MATH 403 Winter 2018
Homework 7
Winter 2018

- **Problem 2**

  1. One checks that the norm $N(a+bi) = a^2 + b^2$ satisfies the property that if $N(\alpha)$ is a prime integer, then α is irreducible in $\mathbf{Z}[i]$. Writing an integer $n = a^2 + b^2$ as a sum of two squares yields a factorization $n = (a+bi)\cdot(a-bi)$ in $\mathbf{Z}[i]$. Here $13 = 3^2 + 2^2$ and $17 = 1^2 + 4^2$. Hence

  $$\begin{aligned} 13 =& (3+2i)(3-2i) \\ 17 =& (1+4i)(1-4i) \end{aligned}$$

     Then as was noted above, $3 \pm 2i$ and $1 \pm 4i$ has prime norm. This shows that the two factorizations I just wrote down are the factorizations of 13 and 17 into irreducible factors.

  2. $$\begin{aligned} 221 = 13 \cdot 17 = (3+2i)(3-2i)\cdot(1+4i)(1-4i) =& (3+2i)(1+4i)\cdot(3-2i)(1-4i) \\ = (-5+14i)\cdot(-5-14i) =& 5^2 + 14^2 \end{aligned}$$

     On the other hand we have $221 = (3+2i)(1-4i)\cdot(3-2i)(1+4i) = 11^2 + 10^2$.

- **Problem 3 and 6**

  Four properties of ω will be used:

  - $\omega = \frac{-1}{2} + \frac{\sqrt{3}}{2}i$;
  - $\omega^2 + \omega + 1 = 0$
  - $\omega \cdot \bar{\omega} = 1$ and
  - $\omega + \bar{\omega} = -1$

  Step 1: A better description of $\mathbf{Z}[\omega]$.
  By property 2, $a + b\omega + c\omega^2 = (a-c) + (b-c)\omega$. Hence every element in $\mathbf{Z}[\omega]$ can be written as $a + b\omega$ for some $a, b \in \mathbf{Z}$. I claim that such expression is actually unique. For this, if $a + b\omega = a' + b'\omega$, then using the first property, we get

  $$a - \frac{b}{2} + \frac{\sqrt{3}b}{2}i = a' - \frac{b'}{2} + \frac{\sqrt{3}b'}{2}i.$$

  Comparing the real and imaginary parts, we conclude that

  $$\begin{aligned} a - \frac{b}{2} =& a' - \frac{b'}{2} \\ \frac{\sqrt{3}b}{2} =& \frac{\sqrt{3}b'}{2} \end{aligned}$$

  Hence $a = a'$ and $b = b'$.

  Step 2: Define a multiplicative norm N on $\mathbf{Z}[\omega]$.
  Inspired by our previous experiences of constructing norms, one naturally tries (and pray)

  $$N(a + b\omega) := (a + b\omega)\cdot\overline{(a + b\omega)}.$$

Since $\overline{a+b\omega} = a + b\bar{\omega}$, with property 3 and 4 of ω, we have

$$(a+b\omega)\cdot(a+b\bar{\omega}) = a^2 - ab + b^2.$$

Since this is just the complex norm of $a+b\omega$, the function N is multiplicative. Moreover this also implies $N(a+b\omega)$ is non-negative. One can also check this by looking at the discriminant of the quadric a^2-ab+b^2. For example, for every fixed $b \in \mathbf{Z}$, the discriminant $D(b)$ is $b^2-4b^2=-3b^2$. So when $b=0$, the norm is a^2, which is non-negative. When $b \neq 0$, $D(b) < 0$ so a^2-ab+b^2 is either positive or negative as a function in a. Plugging in $a=0$, we get a positive value so a^2-ab+b^2 is strictly greater than zero as a function of a with a fixed non-zero b.

