D-MATH
Prof. Richard Pink

Number Theory II

FS 2024

Solutions 17

Absolute values, Extensions of Complete Absolute Values

1. Let $|\ |$ be the usual archimedean absolute value on $\mathbb{R}$ and on $\mathbb{Q}$.

   (a) Prove that $\|(x,y)\| := |x+\sqrt{2}\,y|$ defines a norm on the $\mathbb{Q}$-vector space $\mathbb{Q}^2$, which is not equivalent to the euclidean norm.

   (b) Can one construct a similar example with the p-adic norm on $\mathbb{Q}$?

   Solution:

   (a) Since $\sqrt{2} \notin \mathbb{Q}$, we have $\|(x,y)\| = 0$ if and only if $x = y = 0$. Also, for any $c \in \mathbb{Q}$ we have

   $$\|(cx,cy)\| = \big|cx+\sqrt{2}\,cy\big| = |c|\cdot\|(x,y)\|.$$

   Finally, for any $x_1, x_2, y_1, y_2 \in \mathbb{Q}$ we compute

   $$\begin{aligned}\|(x_1+x_2, y_1+y_2)\| = |(x_1+x_2)+\sqrt{2}\,(y_1+y_2)| &\leqslant |x_1+\sqrt{2}\,y_1| + |x_2+\sqrt{2}\,y_2| \\ &= \|(x_1,y_1)\| + \|(x_2,y_2)\|.\end{aligned}$$

   Thus $\|\ \|$ is a norm.

   Aliter: The axioms for the absolute value imply that $|\ |$ is a norm on the $\mathbb{R}$-vector space $\mathbb{R}$. It is therefore also a norm on $\mathbb{R}$ as a $\mathbb{Q}$-vector space and therefore induces a norm on any $\mathbb{Q}$-subspace thereof. By transport of structure via the isomorphism $\mathbb{Q}^2 \xrightarrow{\sim} \mathbb{Q}+\sqrt{2}\mathbb{Q} \subset \mathbb{R}$, $(x,y) \mapsto x+\sqrt{2}\,y$ we therefore obtain a norm on $\mathbb{Q}^2$.

   Finally consider a sequence (x_n) in $\mathbb{Q}$ that converges to $\sqrt{2}$ in $\mathbb{R}$. Then the sequence $\|(x_n,-1)\|$ converges to 0, but $\sqrt{x_n^2+1} \geqslant 1$ does not. Thus our norm is not equivalent to the euclidean norm.

   (b) This works exactly as in (a) with $\mathbb{R}$ replaced by $\mathbb{Q}_p$ and $\sqrt{2}$ replaced by any element of $\mathbb{Q}_p \smallsetminus \mathbb{Q}$.

2. Determine to which extent the factors in Hensel's lemma are unique.

   Solution: Let K be a field with a complete ultrametric absolute value $|\ |$ and let $\mathfrak{p}$ be the maximal ideal of its valuation ring $\mathcal{O}_\mathfrak{p}$. Consider a primitive $f \in \mathcal{O}_\mathfrak{p}[X]$ and a decomposition $(f \bmod \mathfrak{p}) = \bar{g}\cdot\bar{h}$ with coprime polynomials $\bar{g}$, $\bar{h} \in k[X]$.

Hensel's Lemma states that there exist $g, h \in \mathcal{O}_\mathfrak{p}[X]$ with $(g \bmod \mathfrak{p}) = \bar{g}$ and $(h \bmod \mathfrak{p}) = \bar{h}$ and $\deg(g) = \deg(\bar{g})$ and $f = g \cdot h$.

We claim that arbitrary polynomials g', h' have the same properties if and only if $g' = ug$ and $h' = u^{-1}h$ for some $u \in \mathcal{O}_\mathfrak{p}$ with $u - 1 \in \mathfrak{p}$. The 'if' part is clear. To prove the 'only if' part take g', h' with the same properties. Then by assumption we have $\deg(\bar{g}) = \deg(g) = \deg(g')$, and the highest coefficients of g and g' coincide modulo $\mathfrak{p}$. After multiplying g and g' by suitable units we may assume that g, g' are monic, and then we will prove that $g = g'$ and $h = h'$.

