

OSTROWSKI'S THEOREM FOR $\mathbf{Q}(i)$

KEITH CONRAD

We will extend Ostrowki's theorem from \mathbf{Q} to the quadratic field $\mathbf{Q}(i)$. On \mathbf{Q} , every non-archimedean absolute value is equivalent to the p -adic absolute value for a unique prime number p , and the archimedean absolute values are all equivalent to the usual absolute value on \mathbf{Q} . We will see a similar thing happens in $\mathbf{Q}(i)$: each non-archimedean absolute value is associated to a prime in $\mathbf{Z}[i]$ (unique up to unit multiple) and each archimedean absolute value is equivalent to the complex absolute value $|a + bi|_\infty = \sqrt{a^2 + b^2}$.

First we need some background about $\mathbf{Z}[i]$. For $\alpha = a + bi$ in $\mathbf{Z}[i]$ ($a, b \in \mathbf{Z}$), set the norm of α to be

$$N(\alpha) = a^2 + b^2,$$

which is a nonnegative integer. This norm is multiplicative ($N(\alpha\beta) = N(\alpha)N(\beta)$) and it gives a measure of the size of elements. For an integer $a \in \mathbf{Z}$, its norm is its square: $N(a) = a^2$. In particular, $N(1) = 1$.

Theorem 1. *The units in $\mathbf{Z}[i]$ are $1, -1, i,$ and $-i,$ namely the elements of norm 1.*

Proof. Since $1 \cdot 1 = 1$, $(-1)(-1) = 1$, and $i(-i) = 1$, these four elements are all units in $\mathbf{Z}[i]$. Conversely, if u is a unit in $\mathbf{Z}[i]$ then $uv = 1$ for some v in $\mathbf{Z}[i]$. Taking the norm of both sides, $N(u)N(v) = 1$. This last equation is in the positive integers, so $N(u)$ and $N(v)$ both must be 1. Writing $u = a + bi$, we have $a^2 + b^2 = 1$. The only solutions to this in integers are $(a, b) = (\pm 1, 0)$ and $(0, \pm 1)$, which yield the four numbers $1, -1, i,$ and $-i$. \square

Like \mathbf{Z} , there is a division algorithm in $\mathbf{Z}[i]$. To measure the size of a remainder under division, we use the norm:

Theorem 2. *For α and β in $\mathbf{Z}[i]$ with $\beta \neq 0$, there are γ and ρ in $\mathbf{Z}[i]$ such that*

$$\alpha = \beta\gamma + \rho, \quad N(\rho) \leq \frac{1}{2}N(\beta) < N(\beta).$$

Proof. The norm on $\mathbf{Z}[i]$ is closely related to the absolute value on \mathbf{C} : $N(a + bi) = |a + bi|_\infty^2$. The absolute value on \mathbf{C} is our way of measuring distances in \mathbf{C} , and we will take advantage of this.

In \mathbf{C} , the furthest a complex number can be from an element of $\mathbf{Z}[i]$ is $1/\sqrt{2}$, since the center points of 1×1 squares with vertices in $\mathbf{Z}[i]$ are at distance $1/\sqrt{2}$ from the vertices. Now consider the ratio α/β as a complex number and place it in a 1×1 square having vertices in $\mathbf{Z}[i]$. Let $\gamma \in \mathbf{Z}[i]$ be the vertex of that square that is nearest to α/β , so $|\alpha/\beta - \gamma|_\infty \leq 1/\sqrt{2}$. Multiplying through by $|\beta|_\infty$, $|\alpha - \beta\gamma|_\infty \leq (1/\sqrt{2})|\beta|_\infty$. Squaring both sides and recalling that the squared complex absolute value on $\mathbf{Z}[i]$ is the norm, we obtain

$$N(\alpha - \beta\gamma) \leq \frac{1}{2}N(\beta).$$

Now set $\rho = \alpha - \beta\gamma$. \square

Remark 3. Unlike in \mathbf{Z} , the quotient and remainder in $\mathbf{Z}[i]$ are not unique. For example, take $\alpha = 37 + 2i$ and $\beta = 11 + 2i$. You can check that

$$\alpha = \beta \cdot 3 + (4 - 4i), \quad \alpha = \beta(3 - i) + (2 + 7i).$$

Here both remainders have norm less than $N(\beta) = 125$ (in fact, less than $125/2$). Our proof of Theorem 2 explains geometrically why the quotient and remainder in $\mathbf{Z}[i]$ are not unique: α/β is closer to two vertices in the 1×1 square containing it than the length of a (half-)diagonal of the square.

