Advanced Algebra HW3

October 20, 2008

1. Let $z = a + bi \in \mathbb{C}$ where $a, b \in \mathbb{R}$, and $N(z) := a^2 + b^2$ is the *norm* of z. Let $\mathbb{Z}[\sqrt{-d}] := \{a + b\sqrt{-d} \mid a, b \in \mathbb{Z}\}$, where $d \in \mathbb{N}$.
   (a) Show $N(zz') = Z(z)N(z')$ for $z, z' \in \mathbb{C}$.
   (b) For $z \in \mathbb{Z}[\sqrt{-d}]$ show that $N(z)$ is a nonnegative integer.
   (c) Show that the element $z \in \mathbb{Z}[\sqrt{-d}]$ is a unit if and only if $N(z) = 1$.
   (d) Let $N(z)$ be a prime integer. Show hat z is irreducible in $\mathbb{Z}[\sqrt{-d}]$.
   (e) Find all units of $\mathbb{Z}[\sqrt{-5}]$.
   (f) Show that 3 is irreducible in $\mathbb{Z}[\sqrt{-5}]$.
   (g) Show that 3 is not a prime in $\mathbb{Z}[\sqrt{-5}]$.

   Solution:
   (a) Since $N(z) = z\overline{z}$, $N(zz') = zz' \cdot \overline{zz'} = zz'\overline{z}\overline{z'} = z\overline{z}z'\overline{z'} = N(z)N(z')$.
   (b) Let $z \in \mathbb{Z}[\sqrt{-d}]$. Then $z = a + b\sqrt{-d} = a + b\sqrt{d}i$. $N(z) = a^2 + b^2d \in \mathbb{N}$, since $a, b \in \mathbb{Z}$ and $d \in \mathbb{N}$.
   (c) ($\Rightarrow$) Let $z = a + b\sqrt{-d} = a + b\sqrt{-d}$ is a unit. Then $\exists z'$ s.t $zz' = 1$. $N(1) = N(z)N(z')$. This implies $N(z) = 1$.
   ($\Leftarrow$) $z = a + b\sqrt{-d} \in \mathbb{Z}[\sqrt{-d}]$. $N(z) = a^2 + b^2d = 1$. Take $z' = a - b\sqrt{-d}$. $zz' = (a + b\sqrt{-d})(a - b\sqrt{-d}) = a^2 + b^2d = 1$. Hence z is a unit.
   (d) $N(z)$ is a prime. Then $z \neq 0$ and z is not a unit. Let $z = z_1z_2$.
   Claim: z_1 is a unit or z_2 is a unit.
   $p = N(z) = N(z_1)N(z_2)$, where p is a prime integer. W.L.O.G, $N(z_1) = 1$, by (c), z_1 is a unit.
   (e) Let $z = a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ be a unit. By (c), $N(z) = 1$. Then $a^2 + 5b^2 = 1$. Since $a, b \in \mathbb{Z}$, $a = \pm 1$ and $b = 0$. Thus $z = \pm 1$.
   (f) $3 \neq 0$ and 3 is not a unit. $\because N(3) = 9 \neq 1$. Suppose $3 = \alpha\beta$, where $\alpha = a + b\sqrt{-5}, \beta = a' + b'\sqrt{-5}, a, b, a', b' \in \mathbb{Z}$. Claim: α or β is unit
   Suppose not. α and β are not unit. By (a), we have $N(\alpha)N(\beta) = N(3) = 9$. By (c), α, β are not unit. $N(\alpha)$ and $N(\beta)$ are not equal to 1. Thus, we have $N(\alpha) = N(\beta) = 3$. That is $a^2 + 5b^2 = 3$ and $a'^2 + 5b'^2 = 3$, $a, b, a', b' \in \mathbb{Z}$. This is impossible. Hence α or β is unit.
   (g) $3 \neq 0$ and 3 is not a unit. $3 \mid 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. But $3 \nmid (1 + \sqrt{-5})$. $\because N(3) = 9 \nmid N(1 + \sqrt{-5}) = 6$. Similarly $3 \nmid (1 - \sqrt{-5})$. Hence 3 is not a prime in $\mathbb{Z}[\sqrt{-5}]$.

2. Let S be a nonempty subset of a commutative ring R. An element $d \in R$ is said to be a *greatest common divisor* of X if (i) $d|a$ for all $a \in S$; (ii) If $c|a$ for all $a \in S$, then $c|d$. The *least common multiple* of X can be defined similarly.
   (a) Find the greatest common divisor of 2 and $1 + \sqrt{-5}$ in $\mathbb{Z}[\sqrt{-5}]$.

