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

Solutions 12

Extensions of Absolute Values, Local and Global Fields

1. 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

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

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. Conversely, since K has characteristic > 0, the given absolute value on it is non-archimedean, hence $|\ |^{1/q}$ is again an absolute value on K, and so is its pullback under the homomorphism $L \hookrightarrow K$, $y \mapsto y^q$.

*2. 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 7 of §12 of the lecture course (which does not assume that the absolute value is complete or non-trivial) it follows that $v(y) = 0$. Thus $|y| = 1$, contrary to the assumption.

3. (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 2 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 §12 Theorem 4, it is given by $|a + b\sqrt{5}| := \sqrt{|\operatorname{Nm}_{\hat{L}/\mathbb{Q}_p}(a + b\sqrt{5})|_p} = \sqrt{|a^2 - 5b^2|_p}$.

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 $\mathbb{C} \smallsetminus \mathbb{R}$. 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 $\mathbb{C} \smallsetminus \mathbb{R}$. 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.

4. Let p be a prime number and $\bar{\mathbb{Q}}$ an algebraic closure of $\mathbb{Q}$.

   (a) Show that $|\ |_p$ extends to some absolute value $|\ |$ on $\bar{\mathbb{Q}}$.

   (b) For any subfield $K \subset \bar{\mathbb{Q}}$ which is finite over $\mathbb{Q}$ let $\hat{K}$ be the completion of K with respect to the restriction of $|\ |$. Show that for any subfields $K \subset L \subset \bar{\mathbb{Q}}$ which are finite over $\mathbb{Q}$ we get a natural inclusion $\hat{K} \hookrightarrow \hat{L}$.

   (c) Show that the union $\bar{\mathbb{Q}}_p$ of all these $\hat{K}$ is an algebraic closure of $\mathbb{Q}_p$.

   (d) Show that there is a natural isomorphism
   $$\operatorname{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p) \xrightarrow{\sim} \operatorname{Stab}_{\operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})}(|\ |).$$

Solution:

(a) Let $\bar{\mathbb{Q}}_p$ be any algebraic closure of $\mathbb{Q}_p$. Then the p-adic absolute value on $\mathbb{Q}_p$ possesses a unique extension to $\bar{\mathbb{Q}}_p$. Since $\bar{\mathbb{Q}}_p$ is algebraically closed, the embedding $\mathbb{Q} \hookrightarrow \bar{\mathbb{Q}}_p$ extends to some embedding $\bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_p$. The pullback of the absolute value on $\bar{\mathbb{Q}}_p$ under this embedding yields the desired extension.

Aliter: For any finite extension $K/\mathbb{Q}$, there exists an extension of $| \ |_p$ to K. Construct the desired extension to $\bar{\mathbb{Q}}$ using Zorn's lemma.

(b) Any Cauchy sequence in K is also a Cauchy sequence in L, as the absolute value on K is the restriction of the absolute value on L. Hence we obtain an inclusion of metric spaces $\hat{K} \hookrightarrow \hat{L}$. It follows directly from the definition of addition and multiplication for the completion that this inclusion respects the field structure.

(c) The natural inclusions $\hat{K} \hookrightarrow \hat{L}$ are compatible with each other; hence we can form the union $M := \varinjlim \hat{K}$. Since each $\hat{K}$ is finite over $\mathbb{Q}_p$, this M is algebraic over $\mathbb{Q}_p$. We claim that it is algebraically closed.

For this consider any finite extension $\tilde{K}/\mathbb{Q}_p$. Then $\tilde{K}$ is a local field, so by exercise 6 below it is the completion of a global field K at an absolute value $| \ |$. Since $\mathbb{Q} \subset \mathbb{Q}_p \subset \tilde{K}$, we also have $\mathbb{Q} \subset K$; so K is finite extension of $\mathbb{Q}$. Also, the restriction of $| \ |$ to $\mathbb{Q}$ is the restriction of the usual absolute value on $\mathbb{Q}_p$ and hence equal to $| \ |_p$.