Step 3: Check that N we just defined is a Euclidean norm.
$\mathbf{Z}[\omega] \subset \mathbf{C}$ is a subring. Hence $\mathbf{Z}[\omega]$ is an integral domain. N is non-negative as we have seen. The main task is to show that for any $a+b\omega$ and $c+d\omega$, either $c+d\omega | a+b\omega$ or there exist $m+n\omega$ and $r+s\omega$ such that

$$a+b\omega = (m+n\omega)\cdot(c+d\omega) + r + s\omega$$

with $N(r+s\omega) < N(c+d\omega)$. Suppose $c+d\omega$ does not divide $a+b\omega$. Then in $\mathbf{C}$, with property 4 of ω we have

$$\frac{a+b\omega}{c+d\omega} = \frac{(a+b\omega)(c+d\bar{\omega})}{(c+d\omega)(c+d\bar{\omega})} = \frac{ac+bd-ad}{N(c+d\omega)} + \frac{bc-ad}{N(c+d\omega)}\omega.$$

Let $\alpha = \frac{ac+bd-ad}{N(c+d\omega)}$ and $\beta = \frac{bc-ad}{N(c+d\omega)}$. Choosing $m, n \in \mathbf{Z}$ such that $|m-\alpha| \leq \frac{1}{2}$ and $|n-\beta| \leq \frac{1}{2}$, we have

$$a+b\omega = (c+d\omega)(m+n\omega) + (c+d\omega)(\alpha - m + (\beta - n)\omega).$$

Since $a+b\omega$ and $(c+d\omega)(m+n\omega) \in \mathbf{Z}[\omega]$, $(c+d\omega)(m-\alpha+(n-\beta)\omega) \in \mathbf{Z}[\omega]$. Set $r+s\omega = (c+d\omega)\alpha - m + (\beta-n)\omega)$. Then to prove $N(r+s\omega) < N(c+d\omega)$, it is sufficient to prove that the complex norm $|\alpha - m + (\beta-n)\omega| < 1$. But this follows from our choice of m and n. So far we have done problem 3.

Step 4: Compute the units of $\mathbf{Z}[\omega]$.
I claim that $\alpha \in \mathbf{Z}[\omega]$ is a unit if and only if $N(\alpha) = 1$. If α is a unit, then

$$1 = N(1) = N(\alpha\cdot\alpha^{-1}) = N(\alpha)N(\alpha^{-1}).$$

Since N is non-negative, we see that $N(\alpha) = 1$. But $1 = a^2-ab+b^2$ only when $(a,b) = (\pm1, 0), (0, \pm1), (1,1), (-1,-1)$. We see that the possible choices of a unit is ±1, $\pm\omega$, $1+\omega$ and $-1-\omega$. One easily checks that these are units. Therefore the claim is proved.

Step 5: 7.6(a) $\iff$ 7.6(b)
The ring map $\varphi : \mathbf{Z}[x] \to \mathbf{Z}[\omega]$ that sends x to ω is surjective. Let me show that φ has kernel

(x^2+x+1), namely, if $f \in \mathbf{Z}[x]$ is a polynomial such that $f(\omega) = 0$ as complex numbers, then $x^2+x+1|f$. This is because if $\alpha \in \mathbf{C}$ is a complex root for f, then

$$0 = f(\alpha) = \overline{f(\alpha)} = f(\bar{\alpha})^1.$$

So $\bar{\alpha}$ is also a complex root for f. We know that ω and $\bar{\omega}$ are the two roots of x^2+x+1 as $(x-\omega)(x-\bar{\omega}) = x^2+x+1$. Hence if $f(\omega) = 0$, then $f(\bar{\omega}) = 0$. Viewing f as a polynomial in $\mathbf{C}[x]$, we see that both $(x-\omega)$ and $(x-\bar{\omega})$ divides f. Therefore, $x^2+x+1|f$ inside $\mathbf{C}[x]$. With a bit of work one shows that if $(x^2+x+1)\cdot g(x) = f(x)$ in $\mathbf{C}[x]$, then g has integral coefficients, meaning that $x^2+x+1|f$ in $\mathbf{Z}[x]$. Hence φ has kernel (x^2+x+1). By the first isomorphism theorem, we have

$$\mathbf{Z}[x]/(x^2+x+1) \simeq \mathbf{Z}[\omega].$$

Given a prime integer p, the prime ideal $(p) \subset \mathbf{Z}[\omega]$ corresponds to the ideal $(p+(x^2+x+1)) = (p, x^2+x+1)/(x^2+x+1) \subset \mathbf{Z}[x]/(x^2+x+1)$. Observing that $\mathbf{Z} \twoheadrightarrow \mathbf{Z}/p$ induces an isomorphism