So assume that this is not the case. Since each of these equalities implies the other, we then have $g \neq g'$ and $h \neq h'$. As g and g' coincide modulo $\mathfrak{p}$ and are both monic, there exist $0 \neq \pi_1 \in \mathfrak{p}$ and a primitive $p \in \mathcal{O}_\mathfrak{p}[X]$ with $\deg(p) < \deg(g)$ such that $g' = g + \pi_1 p$. Also, since h and h' coincide modulo $\mathfrak{p}$, there exist $0 \neq \pi_2 \in \mathfrak{p}$ and a primitive $q \in \mathcal{O}_\mathfrak{p}[X]$ such that $h' = h + \pi_2 q$. We then compute

$$0 \;=\; g'h' - gh \;=\; g\pi_2 q + h\pi_1 p + \pi_1\pi_2 pq.$$

If $|\pi_1| < |\pi_2|$, dividing by π_2 and reducing modulo $\mathfrak{p}$ yields $\bar{g}\bar{q} = 0$, which contradicts g and q being primitive. In the same way $|\pi_1| > |\pi_2|$ yields a contradiction. Thus we have $|\pi_1| = |\pi_2|$ and hence $c := \pi_1/\pi_2 \in \mathcal{O}_\mathfrak{p}^\times$. Dividing the equation by π_2 and reducing modulo $\mathfrak{p}$ then yields

$$\bar{g}\bar{q} + \bar{h}\bar{c}\bar{p} \;=\; 0.$$

Since $\bar{g}$ and $\bar{h}$ are coprime, this implies $\bar{g}|\bar{p}$. But by construction $\bar{p} = (p \bmod \mathfrak{p})$ is non-zero of degree $< \deg(g) = \deg(\bar{g})$. Thus we have a contradiction and are therefore done.

*3. Here we consider $\mathbb{Q}_p$ as an abstract field and include $\mathbb{Q}_\infty := \mathbb{R}$.

(a) Show that $\mathbb{Q}_p$ and $\mathbb{Q}_q$ are not isomorphic for any $p \neq q$.

(b) Prove that every automorphism of $\mathbb{Q}_p$ is trivial.

Hint: Look at which elements are squares in the respective field.

Solution: (a) For any prime number p, the equation $x^2 = p$ has a solution in $\mathbb{R}$, but not in $\mathbb{Q}_p$, because every element of $\mathbb{Q}_p^\times$ has the form $x = p^n u$ for some $n \in \mathbb{Z}$ and $u \in \mathbb{Z}_p^\times$ and hence $x^2 = p^2u^2$ with $u^2 \in \mathbb{Z}_p^\times$. Thus $\mathbb{Q}_p \not\cong \mathbb{R}$.

For any two prime numbers $p \neq q$, without loss of generality we can assume that q is odd. Choose an integer a with $pa \equiv 1 \bmod (q)$. After replacing a by $a + q$ if necessary, we can assume that in addition $p \nmid a$. Then the equation $x^2 = pa$ does not have a solution in $\mathbb{Q}_p$ for the same reason as above. But we claim that it has a solution in $\mathbb{Q}_q$. Indeed, for every $n \geqslant 1$ the residue class $pa + q^n\mathbb{Z}$ lies in the subgroup $1 + q\mathbb{Z}/q^n\mathbb{Z}$ of odd order q^{n-1}. Thus the equation $x^2 = pa$ has a solution in $1+q\mathbb{Z}/q^n\mathbb{Z}$, namely $(pa)^k + q^n\mathbb{Z}$ for the integer $k := \frac{q^{n-1}+1}{2}$. Varying n, by Prop 8.1.9 of the lecture course it follows that $x^2 = pa$ has a solution in $\mathbb{Z}_q$, as claimed. (*Aliter:* Use exercise 5 of sheet 16.) As the same equation has a solution in $\mathbb{Q}_p$ but not in $\mathbb{Q}_q$, the fields are not isomorphic.

