OSTROWSKI FOR NUMBER FIELDS

KEITH CONRAD

Ostrowski classified the nontrivial absolute values on $\mathbf{Q}$: up to equivalence, they are the usual (archimedean) absolute value and the p-adic absolute values for different primes p, with none of these being equivalent to each other. We will see how this theorem extends to any number field K, giving a list of all the nontrivial absolute values on K up to equivalence.

For a nonzero prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$ and a constant $c \in (0,1)$, the function $|\alpha| = c^{\operatorname{ord}_{\mathfrak{p}}(\alpha)}$ for $\alpha \in K^\times$ (and $|0| = 0$) defines a nonarchimedean absolute value on K. We call this a $\mathfrak{p}$-adic absolute value. (Changing c produces an equivalent absolute value, so there is a well-defined $\mathfrak{p}$-adic topology on K, independent of c. This topology on $\mathcal{O}_K$ amounts to declaring the ideals $\mathfrak{p}^k$ to be a neighborhood basis of 0 in $\mathcal{O}_K$.) For two different primes $\mathfrak{p}$ and $\mathfrak{q}$, a $\mathfrak{p}$-adic absolute value and $\mathfrak{q}$-adic absolute value are inequivalent: the Chinese remainder theorem lets us find $\alpha \in \mathcal{O}_K$ satisfying $\alpha \equiv 0 \bmod \mathfrak{p}$ and $\alpha \equiv 1 \bmod \mathfrak{q}$, so the $\mathfrak{p}$-adic absolute value of α is less than 1 and the $\mathfrak{q}$-adic absolute value of α equals 1. Thus the two absolute values are inequivalent.

Any embedding of K into $\mathbf{R}$ or $\mathbf{C}$ gives rise to an archimedean absolute value on K, with complex-conjugate embeddings yielding the same absolute value on K since $|a+bi| = |a-bi|$ in $\mathbf{C}$. Letting r_1 be the number of real embedding of K and r_2 be the number of pairs of complex-conjugate embeddings of K, there are $r_1 + 2r_2$ archimedean embeddings of K but only $r_1 + r_2$ archimedean absolute values (up to equivalence) since complex-conjugate embeddings define the same absolute value and the only way two archimedean embeddings define the same absolute value is when they come from a pair of complex-conjugate embeddings. See [3, p. 42] for the proof of that. In particular, when K is real quadratic there are two real embeddings of K, so K has two archimedean absolute values. (For example, the two archimedean absolute values on $\mathbf{Q}(\theta)$ where $\theta^2 = 2$ are $|a+b\theta| = |a+b\sqrt{2}|$ and $|a+b\theta| = |a-b\sqrt{2}|$.) When K is imaginary quadratic there are two complex embeddings which are complex-conjugate to each other, so K has only one archimedean absolute value.

By tradition, the nonarchimedean absolute values on K are called the finite absolute values while the archimedean ones are called the infinite absolute values. This terminology is due to an analogy with the classification of nontrivial absolute values on $\mathbf{C}(z)$ which are trivial on $\mathbf{C}$: they are associated to the different points on the Riemann sphere, by simply measuring the order of vanishing of a rational function at a point in the same way as a p-adic absolute value operates through a valuation function in the exponent. The absolute values on $\mathbf{C}(z)$ are bounded on $\mathbf{C}[z]$ except for the one associated to the order of vanishing at the point ∞ on the Riemann sphere. Since the archimedean absolute value on $\mathbf{Q}$ is the only one which is unbounded on $\mathbf{Z}$, by analogy one calls it an infinite absolute value. (This analogy is actually rather weak, since using a different field generator over $\mathbf{C}$, say $\mathbf{C}(w)$ where $w = 1/z$, changes which absolute value is "at infinity," whereas the archimedean absolute value on $\mathbf{Q}$ can't be turned into one of the p-adic ones by a field automorphism of $\mathbf{Q}$; in fact, the only field automorphism of $\mathbf{Q}$ is the identity.)