(*Aliter:* Consider any irreducible monic polynomial $f \in \mathbb{Q}_p[X]$ with roots $x = x_1, x_2, \ldots, x_n \in \bar{\mathbb{Q}}_p$. As in the solution of exercise 5 of sheet 11, we can choose a monic polynomial $g \in \mathbb{Q}[X]$ of degree n that is coefficientwise close to f and has a root y in M such that $|y - x| < \min\{|x - x_i| : 2 \leqslant i \leqslant n\}$. Krasner's lemma (exercise 4 of sheet 11) then implies that $\mathbb{Q}_p(x) \subset \mathbb{Q}_p(y)$. Thus $\mathbb{Q}_p(x)$ lies in the completion of the number field $K := \mathbb{Q}(y)$ at an absolute value $| \ |$ extending the p-adic absolute value on $\mathbb{Q}$.)

Let L be a galois closure of K over $\mathbb{Q}$. Then $\mathrm{Gal}(L/\mathbb{Q})$ acts transitively on the set of primes of $\mathcal{O}_L$ above p and hence also on the set of extensions of $| \ |_p$ to L. Any such extension thus arises from the extension to $\bar{\mathbb{Q}}$ in (a) via some embedding $L \hookrightarrow \bar{\mathbb{Q}}$. After extending our given absolute value $| \ |$ on K to L, this therefore arises from the extension to $\bar{\mathbb{Q}}$ in (a) via some embedding $K \hookrightarrow \bar{\mathbb{Q}}$. For this embedding we then have $\tilde{K} = \hat{K} \subset M$. Varying $\tilde{K}$ this proves that M is algebraically closed. In particular we have a natural equality $M = \bar{\mathbb{Q}}_p$.

(d) First consider any finite extension $K \subset \bar{\mathbb{Q}}$ which is galois over $\mathbb{Q}$ with galois group G. Then by §13 Proposition 6, the pullback of $| \ |_p$ via $K \hookrightarrow \bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_p$ corresponds to a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ above p, and by §13 Proposition 8 the extension $\hat{K}/\mathbb{Q}_p$ is galois with galois group $G_\mathfrak{p} = \mathrm{Stab}_G(\mathfrak{p})$. By the natural bijection between primes above p and extensions of the absolute value this subgroup is equal to $\mathrm{Stab}_G(| \ |_p|_K)$.

For any two finite extensions $K \subset K' \subset \bar{\mathbb{Q}}$ that are galois over $\mathbb{Q}$ we have a natural surjection $\mathrm{Gal}(K'/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(K/\mathbb{Q})$. Moreover, if $\mathfrak{p} \subset \mathcal{O}_K$ and $\mathfrak{p}' \subset \mathcal{O}_{K'}$ are the primes above p associated to the respective pullbacks of $| \ |_p$, then $\mathfrak{p}'$ lies above $\mathfrak{p}$, and by the solution of exercise 2 of sheet 2 we obtain a natural commutative diagram with vertical surjections

$$\begin{array}{ccccccc}
\mathrm{Gal}(\hat{K}'/\mathbb{Q}_p) & \cong & \mathrm{Stab}_{\mathrm{Gal}(K'/\mathbb{Q})}(\mathfrak{p}') & = & \mathrm{Stab}_{\mathrm{Gal}(K'/\mathbb{Q})}(|\ |_p|_{K'}) & \subset & \mathrm{Gal}(K'/\mathbb{Q}) \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
\mathrm{Gal}(\hat{K}/\mathbb{Q}_p) & \cong & \mathrm{Stab}_{\mathrm{Gal}(K/\mathbb{Q})}(\mathfrak{p}) & = & \mathrm{Stab}_{\mathrm{Gal}(K/\mathbb{Q})}(|\ |_p|_{K}) & \subset & \mathrm{Gal}(K/\mathbb{Q}).
\end{array}$$

As K varies over all finite extensions within $\bar{\mathbb{Q}}$ which are galois over $\mathbb{Q}$, we thus obtain compatible inverse systems. Since the union of the resulting fields $\hat{K}$ is $\bar{\mathbb{Q}}_p$ by part (c), in the limit we obtain an isomorphism

$$\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p) \cong \mathrm{Stab}_{\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})}(|\ |_p|_{\bar{\mathbb{Q}}}) \subset \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$$

5. *(Product formula)* A non-archimedean absolute value $|\ |$ on a field K for which $\mathcal{O}_K$ is a discrete valuation ring with finite residue field $\mathcal{O}_K/\mathfrak{m}$ is called *normalized* if $|\pi| = |\mathcal{O}_K/\mathfrak{m}|^{-1}$ for any element π with $(\pi) = \mathfrak{m}$. The usual absolute value on $\mathbb{Q}_p$ is normalized.

