(*September 29, 2011*)

Number theory exercises-discussion 02

Paul Garrett garrett@math.umn.edu http://www.math.umn.edu/˜garrett/

Due Fri, 30 Sept 2011, preferably as PDF emailed to me.

[number theory 02.1] Show that the *ideal* norm and *Galois* norm agree on $\mathbb{Z}[i]$. That is, show that for $0 \neq \alpha \in \mathbb{Z}[i]$,

$$\mathrm{card}\,\mathbb{Z}[i]/\big(\alpha \cdot \mathbb{Z}[i]\big) \;=\; \alpha \cdot \overline{\alpha}$$

[I'll write a solution in a style that may suggest how this would work in other situations, as well. In particular, it is easily possible to give less-fancy arguments.]

It will become apparent that everything reduces to the case that α is *prime* in $\mathbb{Z}[i]$, so we treat this case first. Let σ be the non-trivial Galois automorphism of $\mathbb{Q}(i)$ over $\mathbb{Q}$.

When the Galois norm of α is a rational prime p, that is, when $\alpha \cdot \alpha^\sigma = p$, neither α nor α^σ can be a *unit*, so p is *split* or else $p = 2$. For split p,

$$\mathbb{Z}[i]/\alpha \oplus \mathbb{Z}[i]/\alpha^\sigma \;\approx\; \mathbb{Z}[i]/p \;\approx\; \mathbb{F}_p[x]/x^2+1 \;\approx\; \mathbb{F}_p[x]/x-\rho \;\oplus\; \mathbb{F}_p[x]/x+\rho$$

where ρ is a square root of -1 in $\mathbb{F}_p$. Both the last two summands are $\mathbb{F}_p$ again, because in those quotients x is mapped to $\pm\rho \in \mathbb{F}_p$. Thus, the cardinality of $\mathbb{Z}[i]/p$ is p^2. The Galois automorphism maps cosets $\beta + \mathbb{Z}[i]\cdot\alpha$ to cosets $\beta^\sigma + \mathbb{Z}[i]\cdot\alpha^\sigma$, so the two quotients $\mathbb{Z}[i]/\alpha$ and $\mathbb{Z}[i]/\alpha^\sigma$ have the same cardinality, necessarily p, as desired.

The case that the ideal norm of α is $p = 2$ can be brute-forced, if wished, or can be treated similarly to the general prime-power case, below.

In the case that $\alpha = \eta \cdot p$ where η is a unit and p is a *rational* prime, then p has *stayed prime*, so $\mathbb{Z}[i]/p$ is a quadratic field extension of $\mathbb{Z}/p$, so has p^2 elements, as desired.

Thus, Galois norm and ideal norm agree on Gaussian primes.

Sun-Ze's theorem gives $\mathbb{Z}[i]/ab \approx \mathbb{Z}/[i]/a \oplus \mathbb{Z}[i]/b$ for relatively prime Gaussian integers a, b, so the ideal norm N is *multiplicative* in the usual sense that $N(I \cdot J) = NI \cdot NJ$ at least for relatively prime ideals I, J. The Galois norm is multiplicative (because it is a product of field isomorphisms, each of which is multiplicative). Thus, it suffices to compare Galois and ideal norms of *prime powers* $\alpha = \pi^\ell$, and show that

$$\text{ideal norm}(\pi^\ell) \;=\; (\text{ideal norm}\,\pi)^\ell$$

We have a chain of submodules

$$\mathbb{Z}[i]\cdot\pi^\ell \;\subset\; \mathbb{Z}[i]\cdot\pi^{\ell-1} \;\subset\; \mathbb{Z}[i]\cdot\pi^{\ell-2} \;\subset\; \ldots \subset\; \mathbb{Z}[i]\cdot\pi \;\subset\; \mathbb{Z}[i]$$

Every quotient $\mathbb{Z}[i]\pi^{j-1}/\mathbb{Z}[i]\pi^j$ is isomorphic to $\mathbb{Z}[i]/\pi$, by

$$\alpha\pi^{j-1} + \mathbb{Z}[i]\pi^j \;\longrightarrow\; \alpha + \mathbb{Z}[i]\pi$$

Thus, all the indices $[\mathbb{Z}[i]\pi^{j-1} : \mathbb{Z}[i]\pi^j]$ are $[\mathbb{Z}[i] : \mathbb{Z}[i]\pi] = N\pi$, and (by multiplicativity of indices) the whole ideal index is $[\mathbb{Z}[i] : \mathbb{Z}[i]\pi^\ell] = [\mathbb{Z}[i] : \mathbb{Z}[i]\pi]^\ell = (N\pi)^\ell$. This gives the equality of ideal norm and Galois norm on prime powers, and we're done.

[number theory 02.2] Show that in a PID every non-zero prime ideal is maximal.

Let $I = R \cdot p$ be a non-zero prime ideal in a PID R, with $p \in R$. A quick review of the implications of prime-ness: since I is prime, for $ab = p \in I$, either $a \in I$ or $b \in I$, that is, either a or b is divisible by p. For $p|a$, write $a = pa'$. Then $p = ab = pa'b$, so a' and b are *units*, since R is a domain. Let $M = R \cdot m$ be an ideal containing I. Then $p = rm$ for some $r \in R$. By the first part of the discussion, p divides one of r, m, and the other is a unit. Thus, either m is a unit, and $M = R$, or $p|m$, and necessarily $M = I$, so I is maximal.

(A stylistic note: there was no need to argue that there was a maximal proper ideal M containing I.)