Ostrowski's theorem for K says every nontrivial absolute value on K is equivalent to exactly one of the absolute values we have already described, that is, $\mathfrak{p}$-adic for one prime $\mathfrak{p}$ of $\mathcal{O}_K$ or an archimedean absolute value associated to a real or complex-conjugate pair of embeddings. When $K = \mathbf{Q}$, the proof of Ostrowki's theorem uses special features of $\mathcal{O}_K = \mathbf{Z}$ (like finite base expansions in $\mathbf{Z}^+$ for the archimedean case and division with remainder in $\mathbf{Z}$ for the nonarchimedean case) which are not valid in number fields, so we need a different argument to prove the theorem for K.

Lemma 1. *Let $\mathfrak{p}$ be a nonzero prime ideal in $\mathcal{O}_K$. If $\alpha \in K^\times$ and $\operatorname{ord}_\mathfrak{p}(\alpha) \geq 0$ then $\alpha = x/y$ where $x, y \in \mathcal{O}_K$ and $\operatorname{ord}_\mathfrak{p}(y) = 0$.*

Proof. Write $\alpha\mathcal{O}_K = \mathfrak{a}\mathfrak{b}^{-1}$ for ideals $\mathfrak{a}$ and $\mathfrak{b}$ of $\mathcal{O}_K$ with no common factors. Because $\operatorname{ord}_\mathfrak{p}(\alpha) \geq 0$ the ideal $\mathfrak{p}$ doesn't divide $\mathfrak{b}$. Since $\mathfrak{a} = (\alpha)\mathfrak{b}$, $\mathfrak{a}$ and $\mathfrak{b}$ lie in the same ideal class.

In any desired ideal class, it is always possible to pick an integral ideal which is relatively prime to a given ideal. (Proof omitted; this follows from the Chinese remainder theorem on $\mathcal{O}_K$.) Let $\mathfrak{c}$ be an integral ideal in the ideal class of $[\mathfrak{a}]^{-1} = [\mathfrak{b}]^{-1}$ which is relatively prime to $\mathfrak{p}$. Then

$$(\alpha) = \mathfrak{a}\mathfrak{b}^{-1} = \mathfrak{a}\mathfrak{c}(\mathfrak{b}\mathfrak{c})^{-1}.$$

The ideals $\mathfrak{a}\mathfrak{c}$ and $\mathfrak{b}\mathfrak{c}$ are both principal. Set $\mathfrak{a}\mathfrak{c} = (x)$ and $\mathfrak{b}\mathfrak{c} = (y)$, so x and y are in $\mathcal{O}_K$. Since $\mathfrak{b}$ and $\mathfrak{c}$ are both prime to $\mathfrak{p}$, $\operatorname{ord}_\mathfrak{p}(y) = 0$. Now $(\alpha) = (x)(y)^{-1} = (x/y)$, so by rescaling x by a unit we have $\alpha = x/y$ with $\operatorname{ord}_\mathfrak{p}(y) = 0$. □

The heart of the proof of Ostrowski's theorem in the nonarchimedean case is the next result.

Theorem 2. *Let $v\colon K^\times \to \mathbf{R}$ be a nonzero homomorphism with*

$$v(\alpha + \beta) \geq \min(v(\alpha), v(\beta)) \tag{1}$$

when α, β, and $\alpha + \beta$ are all in $K^\times$. Then $v = t \operatorname{ord}_\mathfrak{p}$ for a unique nonzero prime ideal $\mathfrak{p}$ and $t > 0$.

Proof. Uniqueness is easy: For a nonzero prime ideal $\mathfrak{p}$,

$$\{\alpha \in \mathcal{O}_K : t \operatorname{ord}_\mathfrak{p}(\alpha) > 0\} = \{\alpha \in \mathcal{O}_K : \operatorname{ord}_\mathfrak{p}(\alpha) > 0\} = \{\alpha \in \mathcal{O}_K : \alpha \in \mathfrak{p}\} = \mathfrak{p}.$$

That is, inside of $\mathcal{O}_K$, $t \operatorname{ord}_\mathfrak{p}$ takes positive values precisely on $\mathfrak{p}$, so we can recover $\mathfrak{p}$ from the properties of $t \operatorname{ord}_\mathfrak{p}$. Since t is the smallest positive value of $t \operatorname{ord}_\mathfrak{p}$ on $K^\times$, the value of t is determined as well.