(b) Let σ be any automorphism of $\mathbb{Q}_p$. In each case we exploit the fact that σ maps the set of squares in $\mathbb{Q}_p$ bijectively to itself.

In $\mathbb{Q}_p = \mathbb{R}$ the squares are precisely the non-negative real numbers. Thus σ preserves the sign. Applying this to the difference $x - y$ of two real numbers it follows that σ preserves the order relation '$<$'. Being order preserving and the identity on the dense subset $\mathbb{Q}$ it must therefore be the identity.

For $\mathbb{Q}_p$ with $p < \infty$ we follow Lahtonen:
`https://math.stackexchange.com/q/449465`

For p odd we first prove that an element $a \in \mathbb{Q}_p$ lies in $\mathbb{Z}_p$ if and only if $1 + pa^2$ is a square in $\mathbb{Q}_p$. Indeed, if $a \in \mathbb{Z}_p$, we have $X^2 - 1 - pa^2 \equiv (X-1)(X+1) \bmod (p)$ with coprime factors $X-1$, $X+1 \in \mathbb{F}_p[X]$; so by Hensel's lemma the left hand side factors in $\mathbb{Z}_p[X]$ and hence $1 + pa^2$ is a square in $\mathbb{Q}_p$. Conversely, if $a \in \mathbb{Q}_p \smallsetminus \mathbb{Z}_p$, then $0 > \mathrm{ord}_p(pa^2) = \mathrm{ord}_p(1+pa^2)$ is odd and so $1+pa^2$ cannot be a square in $\mathbb{Q}_p$.

For $p = 2$ we show that an element $a \in \mathbb{Q}_2$ lies in $\mathbb{Z}_2$ if and only if $1 + 8a^2$ is a square in $\mathbb{Q}_2$. Suppose first that $a \in \mathbb{Z}_2$. Then $1 + 8a^2$ is a square in $\mathbb{Q}_2$ if and only if $X^2 - 1 - 8a^2 = 0$ has a solution in $\mathbb{Q}_2$. Substituting X by $2Y + 1$ and dividing by 4, we obtain the equivalent equation $Y^2 + Y - 2a^2 = 0$. Since $Y^2 + Y - 2a^2 \equiv Y(Y + 1) \bmod (2)$ with coprime factors Y, $Y + 1 \in \mathbb{F}_2[X]$, we can apply Hensel's lemma and deduce that $1 + 8a^2$ is a square in $\mathbb{Q}_2$. Conversely, suppose that $a \in \mathbb{Q}_2 \smallsetminus \mathbb{Z}_2$, that is $\mathrm{ord}_2(a) < 0$. If $\mathrm{ord}_2(a) \leqslant -2$, analogously to the case when p is odd, it follows that $\mathrm{ord}_2(1 + 8a^2)$ is odd and hence $1 + 8a^2$ is not a square in $\mathbb{Q}_2$. By contrast, if $\mathrm{ord}_2(a) = -1$, then $2a \in \mathbb{Z}_2^\times = 1 + 2\mathbb{Z}_2$ and hence $1+8a^2 \equiv 3 \bmod (4)$. In particular $\mathrm{ord}_2(1+8a^2) = 0$, so if $1+8a^2$ is a square in $\mathbb{Q}_2$, it is already the square of an element in $\mathbb{Z}_2^\times = 1+2\mathbb{Z}_2$. But for every $b \in \mathbb{Z}_2$ we have $(1 + 2b)^2 = 1 + 4b + 4b^2 \equiv 1 \bmod (4)$. Thus $1 + 8a^2 \equiv 3 \bmod (4)$ implies that $1 + 8a^2$ is not a square in $\mathbb{Q}_2$.

In all cases we have thus proved that an element $a \in \mathbb{Q}_p$ lies in $\mathbb{Z}_p$ if and only if $1 + qa^2$ is a square in $\mathbb{Q}_p$ for $q := p$ or 8. Since $\sigma(1 + qa^2) = 1 + q\sigma(a)^2$ and the set of squares is preserved by σ, it follows that $\sigma(\mathbb{Z}_p) = \mathbb{Z}_p$. As σ is the identity on $\mathbb{Q}$, for all $\alpha \in \mathbb{Q}$ and all $k \in \mathbb{Z}$ it follows that $\sigma(\alpha + p^k\mathbb{Z}_p) = \alpha + p^k\mathbb{Z}_p$.

