $|\ |$. We extend this absolute value to polynomials by defining $|\sum' b_j X^j| := \max\{|b_j|\}$. This induces a metric on $K[X]$. Convergence of polynomials of a fixed degree is equivalent to convergence of the coefficients.

Lemma 1. *Assume that K is algebraically closed. Let $f \in K[X]$ be a monic polynomial of degree n with roots $\alpha_1, \ldots, \alpha_n \in K$. Then for any $\varepsilon > 0$ there exists $\delta > 0$ such that for any monic polynomial $g \in K[X]$ of degree n with $|g - f| < \delta$, the roots $\beta_i \in K$ of g can be numbered in such a way that $|\alpha_i - \beta_i| < \varepsilon$ for all i.*

Proof. The assertion is equivalent to saying that for any sequence (f_k) of monic polynomials of degree n in $K[X]$ with $\lim_{k\to\infty} f_k = f$, the roots $\alpha_{k,i} \in K$ of the f_k can be numbered in such a way that $\lim_{k\to\infty} \alpha_{k,i} = \alpha_i$ for all i. In the archimedean case, this is for example Proposition 5.2.1 on page 138 in [M. Artin: Algebra. Second edition. Pearson Education, Harlow, 2011]. The proof for the non-archimedean case works analogously. $\square$

Lemma 2. *Assume that K is complete. Let $f \in K[X]$ be a monic separable polynomial of degree n. Then there exists $\delta > 0$ such that for any monic polynomial $g \in K[X]$ of degree n with $|g - f| < \delta$ we have $K[X]/(g) \cong K[X]/(f)$.*

Proof. Let $\bar{K}$ be an algebraic closure of K, endowed with the unique extension of the absolute value. Let $\alpha_1, \ldots, \alpha_n \in \bar{K}$ denote the roots of f. Let $\delta > 0$ be the constant obtained from Lemma 1 for $f \in \bar{K}[X]$ and $\varepsilon := \min\{|\alpha_i - \alpha_j| : i \neq j\}/2$. Let $g \in K[X]$ be any monic polynomial of degree n with $|g - f| < \delta$ and let $\beta_1, \ldots, \beta_n \in \bar{K}$ be the roots of g ordered in such a way that $|\alpha_i - \beta_i| < \varepsilon$ for all i.

Then for all $i \neq j$ we have $|\alpha_i - \beta_j| \geqslant |\alpha_i - \alpha_j| - |\alpha_j - \beta_j| > 2\varepsilon - \varepsilon = \varepsilon > |\alpha_i - \beta_i|$ and hence $\beta_j \neq \beta_i$. Therefore g is also separable. Moreover, any automorphism $\sigma \in \mathrm{Aut}_K(\bar{K})$ preserves the absolute value on $\bar{K}$ and permutes the α_i and independently the β_i. Thus for any indices i, j, k with $\sigma(\alpha_i) = \alpha_j$ and $\sigma(\beta_i) = \beta_k$, we have $|\alpha_j - \beta_k| = |\sigma(\alpha_i) - \sigma(\beta_i)| = |\alpha_i - \beta_i| < \varepsilon$ and hence $|\alpha_j - \alpha_k| \leqslant |\alpha_j - \beta_k| + |\alpha_k - \beta_k| < 2\varepsilon$. By the choice of ε this implies that $j = k$. Thus $\mathrm{Aut}_K(\bar{K})$ permutes the α_i in the same way as the β_i. Since all α_i and β_i are separable over K, it follows in particular that $K(\alpha_i) = K(\beta_i)$ for all i. (*Remark:* One can also deduce this from Krasner's lemma, but this direct proof, inspired by the proof of Krasner's lemma, is more efficient.)

Let $f = \prod_{\nu=1}^r f_\nu$ be the factorization of f into distinct monic irreducible polynomials. Then the roots of the different f_ν are precisely the $\mathrm{Aut}_K(\bar{K})$-orbits in $\{\alpha_1, \ldots, \alpha_n\}$. The corresponding orbits in $\{\beta_1, \ldots, \beta_n\}$ are thus the roots of the different g_ν for the factorization of g into distinct monic irreducible polynomials $g = \prod_{\nu=1}^r g_\nu$. For each ν choose i_ν such that α_{i_ν} is a root of f_ν. Then f_ν is the minimal polynomial of α_{i_ν} over K, and g_ν is the minimal polynomial of β_{i_ν} over K. Using the Chinese Remainder Theorem we now conclude that

$$\begin{array}{ccccc} K[X]/(f) & \cong & \prod_{\nu=1}^r K[X]/(f_\nu) & \cong & \prod_{\nu=1}^r K(\alpha_{i_\nu}) \\ & & & & \wr\| \\ K[X]/(g) & \cong & \prod_{\nu=1}^r K[X]/(g_\nu) & \cong & \prod_{\nu=1}^r K(\beta_{i_\nu}) \end{array}$$

as desired. $\square$

In the given situation let us first fix $p \in S$. As each extension $L_{p,i}/\mathbb{Q}_p$ is finite separable, we can write $L_{p,i} = \mathbb{Q}_p(\alpha_{p,i})$ for some $\alpha_{p,i} \in L_{p,i}$. Let $f_{p,i}$ denote the minimal polynomial of $\alpha_{p,i}$ over $\mathbb{Q}_p$. After possibly replacing $\alpha_{p,i}$ by $\alpha_{p,i} + \gamma_{p,i}$ for some $\gamma_{p,i} \in \mathbb{Q}_p$ we may assume that the $f_{p,i}$ are pairwise inequivalent. Then $f_p := \prod_{i=1}^{r_p} f_{p,i} \in \mathbb{Q}_p[X]$ is separable monic of degree n, and by the Chinese remainder theorem we have $\mathbb{Q}_p[X]/(f_p) \cong \prod_{i=1}^{r_p} L_{p,i}$.

Let $\delta > 0$ be the constant given by Lemma 2 for the polynomial $f_p \in \mathbb{Q}_p[X]$. Since S is finite, we can choose δ independent of $p \in S$. As $\mathbb{Q}$ is dense in $\mathbb{Q}_p$, we can take a polynomial $g_p \in \mathbb{Q}[X]$ with $|g_p - f_p|_p < \delta/2$. By applying the approximation theorem in §10 Proposition 7 of the lecture course coefficientwise, we can then find a monic polynomial $f \in \mathbb{Q}[X]$ of degree n such that $|f - g_p|_p < \delta/2$ for all $p \in S$. By the triangle inequality we then have $|f - f_p|_p < \delta$ for all $p \in S$.

Set $L := \mathbb{Q}[X]/(f)$, which is a $\mathbb{Q}$-algebra of dimension n. By construction and Lemma 2, for every $p \in S$ we then have

$$L \otimes_{\mathbb{Q}} \mathbb{Q}_p \;\cong\; \mathbb{Q}_p[X]/(f) \;\cong\; \mathbb{Q}_p[X]/(f_p) \;\cong\; \prod_{i=1}^{r_p} L_{p,i}.$$

Thus we are done if L is a field. This is the case if $r_p = 1$ for some $p \in S$, because then L embeds into the field $L_{p,1}$. In general we can always add a new prime number ℓ to S with $r_\ell = 1$ and a field extension $L_{\ell,1}/\mathbb{Q}_\ell$ of degree n; achieving again that L is a field.