[number theory 02.3] Carefully show that for a, b in a commutative ring R, with $\overline{a}$ the image of a in $R/\langle b\rangle$ and $\overline{b}$ the image of b in $R/\langle a\rangle$, there is a natural isomorphism

$$(R/\langle a\rangle)/\langle \overline{b}\rangle \;\approx\; (R/\langle b\rangle)/\langle \overline{a}\rangle$$

Naturally, we claim that this isomorphism is given by a natural isomorphism of *both* to $R/\langle a, b\rangle$. By symmetry in a, b, it suffices to show

$$(R/\langle a\rangle)/\langle \overline{b}\rangle \;\approx\; R/\langle a, b\rangle$$

and we anticipate that the identity map $R \to R$ induces this isomorphism on the quotients. Indeed, in the usual construction of quotients, elements $\overline{r} \in R/\langle a\rangle$ are cosets $r + Ra$, and elements of the double quotient are cosets

$$(r + Ra) + R\overline{b} \;=\; (r + Ra) + R(b + Ra) \;=\; r + Ra + Rb$$

The cosets $r + Ra + Rb$ are also elements of $R/\langle a, b\rangle$. Thus, the map $(r + Ra) + R\overline{b} \to r + Ra + Rb$ is a *well-defined bijection*, which is the essential point.

We could also use the *mapping-property characterization* of quotients: a quotient R/I is characterized by the property that any ring hom $R \to R'$ with kernel containing I *factors through* the quotient map $R \to R/I$, and *uniquely* so. Since $R \to (R/a)/\overline{b}$ kill off a and b, it factors through $R/\langle a, b\rangle$. On the other hand, $R \to R/\langle a, b\rangle$ kills off a, first, so factors through R/a; the resulting map $R/a \to R/\langle a, b\rangle$ kills off $\overline{b}$, so *further* factors through $(R/a)/\overline{b}$. Uniquely. Thus, there are *unique* maps (ring homs!) both ways, which therefore must be mutual inverses, so isomorphisms.

How clear *should* it be that this bijection is a ring homomorphism? We could explicitly verify it from the coset description, which wouldn't be hard, but the mapping-property version makes it obviously inevitable, so we don't have to do it. Good.

[number theory 02.4] For rational $p > 2$ splitting in $\mathbb{Z}[i]$, and for ρ any representative in $\mathbb{Z}$ for a square root of -1 mod p, show that the pairs $p, \rho - i$ and $p, \rho + i$ generate the two prime ideals into which $p \cdot \mathbb{Z}[i]$ factors.

Let $I = \langle \rho - i, p\rangle$ and $J = \langle \rho + i, p\rangle$. Let σ be the non-trivial Galois automorphism. Note that $I^\sigma = J$. Certainly both I, J *contain* $p \cdot \mathbb{Z}[i]$.

If $\rho - i = \alpha \cdot p$ for some $\alpha \in \mathbb{Z}[i]$, then application of σ gives $\rho + i = \alpha^\sigma \cdot p$, and p would divide the difference $(\rho - i) - (\rho + i) = -2i$, which is not the case. Thus, both I, J are strictly larger ideals than $p \cdot \mathbb{Z}[i]$.

On the other hand, writing $p = \pi_1\pi_2$ with Gaussian primes π_1 and π_2, we claim that the *only* proper ideals in $\mathbb{Z}[i]$ *strictly* containing $\mathbb{Z}[i] \cdot p$ are $\mathbb{Z}[i] \cdot \pi_1$ and $\mathbb{Z}[i] \cdot \pi_2$. Indeed, for $\mathbb{Z}[i] \cdot \alpha$ to strictly contain $\mathbb{Z}[i] \cdot p$, entails that α divides p but not vice-versa. That is, α is a *proper* factor of $p = \pi_1\pi_2$. Up to Gaussian units, the only possibilities are π_1 and π_2.

Thus, since there are just the two proper ideals strictly containing $\mathbb{Z}[i] \cdot p$, they must be the ideals $\langle \rho \pm i, p\rangle$.

[number theory 02.5] Show that $\mathbb{Z}[\sqrt{2}]$ is Euclidean.

Even though the norm $N(a+b\sqrt{2}) = a^2 - 2b^2$ is not *positive-definite*, we can still use it to execute a Euclidean algorithm, since on $\mathbb{Z}[\sqrt{2}]$ it is integer-valued.

We must prove that, given $\alpha \in \mathbb{Z}[\sqrt{2}]$ and given $0 \neq \delta \in \mathbb{Z}[\sqrt{2}]$, there is $q \in \mathbb{Z}[\sqrt{2}]$ such that the remainder $\alpha - q \cdot \delta$ is smaller than the divisor δ, that is,

$$|N(\alpha - q \cdot \delta)| \; < \; |N\delta|$$

Dividing through by δ, we must show that, given $\alpha = a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, there is $q = u + v\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ such that $|N(\alpha - q)| \; < \; 1$. Indeed, let u, v be rational integers nearest a, b, so $|a - u| \leq \frac{1}{2}$ and $|b - v| \leq \frac{1}{2}$. Then

$$|N(\alpha - q)| \; = \; |(a-u)^2 - 2(b-v)^2| \; \leq \; (a-u)^2 + 2(b-v)^2 \; \leq \; \left(\tfrac{1}{2}\right)^2 + 2 \cdot \left(\tfrac{1}{2}\right)^2 \; \leq \; \frac{3}{4} \; < \; 1$$