$$\mathbf{Z}[x]/p \simeq (\mathbf{Z}/p)[x]$$

and using the third isomorphism theorem, we get that

$$\begin{aligned}
\mathbf{Z}[\omega]/(p) \simeq &(\mathbf{Z}[x]/(x^2+x+1))/((p, x^2+x+1)/(x^2+x+1)) \\
\simeq &\mathbf{Z}[x]/(p, x^2+x+1) \\
\simeq &(\mathbf{Z}[x]/p)/((p, x^2+x+1)/p) \\
\simeq &(\mathbf{Z}/p)[x]/(x^2+x+1).
\end{aligned}$$

By step 3, $\mathbf{Z}[\omega]$ is a PID. Hence $p \subset \mathbf{Z}[\omega]$ is irreducible if and only if $(p) \subset \mathbf{Z}[\omega]$ is maximal if and only if $\mathbf{Z}[\omega]/(p)$ is a field. By the fact that $\mathbf{Z}[\omega]/(p) \simeq (\mathbf{Z}/p)[x]/(x^2+x+1)$, this is equivalent to that $(x^2+x+1) \subset (\mathbf{Z}/p)[x]$ is a maximal ideal. But $(\mathbf{Z}/p)[x]$ is a PID, hence this is equivalent to that x^2+x+1 is irreducible in $(\mathbf{Z}/p)[x]$.

Step 6: Problem 7.6(a).
Suppose x^2+x+1 has a root α in $\mathbf{Z}/p$, then

$$\alpha^3 - 1 = (\alpha-1)\cdot(\alpha^2+\alpha+1) = 0.$$

Since $p \neq 3$, $\alpha \neq 1$. Therefore the order of α is three. The order of α divides the order of the multiplicative group $(\mathbf{Z}/p)^\times$, which has order $p-1$. Therefore, $3|p-1$. Conversely, if $3|p-1$, say $3k = p-1$, then

$$x^{p-1} - 1 = (x^{\frac{p-1}{3}} - 1)(x^{\frac{2(p-1)}{3}} + x^{\frac{p-1}{3}} + 1).$$

But we know $x^{p-1}-1$ factors into distinct linear polynomials in $\mathbf{Z}/p$. Since $(\mathbf{Z}/p)[x]$ is a UFD, some linear factor of $x^{p-1}-1$ divides $x^{\frac{2(p-1)}{3}} + x^{\frac{p-1}{3}} + 1$, meaning that there is an $\alpha \in \mathbf{Z}/p$ such that $\alpha^{\frac{2(p-1)}{3}} + \alpha^{\frac{p-1}{3}} + 1 = 0$ in $\mathbf{Z}/p$. Let $\beta = \alpha^{\frac{p-1}{3}}$, we see that x^2+x+1 has a root β in $\mathbf{Z}/p$.

[1] Make sure you understand where integrality of f is used! In fact, we only need that f has real coefficients.

Step 7: Problem 7.6(c)
Suppose $p = \alpha \cdot \beta$ where both α and β are not units in $\mathbf{Z}[\omega]$. Then

$$p^2 = N(p) = N(\alpha)N(\beta).$$

By step 4, $N(\alpha), N(\beta) > 1$. So we can only have $N(\alpha) = N(\beta) = p$. Then $p = a^2 - ab + b^2$ for some integers a, b. Conversely, if $p = a^2 - ab + b^2$, then $p = (a + b\omega) \cdot (a + b\bar{\omega}) = (a + b\omega) \cdot (a - b - b\omega)$. Since $N(a - b\omega) = N(a + b\bar{\omega}) = p > 1$, we see that both $a + b\omega$ and $a + b\bar{\omega}$ are not units. Hence p factors in $\mathbf{Z}[\omega]$.

- **Problem 7.8**
  See Theorem 9.10 of `http://www.math.uconn.edu/~kconrad/blurbs/ugradnumthy/Zinotes.pdf`.