Now consider an arbitrary $a \in \mathbb{Q}_p$. Since $\mathbb{Q}$ is dense in $\mathbb{Q}_p$, for any $k \in \mathbb{Z}$ there exists an $\alpha \in \mathbb{Q} \cap (a + p^k\mathbb{Z}_p)$. The strict triangle inequality then implies that $a + p^k\mathbb{Z}_p = \alpha + p^k\mathbb{Z}_p$. Thus it follows that $\sigma(a + p^k\mathbb{Z}_p) = a + p^k\mathbb{Z}_p$. Since $\bigcap_{k\geqslant 0}(\alpha + p^k\mathbb{Z}_p) = \{a\}$, we conclude that $\sigma(a) = a$, as desired.

4. 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 $K := \mathbb{C}((t))$ 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 $\mathcal{O}_K = \mathbb{C}[[t]]$. Let L be a finite extension of K of degree n. Since the residue field $\mathbb{C}$ of $\mathcal{O}_K$ is algebraically closed, the extension of residue fields is trivial. Thus L is totally ramified over K. 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 modulo (π). As the residue field $\mathbb{C}$ of $\mathcal{O}_L$ is algebraically closed of characteristic zero, it follows that f mod (π) 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 $K[s] \subset L$ is a subfield of degree n over K, and therefore equal to L. At last the equation $s^n = t$ implies that $L = K[s] = \mathbb{C}((s))$, as desired.

5. 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:
   `https://math.mit.edu/classes/18.785/2016fa/LectureNotes10.pdf`

6. Let K be a field with a complete discrete valuation v, and let $\bar{K}$ be an algebraic closure of K. In the lecture we have seen that v extends uniquely to a valuation $\bar{v}$ on $\bar{K}$. Show that this extension is not complete.

   Hint: Consider roots of an element in K with positive valuation.

   Solution: Without loss of generality we may assume that v is normalized. Choose an element $\pi_0 \in K$ with $v(\pi_0) = 1$. For each $n \geqslant 1$ choose an element $\pi_n \in \bar{K}$ such that $\pi_n^n = \pi_{n-1}$. Then π_n is a root of the polynomial $X^{n!} - \pi_0$ and hence $\bar{v}(\pi_n) = \frac{1}{n!}$. Thus $K_n := K(\pi_n)$ is totally ramified of degree $n!$ over K. In particular the value group of K_n is $\bar{v}(K_n^\times) = \frac{1}{n!}\mathbb{Z}$.

   Now assume that $\bar{v}$ is complete. Then $\bar{K}$ contains the element

   $$\xi := \sum_{n \geqslant 0} \pi_n \pi_0^n.$$

   In other words ξ is algebraic over K, say of degree d. Thus ξ is of degree $\leqslant d$ over

K_m for every $m \geqslant 0$. Since the partial sum

$$\xi_m \;:=\; \sum_{n=0}^{m} \pi_n \pi_0^n$$

already lies in K_m, it follows that

$$\xi - \xi_m \;=\; \sum_{n \geqslant m+1} \pi_n \pi_0^n$$

has degree $\leqslant d$ over $K_{m!}$. The value group $\frac{1}{m!}\mathbb{Z}$ of K_m therefore has index $\leqslant d$ in the value group of $K_m(\xi - \xi_m)$. On the other hand we have

$$\bar{v}(\xi - \xi_m) \;=\; \bar{v}(\pi_{m+1}\pi_0^{m+1}) \;=\; \tfrac{1}{(m+1)!} + m + 1 \;\equiv\; \tfrac{1}{(m+1)!} \bmod \tfrac{1}{m!}\mathbb{Z}.$$

Thus the index of value groups is a multiple of $m+1$. Together this yields a contradiction whenever $m \geqslant d$. Therefore $\bar{v}$ is not complete.