This lack of uniqueness in the quotient and remainder is not a big deal, since the the main consequences of the division algorithm, such as Euclid's algorithm and unique factorization, don't actually use the uniqueness. The main thing is just having the remainder smaller (by some measure) than the divisor, and that's what Theorem 2 gives us.

Corollary 4. *The ring $\mathbf{Z}[i]$ has unique factorization, and in fact is a principal ideal domain.*

Proof. A domain with a division algorithm is a PID and a UFD. \square

Now that we have unique factorization, we are ready to introduce the analogue of p -adic valuations for $\mathbf{Q}(i)$. This will use primes in $\mathbf{Z}[i]$. Here are some examples of primes:

$$1 + i, \quad 3, \quad 1 + 2i, \quad 1 - 2i, \quad 7, \quad 11, \quad 2 + 3i, \quad 2 - 3i.$$

Notice 2 and 5 are not here, because they are not prime in $\mathbf{Z}[i]$: $2 = (1 + i)(1 - i)$ and $5 = (1 + 2i)(1 - 2i)$.

For a prime π in $\mathbf{Z}[i]$, we can define a π -adic valuation in the same way as the p -adic valuation on \mathbf{Q} : for nonzero $x \in \mathbf{Q}(i)$, write x as a ratio of elements in $\mathbf{Z}[i]$ and pull out the largest power of π from the numerator and denominator:

$$x = \pi^n \frac{\alpha}{\beta}$$

where $\alpha, \beta \in \mathbf{Z}[i]$ and π does not divide α or β . Then we set

$$\text{ord}_\pi(x) = n$$

and call n the π -adic valuation of x . At $x = 0$, we set $\text{ord}_\pi(0) = \infty$.

Example 5. Let $\alpha = 19 + 83i$. What are $\text{ord}_{1+i}(\alpha)$, $\text{ord}_3(\alpha)$, and $\text{ord}_{1+2i}(\alpha)$? We divide α by $1 + i$, 3 , and $2 + 3i$ until we can go no further, and see how many times we are able to divide.

Since $\alpha/(1+i) = (19+83i)/(1+i) = 51+32i$ and $(51+32i)/(1+i) = 83/2 - 19/2i \notin \mathbf{Z}[i]$, the largest power of $1 + i$ in α is the first power: $\alpha = (1 + i)(51 + 32i)$ and $1 + i$ doesn't divide $51 + 32i$. Therefore $\text{ord}_{1+i}(\alpha) = 1$.

Since $\alpha/3 \notin \mathbf{Z}[i]$, 3 doesn't divide α at all, so $\text{ord}_3(\alpha) = 0$.

If we divide α by $1 + 2i$, this can be done three times and we find $\alpha = (1 + 2i)^3(-3 - 7i)$, where $1 + 2i$ doesn't divide $-3 - 7i$ (their ratio is not in $\mathbf{Z}[i]$). Therefore $\text{ord}_{1+2i}(\alpha) = 3$.

As with the p -adic valuation ord_p on \mathbf{Q} , you can check using unique factorization in $\mathbf{Z}[i]$ that for a prime π in $\mathbf{Z}[i]$ and x and y in $\mathbf{Q}(i)$

$$(1) \quad \text{ord}_\pi(xy) = \text{ord}_\pi(x) + \text{ord}_\pi(y) \text{ and } \text{ord}_\pi(x + y) \geq \min(\text{ord}_\pi(x), \text{ord}_\pi(y)).$$

To turn the π -adic valuation into an absolute value, pick $c \in (0, 1)$ and set

$$|x|_\pi = c^{\text{ord}_\pi(x)}$$

for $x \in \mathbf{Q}(i)$. In particular, $|0|_\pi = 0$. The algebraic properties of ord_π in (1) show $|\cdot|_\pi$ is an absolute value on $\mathbf{Q}(i)$ and is non-archimedean. Just as the p -adic absolute values on \mathbf{Q} are ≤ 1 on \mathbf{Z} , a π -adic absolute value on $\mathbf{Q}(i)$ is ≤ 1 on $\mathbf{Z}[i]$, simply because ord_π is nonnegative on $\mathbf{Z}[i]$.