(b) Find the greatest common divisor of $6-6\sqrt{-5}$ and 18 in $\mathbb{Z}[\sqrt{-5}]$.

Solution:

(a) $N(1+\sqrt{-5})=6=\begin{cases}2\times 3\\ 1\times 6\end{cases}$ By (f), this is impossible.
$\because \forall z, N(z)\neq 3$, by (f). By (c), $1+\sqrt{-5}=zz'$, one of them is unit. Hence $1+\sqrt{-5}$ is irreducible. $1+\sqrt{-5}=1\times(1+\sqrt{-5})=(-1)\times(-1-\sqrt{-5})$.
$2=(1+\sqrt{-5})\times(a+b\sqrt{-5})=(a-5b)+(a+b)\sqrt{-5}$.
This implies that $\begin{cases}a-5b=2\\ a+b=0\end{cases}$ Then $b=-\frac{1}{3}, a=\frac{1}{3}$, a contradiction.
($\because a,b\in\mathbb{Z}$.) Hence $gcd(1+\sqrt{-5},2)=1$.

(b) Suppose $gcd(6-6\sqrt{-5},18)=a$.
Then (1) $6\mid a$ and (2) a,b are associate. $a=6c$ and $N(c)\neq 1$.
Then

1. $N(a)=N(6)N(c)=36N(c)$.
2. $N(a)\mid N(18)=2^2\times 3^4$. and $N(a)\mid N(6-6\sqrt{-5})=2^3\times 3^3$.

Then $36\mid N(a)$. Thus $N(a)=36\times 3$. This implies $N(c)=3$, a contradiction. Hence no such a exists.

3. An commutative integral domain D is a *Euclidean domain* if there is a function $\mu: D\setminus\{0\}\to\mathbb{N}$ such that for all $a,b\in D$ with $b\neq 0$, there exist $q,r\in D$ such that $a=bq+r$, where $r=0$ or $\mu(r)<\mu(b)$.

(a) Show that $\mathbb{Z}$ is a Euclidean domain.

(b) Show that every Euclidean domain is a principal ideal domain.

(c) Show that the ring $\mathbb{Z}[\sqrt{-1}]$ is a Euclidean domain.

(d) Find all units of $\mathbb{Z}[\sqrt{-1}]$.

(e) Determine all the prime elements in $\mathbb{Z}[\sqrt{-1}]$.

Solution:

(a) $\mathbb{Z}$ is a commutative integral domain. Define $\mu(b)=|b|, b\neq 0$. $\forall a,b\in\mathbb{Z}, b\neq 0, \exists q,r\in\mathbb{Z}$ s.t $a=bq+r, 0\leq r<|b|=\mu(b)$. Then $\mu(r)<\mu(b)$.

(b) Let I be a nonzero ideal in D. Let $b\in I$ s.t $\mu(b)$ is the least integer in the set $\{\mu(x)|x\in I\}$. If $a\in I, \exists q,r\in D$ s.t $a=bq+r$ where $r=0$ or $\mu(r)<\mu(b)$. $\because a\in I, bq\in I\Rightarrow r\in I$. Since $\mu(b)$ is the least integer, $r=0$. Then $a=bq$. Therefore $I\subseteq(b)$.
$(b)\subseteq I$ is clear. Hence $I=(b)$.

(c) $\mathbb{Z}[\sqrt{-1}]=\{m+ni|m,n\in\mathbb{Z}\}$.
$\forall a,b\in\mathbb{Z}[\sqrt{-1}], \exists q,r\in\mathbb{Z}[\sqrt{-1}]$ s.t $a=bq+r$.
Define $\mu:\mathbb{Z}[\sqrt{-1}]\to\mathbb{N}$ by $\mu(z)=a^2+b^2$ where $z=a+bi$.
Let $a=a_1+a_2i, b=b_1+b_2i, \frac{a}{b}=s+ti, s,t\in\mathbb{Q}$.
Let $m,n\in\mathbb{Z}$ s.t $|s-m|\leq\frac{1}{2}, |t-n|\leq\frac{1}{2}$. $q=m+ni, r=a-bq$.
$\mu(r)=\mu(b(\frac{a}{b}-q))=\mu(b)\mu(\frac{a}{b}-q)=\mu(b)((s-m)^2+(t-n)^2)\leq\mu(b)[(\frac{1}{2})^2+(\frac{1}{2})^2]<\mu(b)$. Then $\mu(r)<\mu(b)$.