As for the existence of a $\mathfrak{p}$ and t such that $v = t \operatorname{ord}_\mathfrak{p}$, we will show that the set

$$\mathfrak{p} := \{\alpha \in \mathcal{O}_K - \{0\} : v(\alpha) > 0\} \cup \{0\} \tag{2}$$

is a nonzero prime ideal in $\mathcal{O}_K$ and then we will show $v = t \operatorname{ord}_\mathfrak{p}$ for some $t > 0$. Obviously this definition for $\mathfrak{p}$ is motivated by the calculation we made just before: if there is going to be a prime ideal for which v is the corresponding valuation, the set in (2) has to be that ideal.

Before we even discuss $\mathfrak{p}$ in (2), we show $v(\alpha) \geq 0$ on all nonzero algebraic integers. Since $v(1 \cdot 1) = v(1) + v(1)$, $v(1) = 0$. Then $0 = v(1) = v((-1)^2) = 2v(-1)$, so $v(-1) = 0$. Now by (1), $v(a) \geq 0$ for all nonzero $a \in \mathbf{Z}$. In a sense, the nonnegativity of v on $\mathbf{Z} - \{0\}$ underlies everything that follows. For $\alpha \in \mathcal{O}_K$, we can write an equation of integral dependence for it over $\mathbf{Z}$, say

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$$

with $a_j \in \mathbf{Z}$. Choose n as small as possible, so $a_0 \neq 0$. If $v(\alpha) < 0$, then heuristically α^n has an n-th order pole at v, while the other terms in the sum on the left have a lower order pole (the a_j's don't contribute polar data since $v(a_j) \geq 0$ or $a_j = 0$). Thus the whole sum on the left has a pole at v, but the sum is 0, a contradiction.

For a rigorous argument, we rewrite the above equation as

$$\alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_1\alpha - a_0.$$

When $a_j \neq 0$, $v(-a_j\alpha^j) = v(a_j) + jv(\alpha) \geq jv(\alpha)$. When $a_j = 0$, of course the term $a_j\alpha^j$ is 0 so we ignore it. Now if $v(\alpha) < 0$, then $v(-a_j\alpha^j) \geq (n-1)v(\alpha)$ since $j \leq n-1$. Therefore by (1) extended to a sum of several terms,

$$v(-a_{n-1}\alpha^{n-1} - \cdots - a_1\alpha - a_0) \geq (n-1)v(\alpha).$$

Since $v(\alpha^n) = nv(\alpha)$, we have $nv(\alpha) \geq (n-1)v(\alpha)$, so $v(\alpha) \geq 0$. This contradicts the assumption that $v(\alpha) < 0$. Therefore $v(\alpha) \geq 0$.

Since v is not identically 0 on $K^\times$, it is not identically 0 on $\mathcal{O}_K - \{0\}$, which means v must take some positive values on $\mathcal{O}_K - \{0\}$ (we just eliminated the possibility of negative values on $\mathcal{O}_K - \{0\}$). Thus the set $\mathfrak{p}$ in (2) is not $\{0\}$. Since v is a homomorphism, easily $\mathfrak{p}$ is a subgroup of $\mathcal{O}_K$, and in fact an $\mathcal{O}_K$-module on account of the nonnegativity of v on $\mathcal{O}_K - \{0\}$. So $\mathfrak{p}$ is an ideal in $\mathcal{O}_K$. Since $v(1) = 0$, $\mathfrak{p}$ is a proper ideal of $\mathcal{O}_K$. Let's show it is a prime ideal. For α and β in $\mathcal{O}_K$, assume $\alpha\beta \in \mathfrak{p}$. To show α or β is in $\mathfrak{p}$, assume neither is in $\mathfrak{p}$. Then $v(\alpha) = 0$ and $v(\beta) = 0$, so $v(\alpha\beta) = v(\alpha) + v(\beta) = 0$, but that contradicts $\alpha\beta$ being in $\mathfrak{p}$.