Picking two different c_1 and c_2 in $(0, 1)$ leads to two different π -adic absolute values: $|x| = c_1^{\text{ord}_\pi(x)}$ and $|x|' = c_2^{\text{ord}_\pi(x)}$. However, since c_1 and c_2 are (positive) powers of each other, these absolute values are equivalent (that is, they define the same topology on $\mathbf{Q}(i)$). From each prime π we get a single equivalence class of absolute values by using different choices of c in $(0, 1)$. (We will find out later what the best choice of c is, to get a product formula on $\mathbf{Q}(i)$.)

If we replace π by a unit multiple $\pi' = u\pi$ then we don't change the valuation: $\text{ord}_\pi(x) = \text{ord}_{\pi'}(x)$ for all x . Therefore primes that differ by a unit multiple give rise to the same absolute value on $\mathbf{Q}(i)$. For example, $1 - i = -i(1 + i)$, so $1 - i$ and $1 + i$ have the same valuation functions. But watch out: the primes $1 + 2i$ and $1 - 2i$ are not unit multiples of each other (compute all four unit multiples of $1 + 2i$ and you won't get $1 - 2i$) and in fact they define different valuations. Indeed, $\text{ord}_{1+2i}(1 + 2i) = 1$ and $\text{ord}_{1-2i}(1 + 2i) = 0$ since $1 - 2i$ doesn't divide $1 + 2i$ (the ratio $(1 + 2i)/(1 - 2i)$ is not in $\mathbf{Z}[i]$).

We are almost ready for Ostrowski's theorem in $\mathbf{Q}(i)$. The proof of Ostrowski's theorem in \mathbf{Q} uses base expansions to handle the archimedean case. Are there base expansions in $\mathbf{Z}[i]$? Not in the same canonical way as in \mathbf{Z} (really, \mathbf{Z}^+). We will only need an expansion for base $1 + i$, which goes as follows.

Lemma 6. *For nonzero α in $\mathbf{Z}[i]$, we can write*

$$\alpha = c_0 + c_1(1 + i) + c_2(1 + i)^2 + \cdots + c_k(1 + i)^k,$$

where $2^k \leq N(\alpha) < 2^{k+1}$ and $c_j \in \{0, \pm 1, \pm i\}$, with $c_k \neq 0$.

This lemma is not saying the coefficients c_j are unique for α .

Proof. We argue by induction on $N(\alpha)$. If $N(\alpha) = 1$ then $k = 0$ and α is ± 1 or $\pm i$.

Now suppose $N(\alpha) \geq 2$, so $k \geq 1$. Assume the theorem is true for elements with norm less than $N(\alpha)$. Since we will only be using the complex absolute value in this proof, we write it as $|\cdot|$ rather than as $|\cdot|_\infty$.

From the inequalities on $N(\alpha) = |\alpha|^2$, $|1+i|^k \leq |\alpha| < |1+i|^{k+1}$, so $1 \leq |\alpha/(1+i)^k| < |1+i|$. In the annulus $\{z : 1 \leq |z| < |1+i|\}$, the points farthest away from ± 1 and $\pm i$ are $\pm 1 \pm i$ (independent signs), at distance 1. We can't have $\alpha/(1+i)^k = \pm 1 \pm i$, since then $|\alpha| = |1+i|^{k+1}$, so $N(\alpha) = 2^{k+1}$, but actually $N(\alpha) < 2^{k+1}$. Therefore $\alpha/(1+i)^k$ has distance less than 1 from one of ± 1 or $\pm i$: $|\alpha/(1+i)^k - \varepsilon| < 1$ where $\varepsilon \in \{\pm 1, \pm i\}$. Hence $|\alpha - \varepsilon(1+i)^k| < |(1+i)^k|$, so