(d) Let S be the set of all units in $\mathbb{Z}[\sqrt{-1}]$. Then $S=\{a+bi|a,b\in\mathbb{Z}\text{and } a^2+b^2=1\}$.
$a^2+b^2=1, \because a,b\in\mathbb{Z}\therefore a^2,b^2\geq 0$ and $a^2,b^2\in\mathbb{Z}$. Then $\begin{cases}a^2=1\\ b^2=0\end{cases}$ or $\begin{cases}a^2=0\\ b^2=1\end{cases}$. Thus $\begin{cases}a=\pm 1\\ b=0\end{cases}$ or $\begin{cases}a=0\\ b=\pm 1\end{cases}$. This implies $S=\{\pm 1,\pm i\}$.

(e) Note that an irreducible element in $Z[i]$ is the same as a prime element in $Z[i]$ since $Z[i]$ is UFD. We claim that $\alpha \in \mathbb{Z}[i]$ is irreducible if and only if exactly one of the following holds: (1) $N(\alpha) = 2$, (2)$N(\alpha) \equiv 1 \pmod 4$ is a prime, (3)$\alpha = cp$, where c is a unit in $\mathbb{Z}[i]$, and $p \equiv 3 \pmod 4$ is a prime in $\mathbb{Z}$.

Lemma 1 α is irreducible iff $\overline{\alpha}$ is irreducible.

Proof This is clear.

Lemma 2 If α is irreducible then $N(\alpha) = p$ or p^2, where p is a prime. Furthermore in the case $N(\alpha) = p^2$ we must have $\alpha = cp$ for some unit $c \in \mathbb{Z}[i]$.

Proof. Suppose that $\alpha \in \mathbb{Z}[i]$ is irreducible. By Lemma 1 and the UFD of $\mathbb{Z}[i]$, $\alpha\overline{\alpha} \in \mathbb{Z}$ has two irreducible terms in $\mathbb{Z}[i]$ and hence $\alpha\overline{\alpha}$ has at most two irreducible terms in $\mathbb{Z}$, i.e. $\alpha\overline{\alpha} = p$ or pq, where p, q are primes in $\mathbb{Z}$. We have the lemma except that $\alpha\overline{\alpha} = pq$ and $p \neq q$. In this case we can assume $\alpha = cp$ and $\overline{\alpha} = c^{-1}q = \overline{c}q$, where c is a unit, and then $\overline{cp} = \overline{\alpha} = \overline{c}q$. This forces $p = q$, a contradiction.

The following two lemmas are a little harder to prove, so we skip their proof this time.

Lemma 3 If $\alpha \in \mathbb{Z}$ and $\alpha = 2$ or $\alpha \equiv 1 \pmod 4$ then α is not irreducible in $\mathbb{Z}[i]$.

Lemma 4 If $\alpha \in \mathbb{Z}$ is a prime with $\alpha \equiv 3 \pmod 4$ then α is irreducible.

Proof of the Claim. ($\Longrightarrow$) This is immediate from Lemma 1 and Lemma 2.

($\Longleftarrow$) If $\alpha = \beta\gamma$ is not irreducible in $\mathbb{Z}[i]$ then $\alpha\overline{\alpha} = \beta\gamma\overline{\beta\gamma}$ is not a prime, where α, β are not units, i.e., $N(\alpha), N(\beta) \neq 1$. Then $N(\alpha) = \alpha\overline{\alpha}$ is a product of two sums, each a sum of two squares. This is impossible in one of the first two cases (1) or (2), since $N(\alpha)$ is a prime. In the third case we must have $p^2 = cp\overline{cp} = N(\alpha) = \beta\overline{\beta}\gamma\overline{\gamma}$ and hence $p = \beta\overline{\beta}$, a sum of two squares, a contradiction to $p \equiv 3 \pmod 4$.

(f) $11 + 3i = (1 - 2i)(1 + 5i) = (1 - 2i)(1 + i)(3 + 2i)$
$8 - i = (1 - 2i)(2 + 3i)$. $2 + 3i, 3 + 2i$ are not associate.
Hence $(1 - 2i)$ is the *gcd* and $(1 - 2i)(1 + i)(3 + 2i)(2 + 3i)$ is the *lcm*.