Now we have our nonzero prime ideal $\mathfrak{p}$, so it is time to show $v = t\,\mathrm{ord}_\mathfrak{p}$ for some t.

First we'll show that if $\mathrm{ord}_\mathfrak{p}(\alpha) = 0$ then $v(\alpha) = 0$. By Lemma 1 we can write $\alpha = x/y$ with $x, y \in \mathcal{O}_K$ and $\mathrm{ord}_\mathfrak{p}(y) = 0$. Therefore $\mathrm{ord}_\mathfrak{p}(x) = \mathrm{ord}_\mathfrak{p}(\alpha y) = 0 + 0 = 0$. Since x and y are in $\mathcal{O}_K$ and are not in $\mathfrak{p}$, the definition of $\mathfrak{p}$ tells us $v(x) = 0$ and $v(y) = 0$. Therefore $v(\alpha) = 0$.

Now we show $v = t\,\mathrm{ord}_\mathfrak{p}$ for some $t > 0$. For $\alpha \in K^\times$, let $n = \mathrm{ord}_\mathfrak{p}(\alpha) \in \mathbf{Z}$. Pick $\gamma \in \mathfrak{p} - \mathfrak{p}^2$, so $\mathrm{ord}_\mathfrak{p}(\gamma) = 1$ and $v(\gamma) > 0$. Then $\mathrm{ord}_\mathfrak{p}(\alpha/\gamma^n) = 0$, so $v(\alpha/\gamma^n) = 0$, so

$$v(\alpha) = nv(\gamma) = \mathrm{ord}_\mathfrak{p}(\alpha)v(\gamma).$$

The choice of γ has nothing to do with α. This equation holds for all $\alpha \in K^\times$, so $v = t\,\mathrm{ord}_\mathfrak{p}$ where $t = v(\gamma) > 0$. □

Theorem 3 (Ostrowski). *Any nontrivial absolute value on K is equivalent to a $\mathfrak{p}$-adic absolute value for a unique prime $\mathfrak{p}$ in $\mathcal{O}_K$ or is equivalent to an absolute value coming from a real or complex embedding of K.*

Proof. We have already discussed the inequivalence of the absolute values on the list. To show they are the only ones, we take cases.

If $|\cdot|$ is a nonarchimedean absolute value on K, we expect $|\cdot|$ to look like $c^{\mathrm{ord}_\mathfrak{p}(\alpha)}$, with $c \in (0,1)$, so the function $v(\alpha) := -\log|\alpha|$ should look like a positive scalar multiple of $\mathrm{ord}_\mathfrak{p}$. To prove this really happens, note v satisfies the conditions of Theorem 2, so $-\log|\alpha| = t\,\mathrm{ord}_\mathfrak{p}(\alpha)$ for some $t > 0$ and prime $\mathfrak{p}$. Rewriting this as $|\alpha| = (e^{-t})^{\mathrm{ord}_\mathfrak{p}(\alpha)}$, we see $|\cdot|$ is a $\mathfrak{p}$-adic absolute value with constant $c = e^{-t} < 1$. Since different nonzero prime ideals define inequivalent absolute values, the $\mathfrak{p}$ here is unique, which forces c to be unique as well.