$$N(\alpha - \varepsilon(1+i)^k) < N((1+i)^k) = 2^k.$$

If $\alpha = \varepsilon(1+i)^k$ then we are done. Otherwise $\alpha - \varepsilon(1+i)^k$ is nonzero and by induction on the norm we can write

$$\alpha - \varepsilon(1+i)^k = a_0 + a_1(1+i) + \cdots + a_\ell(1+i)^\ell,$$

where $a_j \in \{0, \pm 1, \pm i\}$ and $\ell \leq k - 1$. Therefore

$$\alpha = a_0 + a_1(1+i) + \cdots + a_\ell(1+i)^\ell + \varepsilon(1+i)^k,$$

which has the desired form. □

Example 7. The number $3 + 4i$ has norm 25, with $2^4 \leq 25 < 2^5$, so $k = 4$. Explicitly, $3 + 4i = 1 - i(1 + i)^2 - i(1 + i)^4$.

Example 8. We can write $3 + i = (1 + i) - i(1 + i)^2$ and $3 + i = -i(1 + i) - i(1 + i)^3$. Since $N(3 + i) = 10$, $k = 3$ and it is the second expression for $3 + i$ that corresponds to Lemma 6, not the first.

Theorem 9. *Let $|\cdot|$ be a nontrivial absolute value on $\mathbf{Q}(i)$. If $|\cdot|$ is nonarchimedean then $|\cdot|$ is a π -adic absolute value for some prime π in $\mathbf{Z}[i]$ that is unique up to unit multiple. If $|\cdot|$ is archimedean then $|\cdot|$ is equivalent to the usual complex absolute value.*

Proof. Our treatment of the non-archimedean case will be similar to the non-archimedean case in the proof of Ostrowski's theorem over \mathbf{Q} , but it will be logically self-contained. However, when it comes to the archimedean case we will actually use Ostrowski's theorem over \mathbf{Q} to know how the absolute value on $\mathbf{Q}(i)$ already looks on the subfield \mathbf{Q} .

Since $|\cdot|$ is nontrivial on $\mathbf{Q}(i)$ and every element of $\mathbf{Q}(i)$ is a ratio of elements of $\mathbf{Z}[i]$, we must have $|\alpha| \neq 1$ for some nonzero α in $\mathbf{Z}[i]$.

First assume $|\alpha| \leq 1$ for all α in $\mathbf{Z}[i]$. In particular, $|n| \leq 1$ for all $n \in \mathbf{Z}$, so $|\cdot|$ is non-archimedean. Because $|\cdot|$ is nontrivial, $|\alpha| < 1$ for some nonzero α in $\mathbf{Z}[i]$. Let π be an element of $\mathbf{Z}[i]$ with the *least norm* satisfying $|\pi| < 1$. That is, $|\pi| < 1$ and if $N(\alpha) < N(\pi)$ with $\alpha \neq 0$ then $|\alpha| = 1$. We will show π is prime and that $|\cdot|$ is a π -adic absolute value.

First we observe π is not a unit in $\mathbf{Z}[i]$, since the units in $\mathbf{Z}[i]$ are roots of unity and roots of unity always have absolute value 1. Therefore $N(\pi) > 1$, so if π is not prime then we can write $\pi = \alpha\beta$ where α and β are both non-units. That means α and β are not 1, -1 , i , or $-i$, so α and β both have norm greater than 1. Since $N(\pi) = N(\alpha)N(\beta)$, with both factors on the right being greater than 1, both α and β have smaller norm than π does. Therefore $|\alpha| = 1$ and $|\beta| = 1$, by the minimality of π , but then $|\pi| = |\alpha\beta| = 1$, a contradiction. Hence π is prime in $\mathbf{Z}[i]$.

