Solutions 18

Newton Polygons, Extensions of Absolute Values

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

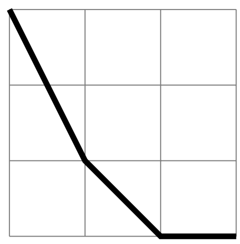
   (b) Find two monic polynomials of degree 3 in $\mathbb{Q}_5[X]$ with the same Newton polygons, but one irreducible and the other not.

   (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) Since the polynomial is monic, any rational root would be an integer that divides the constant coefficient 8, but $\pm 1, \pm 2, \pm 4, \pm 8$ are no roots. Thus the polynomial has no linear factor, and being of degree 3 it is therefore irreducible in $\mathbb{Q}[X]$.

The Newton polygon with respect to ord_2 has the three distinct slopes $2, 1, 0$. By Proposition 9.3.5 from the lecture the polynomial therefore splits completely over $\mathbb{Q}_2$. The following drawing shows the Newton polygon:



(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, that is a generator of the maximal ideal of $\mathcal{O}_K$. 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. *(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 $\alpha = \alpha_1, \ldots, \alpha_n$ 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 $\mathrm{Gal}(M/K(\beta))$ 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].

*3. Consider an integer $n \geqslant 1$ and a finite set S of rational primes $p \leqslant \infty$ (including $\mathbb{Q}_\infty = \mathbb{R}$). 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 from above 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. □

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. □

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 Prop 9.5.1 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.

4. Let L/K be a purely inseparable finite extension of degree q. Show that every absolute value $|\ |$ on K possesses a unique extension to L, given by the formula

$$|y| \ := \ |y^q|^{1/q}.$$

Solution: By assumption, for every $y \in L$ we have $y^q \in K$. Thus any extension $\|\ \|$ of the absolute value must satisfy $\|y\|^q = \|y^q\| = |y^q|$, so it is given by the indicated formula.

The converse is trivial if $q = 1$. Otherwise K has characteristic > 0, so the given absolute value on it is non-archimedean. Thus $|\ |^{1/q}$ is again an absolute value on K, and so is its pullback under the homomorphism $L \hookrightarrow K$, $y \mapsto y^q$.

*5. Let L/K be a finite field extension and let $|\ |$ be a (nontrivial) absolute value on L. Show that the restriction of $|\ |$ to K is nontrivial.

(*Hint:* Use Newton polygons.)

Solution: Suppose that the restriction of $|\ |$ to K is trivial. Then $|n \cdot 1_K| \leqslant 1$ for all integers n; hence the absolute value is non-archimedean. Write $|x| = c^{-v(x)}$ for $c > 1$ and a valuation $v\colon L \to \mathbb{R} \cup \{\infty\}$. Choose $y \in L$ with $|y| \neq 0, 1$. Let $f(X) = \sum_{i=0}^{n} a_i X^i$ be its minimal polynomial over K. Then $a_n = 1$, and $y \neq 0$ implies that $a_0 \neq 0$. Thus $v(a_n) = v(a_0) = 0$, and since $v|K$ is trivial, we have $v(a_i) \in \{0, \infty\}$ for all $1 \leqslant i \leqslant n$. Thus the Newton polygon of f is a horizontal straight line segment.

By Proposition 9.3.4 of the lecture course it follows that $v(y) = 0$. Thus $|y| = 1$, contrary to the assumption.

6. (a) Determine all the absolute values on $\mathbb{Q}(\sqrt{5}\,)$.
   (b) How many extensions to $\mathbb{Q}(\sqrt[n]{2}\,)$ does the archimedean absolute value on $\mathbb{Q}$ admit?

Solution: (a) Every absolute value on $\mathbb{Q}(\sqrt{5}\,)$ is an extension of an absolute value on $\mathbb{Q}$. The restriction to $\mathbb{Q}$ is nontrivial by exercise 5 above. Up to equivalence, the absolute values on $\mathbb{Q}$ are precisely the $|\ |_p$ for primes p including the archimedean case $p = \infty$. We distinguish the case when $X^2 - 5$ splits in $\mathbb{Q}_p[X]$ and the case when it is irreducible.

