MATH 403 Winter 2018
Homework 6
Winter 2018

1. **Problem Set 6.3(a)** Observe that we have
$$6 = 2 \cdot 3 = (1+\sqrt{-5}) \cdot (1-\sqrt{-5}).$$
As before, the function $N : \mathbf{Z}[\sqrt{-5}] \to \mathbf{Z}$ defined by
$$(a + b\sqrt{-5}) \mapsto a^2 + 5b^2$$
is multiplicative. Hence if $\alpha \in \mathbf{Z}[\sqrt{-5}]$ is a unit, we have
$$1 = N(1) = N(\alpha\alpha^{-1}) = N(\alpha)N(\alpha^{-1}).$$
This shows that $N(\alpha) = \pm 1$ is necessary for α to be unit in $\mathbf{Z}[\sqrt{-5}]$. Conversely, if α is a unit, we have
$$\frac{1}{\alpha} = \frac{\bar{\alpha}}{\alpha\bar{\alpha}} = \frac{\bar{\alpha}}{N(\alpha)} = \pm\bar{\alpha} \in \mathbf{Z}[\sqrt{-5}].$$
We deduce that α is a unit if and only if $N(\alpha) = a^2 + 5b^2 = \pm 1$. In this case we have that α is a unit exactly when $\alpha = \pm 1$. Then clearly 2 is not an associate to $1+\sqrt{-5}$ nor to $1-\sqrt{-5}$. 3 is not an associate to $1+\sqrt{-5}$ nor to $1-\sqrt{-5}$.

2. **Problem 6.5: Judson 18.3.9** The ring $\mathbf{Z}[i]$ is obviously a subring of $\mathbf{Q}(i)$. You can easily check that $\mathbf{Q}(i)$ is a field. Hence the field of fractions Q of $\mathbf{Z}[i]$ is contained inside $\mathbf{Q}(i)$. To see that $Q = \mathbf{Q}(i)$, it remains to show that any element $q_1 + q_2 \cdot i$ for $q_1, q_2 \in \mathbf{Q}$ is actually an element in Q. For this, write $q_1 = \frac{a_1}{b_1}$ and $q_2 = \frac{a_2}{b_2}$ for some $a_1, a_2, b_1, b_2 \in \mathbf{Z}$. Then
$$q_1 + q_2 i = \frac{a_1b_2 + a_2b_1 i}{b_1b_2} = \frac{a_1b_2 + a_2b_1 i}{b_1b_2 + 0i} \in Q.$$

3. **Problem 6.7: Judson 18.3.11**
   (a) $\mathbf{Z}[\sqrt{2}]$ is a subring of $\mathbf{R}$.
   (b) The function $N : \mathbf{Z}[\sqrt{2}] \to \mathbf{Z}$ defined by
   $$N(a + b\sqrt{2}) = a^2 - 2b^2$$
   is multiplicative. Hence if $\alpha \in \mathbf{Z}[\sqrt{2}]$ is a unit, we have
   $$1 = N(1) = N(\alpha \cdot \alpha^{-1}) = N(\alpha) \cdot N(\alpha^{-1}).$$
   Since $N(\alpha) \in \mathbf{Z}$, the only possibility is that $N(\alpha) = \pm 1$. This is a necessary condition for α to be a unit in $\mathbf{Z}[\sqrt{2}]$. Conversely, if $N(\alpha) = \pm 1$, we have
   $$\frac{1}{\alpha} = \frac{\bar{\alpha}}{\alpha\bar{\alpha}} = \frac{\bar{\alpha}}{N(\alpha)} = \pm\bar{\alpha} \in \mathbf{Z}[\sqrt{2}].$$
   Hence $N(\alpha) = \pm 1$ is a necessary and sufficient condition for α to be a unit in $\mathbf{Z}[\sqrt{2}]$. Translating this, we have $\alpha = a + b\sqrt{2}$ is a unit if and only if $a^2 - 2b^2 = \pm 1$.
   (c) Let $\mathbf{Q}(\sqrt{2})$ be the subset of $\mathbf{R}$ defined by $r \in \mathbf{R}$ is in $\mathbf{Q}(\sqrt{2})$ if and only if there are $q_1, q_2 \in \mathbf{Q}$ such that $r = q_1 + q_2 \cdot \sqrt{2}$. You can easily check that $\mathbf{Q}(\sqrt{2})$ is a field that contains $\mathbf{Z}[\sqrt{2}]$. Hence the field Q of fractions of $\mathbf{Z}[\sqrt{2}]$ is contained in $\mathbf{Q}(\sqrt{2})$. Conversely, we have for any $q_1, q_2 \in \mathbf{Q}$, choose $a_1, a_2, b_1, b_2 \in \mathbf{Z}$ such that $q_1 = \frac{a_1}{b_1}$ and $q_2 = \frac{a_2}{b_2}$. Then
   $$q_1 + q_2\sqrt{2} = \frac{a_1b_2 + a_2b_1\sqrt{2}}{b_1b_2} = \frac{a_1b_2 + a_2b_1\sqrt{2}}{b_1b_2 + 0\sqrt{2}} \in Q.$$