Now pick a nonzero $x \in \mathbf{Z}[i]$ and pull out the largest power of π from it: $x = \pi^n y$, where $y \in \mathbf{Z}[i]$ and π doesn't divide y . So $n = \text{ord}_\pi(x)$ and $|x| = |\pi|^n |y|$. We will show y has absolute value 1. Use the division algorithm in $\mathbf{Z}[i]$ to write $y = \pi\gamma + \rho$ where $N(\rho) < N(\pi)$. As π doesn't divide y , ρ is nonzero. Then $|\rho| = 1$ because ρ is a nonzero number in $\mathbf{Z}[i]$ with smaller norm than π . (Recall the way we defined π .) Therefore $|\pi\gamma| \leq |\pi| < 1$ and $|\rho| = 1$, so by the non-archimedean property $|y| = |\pi\gamma + \rho| = 1$. Hence

$$|x| = |\pi|^n |y| = |\pi|^n = |\pi|^{\text{ord}_\pi(x)}.$$

Since both sides are multiplicative in x , this equation in $\mathbf{Z}[i]$ extends to $\mathbf{Q}(i)$ by writing an element of $\mathbf{Q}(i)$ as a ratio from $\mathbf{Z}[i]$. Set $c = |\pi| < 1$, so $|\cdot| = c^{\text{ord}_\pi(\cdot)}$ is a π -adic absolute value.

If we replace π by a unit multiple π' then we don't change the valuation function: $\text{ord}_\pi = \text{ord}_{\pi'}$, so $|\cdot|$ is also a π' -adic absolute value. To show $|\cdot|$ can only be a π' -adic absolute value when π' is a unit multiple of π , let π' be a prime in $\mathbf{Z}[i]$ that is not a unit multiple of π . Then π' is not divisible by π , so from our work above we have $|\pi'| = 1$. This is not how π' -adic absolute values behave, so $|\cdot|$ is not π' -adic.

Now assume $|\alpha| > 1$ for some $\alpha \in \mathbf{Z}[i]$. Then $|\cdot|$ has values > 1 on \mathbf{Z} , as otherwise $|\cdot|$ is nonarchimedean and then $|a + bi| \leq 1$ for each nonzero $a + bi \in \mathbf{Z}[i]$. From Ostrowski's theorem on \mathbf{Q} , there is $t > 0$ such that $|n| = n^t$ for all $n \in \mathbf{Z}^+$. In particular, since $2 = -i(1 + i)^2$ we have $|1 + i|^2 = |2| = 2^t$, so $|1 + i| = 2^{t/2} > 1$. We'll write elements of $\mathbf{Z}[i]$ in base $1 + i$, in accordance with Lemma 6.

Pick nonzero $\alpha \in \mathbf{Z}[i]$ and set $2^k \leq N(\alpha) < 2^{k+1}$, where $k \geq 0$. Since $N(\alpha) = |\alpha|_\infty^2$, $2^{k/2} \leq |\alpha|_\infty < 2^{(k+1)/2}$. Writing α as in Lemma 6,

$$\begin{aligned} |\alpha| &\leq 1 + |1+i| + \cdots + |1+i|^k \\ &= \frac{|1+i|^{k+1} - 1}{|1+i| - 1} \\ &< \frac{|1+i|}{|1+i| - 1} |1+i|^k \\ &= \frac{|1+i|}{|1+i| - 1} 2^{tk/2} \\ &\leq \frac{|1+i|}{|1+i| - 1} |\alpha|_\infty^t. \end{aligned}$$

So $|\alpha| < C|\alpha|_\infty^t$ for all nonzero α in $\mathbf{Z}[i]$, where $C = |1+i|/(|1+i|-1)$. By the power trick (replacing α with α^N , taking N th roots, and letting $N \rightarrow \infty$), we get $|\alpha| \leq |\alpha|_\infty^t$ for all α in $\mathbf{Z}[i]$.

At this point in the proof of Ostrowski's theorem in \mathbf{Q} , the reverse inequality is obtained by returning to the base expansions again. Instead, we will use the inequality already obtained in order to show $|\alpha| = |\bar{\alpha}|$ for all α in $\mathbf{Z}[i]$ and wrap up the proof from that.