If $X^2 - 5$ splits over $\mathbb{Q}_p$, then $\mathbb{Q}(\sqrt{5}\,) \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong \mathbb{Q}_p \times \mathbb{Q}_p$ and the extensions of $|\ |_p$ are the pullbacks of the absolute value on $\mathbb{Q}_p$ under the two embeddings $\mathbb{Q}(\sqrt{5}\,) \hookrightarrow \mathbb{Q}_p$.

Letting $\pm\alpha$ denote the roots of $X^2 - 5$ in $\mathbb{Q}_p$, the extensions of $|\ |_p$ are therefore given by $|a + b\sqrt{5}| := |a \pm b\alpha|_p$.

If $X^2 - 5$ is irreducible over $\mathbb{Q}_p$, then $\mathbb{Q}(\sqrt{5}\,) \otimes_{\mathbb{Q}} \mathbb{Q}_p$ is a field and there is a unique extension of $|\ |_p$ to $\mathbb{Q}(\sqrt{5}\,)$, which is the pullback of the unique extension of the absolute value of $\mathbb{Q}_p$ to $\mathbb{Q}_p[X]/(X^2-5)$. By Proposition 9.2.4 of the lecture course, it is given by $|a + b\sqrt{5}| := \sqrt{|\operatorname{Norm}_{\hat{L}/\mathbb{Q}_p}(a + b\sqrt{5})|_p} = \sqrt{|a^2 - 5b^2|_p}$.

It remains to determine the $p \leqslant \infty$ for which $X^2 - 5$ splits. Since $\sqrt{5} \in \mathbb{R}$, it splits for $p = \infty$. Since 5 is not a square modulo 2^3, it follows that $X^2 - 5$ does not split over $\mathbb{Z}_2$ and hence neither over $\mathbb{Q}_2$ as $\mathbb{Z}_2$ is normal. Furthermore $X^2 - 5$ is irreducible over $\mathbb{Z}_5$ by the Eisenstein criterion and hence it does not split over $\mathbb{Q}_5$.

For $p \notin \{2, 5, \infty\}$ it follows from Hensel's lemma that $X^2 - 5$ splits if and only if it splits over $\mathbb{F}_p$. This is so if and only if the Legendre symbol $\left(\frac{5}{p}\right)$ is 1. By quadratic reciprocity that is equal to $\left(\frac{p}{5}\right)$, which is 1 if and only if $p \equiv \pm 1$ modulo (5).

(b) The number $\sqrt[n]{2}$ is a root of the polynomial $X^n - 2$, which is irreducible over $\mathbb{Q}$ by the Eisenstein criterion for the prime 2. Thus $X^n - 2$ is the minimal polynomial of $\sqrt[n]{2}$ over $\mathbb{Q}$.

If n is even, it has 2 roots in $\mathbb{R}$ and $\frac{n-2}{2}$ pairs of complex conjugate roots in $\mathbb{C} \setminus \mathbb{R}$. In that case we thus have $\mathbb{Q}(\sqrt[n]{2}\,) \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^2 \times \mathbb{C}^{\frac{n-2}{2}}$ and hence $2 + \frac{n-2}{2} = \frac{n+2}{2}$ distinct extensions.

If n is odd, the polynomial $X^n - 2$ has 1 root in $\mathbb{R}$ and $\frac{n-1}{2}$ pairs of complex conjugate roots in $\mathbb{C} \setminus \mathbb{R}$. In that case thus we have $\mathbb{Q}(\sqrt[n]{2}\,) \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R} \times \mathbb{C}^{\frac{n-1}{2}}$ and hence $1 + \frac{n-1}{2} = \frac{n+1}{2}$ distinct extensions.