To show any archimedean absolute value on K is equivalent to an absolute value coming from a real or complex embedding of K, we omit the details and give references. See [1, pp. 278–280] or [3, pp. 40–41]. (This case is not a triviality; look at the references!) $\square$

In Theorem 3, the description of the nontrivial absolute values in the archimedean and non-archimedean cases sounds different: use real or complex embeddings in one case or nonzero prime ideals in the other case. There is a way to describe the situation in a uniform way: consider field embeddings of K into any of the algebraic closures of a completion of $\mathbf{Q}$: $\overline{\mathbf{R}} = \mathbf{C}$ or $\overline{\mathbf{Q}}_p$ as p varies. Embedding K into such a field provides K with a nontrivial absolute value by using the absolute value from $\mathbf{C}$ or $\overline{\mathbf{Q}}_p$ on the image of K under the embedding. Every nontrivial absolute value on K arises in this way (proof?), but it is not quite true that different embeddings of K into some $\overline{\mathbf{Q}}_v$ produce different absolute values. For instance, we have already noted that in the archimedean setting complex-conjugate embeddings of K into $\mathbf{C}$ define the same absolute value. A similar thing can happen p-adically. As an example, the two embeddings $\mathbf{Q}(i) \to \overline{\mathbf{Q}}_2$, obtained by sending i to the two different square roots of -1 in $\overline{\mathbf{Q}}_2$, define the same absolute value on $\mathbf{Q}(i)$. Similarly, the two embeddings $\mathbf{Q}(i) \to \overline{\mathbf{Q}}_3$ give $\mathbf{Q}(i)$ the same absolute value. However, the two embeddings $\mathbf{Q}(i) \to \overline{\mathbf{Q}}_5$ define different absolute values. To describe which embeddings of K into some $\overline{\mathbf{Q}}_v$ define the same absolute value on K, see [2, Theorem 2, p. 38] (setting $K = \mathbf{Q}$ there).

The set of all absolute values on K are tied together by a product formula, just like over $\mathbf{Q}$. To write down this formula, we have to normalize the absolute values in the right way. Here's how that is done. For any prime $\mathfrak{p}$, use $1/\operatorname{N}\mathfrak{p}$ as the base for the $\mathfrak{p}$-adic absolute value:

$$|\alpha|_{\mathfrak{p}} = \left(\frac{1}{\operatorname{N}\mathfrak{p}}\right)^{\operatorname{ord}_{\mathfrak{p}}(\alpha)}$$

for $\alpha \in K^\times$. For the archimedean absolute values, we use the absolute values from every real embedding and the *squares* of the absolute values from the complex-conjugate pairs of complex embeddings. We have now selected one absolute value on K from every nontrivial equivalence class, with a peculiar twist in the complex case of using the square of the absolute value.

Theorem 4 (Product Formula)**.** *For any $\alpha \neq 0$ in K,*

$$\prod_v |\alpha|_v = 1,$$

where the product runs over the absolute values as described above.

All but finitely many of the $|\alpha|_v$'s are 1, so their formally infinite product is really a finite product, and thus the product makes algebraic sense.

Proof. The product is multiplicative in α, so it suffices to check the product formula when $\alpha \in \mathcal{O}_K - \{0\}$. The formula is clear when $\alpha \in \mathcal{O}_K^\times$, since every term in the product is 1. For non-unit α, factor $\alpha\mathcal{O}_K$ as

$$\alpha\mathcal{O}_K = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r},$$

where $a_i \geq 1$. The only terms in the product which are not necessarily 1 come from the absolute values attached to these $\mathfrak{p}_j$'s and to the archimedean absolute values. We will look separately at the contribution from the non-archimedean and archimedean absolute values.

The contribution to the product formula from the $\mathfrak{p}_j$'s is

$$\prod_{j=1}^{r}\left(\frac{1}{\mathrm{N}\mathfrak{p}_j}\right)^{a_j}.$$

Since the archimedean absolute values correspond to the real and complex embeddings of K, and we use the squared absolute value for the complex embeddings, the contribution to the product formula from the archimedean absolute values is the absolute value of the product of the images of α under all embeddings of K into the real and complex numbers. (Specifically, if $\sigma\colon K \to \mathbf{C}$ is an embedding then $|\sigma(\alpha)|^2 = |\sigma(\alpha)||\overline{\sigma}(\alpha)|$ can be interpreted as a contribution to the product formula from both σ and $\overline{\sigma}$ rather than as a "double" contribution from σ.) The product of the absolute values of α under all real and complex embeddings of K is nothing other than $\mathrm{N}_{K/\mathbf{Q}}(\alpha)$, so the archimedean contribution to the product formula is $|\,\mathrm{N}_{K/\mathbf{Q}}(\alpha)|$.