   (a) Show that for all $a \in \mathbb{Q}^\times$ we have $\prod_{p\leqslant\infty} |a|_p = 1$.

   (b) For any finite field k, write down all normalized absolute values on $k(t)$.

   (c) For any finite field k and any $a \in k(t)^\times$, prove that $\prod_v |a|_v = 1$, where the product is taken over all normalized absolute values on $k(t)$.

Solution:

(a) For the rational case, see Proposition 2.1 in Section 2 of Chapter II in Neukirch.

(b) For any monic irreducible polynomial $p \in k[t]$ and any $f \in k(t)$ we define $|f|_p := |k[t]/(p)|^{-\operatorname{ord}_p(f)}$. This defines a non-archimedean absolute value with $\mathcal{O}_{k(t)} = k[t]_{(p)}$, which is normalized because $|p|_p = |k[t]/(p)|^{-1} = |\mathcal{O}_{k(t)}/(p)|^{-1}$. Varying p, this yields all the normalized absolute values on $k(t)$ associated to maximal ideals of $k[t]$.

An additional normalized absolute value $|\ |_\infty$ is obtained in the same way from the maximal ideal $(s) \subset k[s]$ after the substitution $s = \frac{1}{t}$. For any non-zero polynomial $f \in k[t]$ of degree $n \in \mathbb{Z}$ the substitution yields $f(t) = s^n \cdot f(\frac{1}{s}) \cdot s^{-n}$ with $|s^n \cdot f(\frac{1}{s})|_\infty = 1$ and hence $|f|_\infty = |s|_\infty^{-n} = |k|^{\deg(f)}$. For arbitrary non-zero $f, g \in k[t]$ we therefore have $|\frac{f}{g}|_\infty = |k|^{\deg(f)-\deg(g)}$.

Clearly every absolute value on $k(t)$ is equivalent to a unique normalized one. Thus by Theorem 4.1 in the following notes by Brian Conrad the above list of normalized absolute values on $k(t)$ is complete:

`http://math.stanford.edu/~conrad/676Page/handouts/ostrowski.pdf`

(c) By multiplicativity it suffices to prove this for generators of the group $k(t)^\times$, namely for any monic irreducible polynomial $p \in k[t]$ and any element $\alpha \in k^\times$. The latter has finite order and hence satisfies $|\alpha|_v = 1$ for all absolute values $|\ |_v$, and therefore also $\prod_v |a|_v = 1$. The former satisfies $|p|_p = |k[t]/(p)|^{-1} = |k|^{-\deg(p)}$ and $|p|_\infty = |k|^{\deg(p)}$, while $|p|_{p'} = 1$ for all monic irreducible polynomials $p' \in k[t]$ that are distinct from p. Thus the product is again 1.

*6. Show that any local field is the completion of a global field at an absolute value.

Solution: By definition the local fields are, up to isomorphism, finite extensions of $\mathbb{R}$, $\mathbb{F}_p((t))$ and $\mathbb{Q}_p$.

The archimedean complete fields $\mathbb{R}$ and $\mathbb{C}$ are the completions of $\mathbb{Q}$ and $\mathbb{Q}(i)$ with respect to the usual archimedean absolute value.

Suppose that K is a local field of positive characteristic. Then, the last part of the proof of Proposition 5.2 in Section 5 of Chapter II of Neukirch states that $K \cong k((t))$, where k is a finite extension of $\mathbb{F}_p$. Hence, we have $K \cong \mathbb{F}_q((t))$ for some prime power q. In this case K is isomorphic to the completion of $\mathbb{F}_q(t)$ at the absolute value induced by $\mathrm{ord}_t : \mathbb{F}_q(t) \to \mathbb{Z} \cup \{\infty\}$.

Suppose now that $K = \mathbb{Q}_p(\alpha)$ is a finite extension of $\mathbb{Q}_p$. Let f be the minimal polynomial of α over $\mathbb{Q}_p$. As in the aliter of the solution of exercise 4(c), we can choose a polynomial $g \in \mathbb{Q}[X]$ of degree $[K : \mathbb{Q}_p]$ with a root $\beta \in \bar{\mathbb{Q}}_p$, such that K is the completion of the number field $\mathbb{Q}(\beta)$ with respect to $|\ |_p$.