If there is an α such that $|\alpha| \neq |\bar{\alpha}|$, then replacing α by $\bar{\alpha}$ if necessary we may suppose $|\bar{\alpha}| < |\alpha|$. Then multiplying both sides by $|\alpha|$, $|\alpha\bar{\alpha}| < |\alpha|^2 \leq |\alpha|_\infty^{2t}$. Also, $|\alpha\bar{\alpha}| = |N(\alpha)| = N(\alpha)^t = |\alpha|_\infty^{2t}$, so $|\alpha|_\infty^{2t} < |\alpha|_\infty^{2t}$. This is absurd.

Now that we have $|\alpha| = |\bar{\alpha}|$ for all $\alpha \in \mathbf{Z}[i]$,

$$|\alpha|^2 = |\alpha\bar{\alpha}| = |N(\alpha)| = N(\alpha)^t = |\alpha|_\infty^{2t},$$

so $|\alpha| = |\alpha|_\infty^t$ for all α in $\mathbf{Z}[i]$. Taking ratios shows this same equation holds for all α in $\mathbf{Q}(i)$ and we're done. \square

Having found all the nontrivial absolute values are on $\mathbf{Q}(i)$, we can establish a product formula on $\mathbf{Q}(i)$. As with the product formula on \mathbf{Q} , a product formula on $\mathbf{Q}(i)$ requires a *compatible* choice of constants for different non-archimedean absolute values. On \mathbf{Q} , the constants are $1/p$ for different primes p . We will use the same idea on $\mathbf{Q}(i)$ with norms of primes: for a prime π in $\mathbf{Z}[i]$ and x in $\mathbf{Q}(i)$, set

$$|x|_\pi = \left(\frac{1}{N(\pi)} \right)^{\text{ord}_\pi(x)}.$$

Example 10. By Example 5,

$$|19 + 83i|_{1+i} = \frac{1}{2}, \quad |19 + 83i|_3 = 1, \quad |19 + 83i|_{1+2i} = \frac{1}{125}.$$

Also set $|x|_1 = |x|_\infty^2$. That is, $|a + bi|_1 = |a + bi|_\infty^2 = a^2 + b^2$ is the square of the usual absolute value on \mathbf{C} . While $|\cdot|_1$ is multiplicative, it is not an absolute value since it fails the triangle inequality. But we do have $|x + y|_1 \leq 2(|x|_1 + |y|_1)$, so we can use $|\cdot|_1$ in place of $|\cdot|_\infty$ to talk about convergence and nothing is really lost. We need $|\cdot|_1$ (a squared absolute value) to get the product formula to work out. Here it is.

Theorem 11. For each nonzero $x \in \mathbf{Q}(i)$,

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

where the product runs over inequivalent nontrivial absolute values on $\mathbf{Q}(i)$ that are chosen according to the above conventions using $1/N(\pi)$ for the non-archimedean case and using the squared absolute value in the archimedean case.

Proof. For nonzero x , $|x|_v = 1$ for all but finitely many of the absolute values since the numerator and denominator of x are divisible by only finitely many primes in $\mathbf{Z}[i]$. The product $\prod_v |x|_v$ is multiplicative in x , so to check this is always 1 it suffices to check it on nonzero elements of $\mathbf{Z}[i]$. Since units and primes generate $\mathbf{Z}[i]$ multiplicatively, it suffices to check the product formula on units and primes.

The units in $\mathbf{Z}[i]$ are ± 1 and $\pm i$, which are roots of unity, so the product formula is obvious on units because every absolute value of a root of unity is 1.

Taking $x = \pi$ to be a prime in $\mathbf{Z}[i]$, the left side of the product formula has only two terms that are not automatically 1, namely $|\pi|_1$ and $|\pi|_\pi$. Therefore

$$\prod_v |\pi|_v = |\pi|_1 |\pi|_\pi = |\pi|_\infty^2 \frac{1}{N(\pi)},$$

which is 1 since $|a + bi|_\infty^2 = a^2 + b^2 = N(a + bi)$ for $a, b \in \mathbf{Z}$. □