From the compatibility of the norm on principal ideals and elements,

$$|\,\mathrm{N}_{K/\mathbf{Q}}(\alpha)| = \mathrm{N}(\alpha\mathcal{O}_K) = \prod_{j=1}^{r}\mathrm{N}\mathfrak{p}_j^{a_j},$$

which means the archimedean and non-archimedean contributions to the product formula for α are inverses of each other, so their product is 1. □

The need to use the square of the complex absolute value instead of the complex absolute value is not just a weird fix to make the product formula work out; it shows up in a lot of other situations in algebraic number theory.

There is a second way to prove the product formula. Collect together the factors in the product for absolute values on K which extend a given absolute value on $\mathbf{Q}$ and see what these subproducts turn out to be:

$$\prod_{v}|\alpha|_v = \prod_{v|\infty}|\alpha|_v \cdot \prod_{p}\prod_{\mathfrak{p}|p}|\alpha|_{\mathfrak{p}},$$

where we write $v|\infty$ to mean v is an archimedean absolute value on K and it is understood that we use the squares of absolute values from complex embeddings. The product of the archimedean absolute values is $|\,\mathrm{N}_{K/\mathbf{Q}}(\alpha)|$, which we used in the proof above. For each prime number p it turns out that the piece of the product formula coming from the absolute values attached to primes in $\mathcal{O}_K$ lying over p is precisely $|\,\mathrm{N}_{K/\mathbf{Q}}(\alpha)|_p$. Therefore

$$\prod_{v}|\alpha|_v = |\,\mathrm{N}_{K/\mathbf{Q}}(\alpha)| \cdot \prod_{p}|\,\mathrm{N}_{K/\mathbf{Q}}(\alpha)|_p,$$

so the product formula for α as an element of K turns into the product formula for $\mathrm{N}_{K/\mathbf{Q}}(\alpha)$ as a rational number. Therefore if we already know the product formula over $\mathbf{Q}$ the right side above is 1, which proves the product formula over K!

In addition to number fields, one should consider at the same time the function field case. That is, we ought to allow K to be a finite extension of $\mathbf{F}_p(T)$, where T transcendental over $\mathbf{F}_p$. (Equivalently, K has transcendence degree 1 over $\mathbf{F}_p$ and the algebraic closure of $\mathbf{F}_p$ in K is a finite extension of $\mathbf{F}_p$.) We know what the nontrivial absolute values are on $\mathbf{F}_p(T)$; they are associated to the monic irreducibles in $\mathbf{F}_p[T]$ and to the negative degree function. Each of these lifts to some absolute values on K in terms of nonzero prime ideals (no archimedean absolute values in characteristic p), but trying to think of these prime ideals as lying in some "ring of integers" is a bit awkward because there is no canonical ring of integers in K, essentially because there isn't one in $\mathbf{F}_p(T)$ either. The ring $\mathbf{F}_p[T]$ could just as well be replaced with $\mathbf{F}_p[1/T]$. Using a geometric language, one can think of K as functions on a certain smooth curve, and the absolute values on K (or rather, the associated valuations) turn out to be the order-of-vanishing functions at the points on this curve. The main argument one needs in this development is an analogue of Theorem 2.

References

[1] V. I. Borevich and I. R. Shafarevich, "Number Theory," Academic Press, New York, 1966.

[2] S. Lang, "Algebraic Number Theory," 2nd ed., Springer–Verlag, New York, 1994.

[3] P. Ribenboim, "The Theory of Classical Valuations," Springer–Verlag, New York, 1999.