(d) Let $a_1+b_1\sqrt{-2}$ and $a_2+b_2\sqrt{-2}$ be two elements in $\mathbf{Z}[\sqrt{-2}]$. The main task is to show that there exist an $m+n\sqrt{-2}\in\mathbf{Z}[\sqrt{-2}]$ and an $r+s\sqrt{-2}\in\mathbf{Z}[\sqrt{-2}]$ such that

- $a_1+b_1\sqrt{-2}=(m+n\sqrt{-2})\cdot(a_2+b_2\sqrt{-2})+(r+s\sqrt{-2})$ and
- $\mu(r+s\sqrt{-2})<\mu(a_2+b_2\sqrt{-2})$.

For this, note that in $\mathbf{C}$, we have

$$\frac{a_1+b_1\sqrt{-2}}{a_2+b_2\sqrt{-2}}=\frac{a_1a_2-2b_1b_2}{a_2^2+2b_2^2}+\frac{a_1b_2+a_2b_1}{a_2^2+2b_2^2}\sqrt{-2}.$$

Choose $m\in\mathbf{Z}$ and $n\in\mathbf{Z}$ so that m is the closest to $\frac{a_1a_2-2b_1b_2}{a_2^2+2b_2^2}$ and n is the closest to $\frac{a_1b_2+a_2b_1}{a_2^2+2b_2^2}$. Let $c_1=\frac{a_1a_2-2b_1b_2}{a_2^2+2b_2^2}-m$ and $c_2=\frac{a_1b_2+a_2b_1}{a_2^2+2b_2^2}-n$. Then necessarily we have

$$|c_1|,|c_2|\leq\frac{1}{2}.$$

Letting $r+s\sqrt{-2}=(c_1+c_2\sqrt{-2})\cdot(a_2+b_2\sqrt{-2})$, we have

$$a_1+b_1\sqrt{-2}=(m+n\sqrt{-2})\cdot(a_2+b_2\sqrt{-2})+r+s\sqrt{-2}.$$

Since $a_1+b_1\sqrt{-2}$ and $m+n\sqrt{-2}$ are in $\mathbf{Z}[\sqrt{-2}]$, we have that $r+s\sqrt{-2}\in\mathbf{Z}[\sqrt{-2}]$. It remains to check that $\mu(r+s\sqrt{-2})<\mu(a_2+b_2\sqrt{-2})$. Since

$$\begin{aligned}\mu(r+s\sqrt{-2})=&(r+s\sqrt{-2})(r-s\sqrt{-2})\\=&(c_1+c_2\sqrt{-2})(c_1-c_2\sqrt{-2})(a_2+b_2\sqrt{-2})(a_2-b_2\sqrt{-2})\\=&(c_1+c_2\sqrt{-2})(c_1-c_2\sqrt{-2})\cdot\mu(a_2+b_2\sqrt{-2}),\end{aligned}$$

it is sufficient to show that $(c_1+c_2\sqrt{-2})\cdot(c_1-c_2\sqrt{-2})<1$. This is clear from the fact that

$$|c_1|,|c_2|\leq\frac{1}{2}.$$

4. **Problem 6.8: Judson 18.3.12**

(a) If d and d' are both greatest common divisors for a,b, then $d|d'$ and $d'|d$. Then there are $r,r'\in D$ such that

$$\begin{aligned}d=&r'd'\\d'=&rd\end{aligned}$$

Then

$$d=rr'd.$$

Since D is an integral domain, we have that $rr'=1$. Hence r,r' are units, meaning that d and d' are associates.

(b) Since D is a PID, the ideal (a,b) is generated by one element d. I claim that d is a greatest common divisor for a,b. Clearly d divides both a and b. If d' divides both a and b then

$$(d)=(a,b)\subset(d').$$

This implies $d'|d$ and shows that d is a greatest common divisor for a,b. The result follows.

5. **Problem 6.9** Suppose r is a prime, then $r = r_1 r_2$ implies either $r|r_1$ or $r|r_2$. If $r|r_1$, we have $r_1 = s_1 r$ for some $s_1 \in R$. Then $r = s_1 r r_2$. Since R is a domain, we get $s_1 r_2 = 1$. Hence r_2 is a unit. We can argue entirely the same if $r|r_2$ and conclude that r_1 is a unit. Hence r is irreducible. Conversely, if r is irreducible and $r|r_1 r_2$. Since R is a UFD, r has to be a factor of r_1 or r_2, showing that r is a prime.