PMAT 431, Fall 2006

Solution to Assignment 1

1. §5.1, # 18: Show that $\mathbb{Z}[\sqrt{5}]$ is not a UFD by showing that $1+\sqrt{5}$ is an irreducible that is not prime. [*Hint*: Use $N(m+n\sqrt{5}) = m^2 - 5n^2$.]

   Solution: It is easily verified that $N(xy) = N(x)N(y)$ holds for all x, y in $\mathbb{Z}(\sqrt{-5})$. Let $p = 1+\sqrt{5}$. If $p = xy$ then $-4 = N(p) = N(x)N(y)$ so $N(x) = \pm 1, \pm 2, \pm 4$. If $x = m+n\sqrt{5}$, then $(m+n\sqrt{5})(m-n\sqrt{5}) = m^2 - 5n^2 = N(x)$. Thus $x^{-1} = \pm(m-n\sqrt{5})$ if $N(x) = \pm 1$. If $N(x) = \pm 2$ then $m^2 - 5n^2 = \pm 2$. Hence m and n are both even or both odd. If $m = 2k$ and $n = 2l$ then $4n^2 - 20l^2 = \pm 2$, whence $2(k^2 - 5l^2) = \pm 1$, a contradiction. If $m = 2k+1$ and $n = 2l+1$, then $(4k^2+4k+1) - 5(4l^2+4l+1) = \pm 2$, so $2(k^2+k-5l^2-5l-1) = \pm 1$,again a contradiction. So $N(x) = \pm 1$ or $N(y) = \pm 1$; that is x or y is a unit. Thus p is irreducible. To see that p is not prime, note that

   $p(1-\sqrt{5}) = -4 = 2(-2)$. So if p is prime, $p \mid \pm 2$, say $\pm 2 = (1+\sqrt{5})(a+b\sqrt{5})$. Hence $a+5b = \pm 2$ and $a+b = 0$. This gives $-4a = \pm 2$, $2a = \pm 1$, a contradiction. So $p = 1+\sqrt{5}$ is not a prime.

2. §5.1, # 37: Show that an integral domain R is a UFD if and only if it satisfies the ACCP and $\text{lcm}(a,b)$ exists for all $a \neq 0$ and $b \neq 0$ in R. [*Hint*: If $p \mid ab$, p irreducible, consider $m = \text{lcm}(a,b)$. Use the fact that $m \mid ap$ and $m \mid ab$.]

   Solution: If R has the ACCP, we show each irreducible $p \in R$ is prime and use Theorem 7. If $p|ab$, write $m \sim \text{lcm}(a,p)$. Then $m|ap$ (because ap is a common multiple) say $ap = dm$, $d \in R$. If $m = fa$ then $dfa = ap$ so $p = fd$. Since p is irreducible either $f \sim 1$ or $d \sim 1$. If $f \sim 1$ then $a \sim m$ so $p|a$ (because $p|m$). If $d \sim 1$ then $ap \sim m$. Now ab is a common multiple of a and (by hypothesis) p, so $m|ab$. Thus $ap|ab$, whence $p|b$.

3. §5.2, # 28: An ideal A of a commutative ring R is called **finitely generated** if $A = \{r_1a_1 + r_2a_2 + \cdots + r_na_n \mid r_i \in R\}$ for some $a_1, a_2, \ldots, a_n$ A. We write $A = \langle a_1, \ldots, a_n \rangle$ in this case, and say that $a_1, a_2, \ldots, a_n$ **generate** A.

   (a) Show that the following conditions are equivalent for an integral domain R (then called a **Bézout** domain):

   (1) Every 2-generated ideal $A = \langle a, b \rangle$ is principal.

   (2) If $a \neq 0$ and $b \neq 0$, then $d = \gcd(a,b)$ exists and $d = ra + sb$ for some $r, s \in R$.

   (b) If R is a Bézout domain, show that every finitely generated ideal is principal; in fact, for all $a_1, \ldots, a_n$ in R show that $d \sim \gcd(a_1, \ldots, a_n)$ exists and that $\langle a_1, \ldots, a_n \rangle = \langle d \rangle$.

   Solution: (a). (1) $\Rightarrow$ (2). Given $a \neq 0$, $b \neq 0$, let $\langle a, b \rangle = \langle d \rangle$. Then $d = ra + sb$ for some r, $s \in R$, so if $k|a$ and $k|b$ in R then $k|d$. But $d|a$ and $d|b$ because $a, b \in \langle d \rangle$.

   (2) $\Rightarrow$ (1). Given $A = \langle a, b \rangle$, clearly A is principal if $a = 0$ or $b = 0$. Otherwise let $\gcd(a,b) \sim d$ where $d = ra + sb$ for r, $s \in R$. Then $d \in A$ so $\langle d \rangle \subseteq A$. On the other hand, $d|a$ and $d|b$ so $a \in \langle d \rangle$ and $b \in \langle d \rangle$. Hence $\langle a, b \rangle \subseteq \langle d \rangle$.

   (b). Given $a_1, \ldots, a_n$ in R, we show $\langle a_1, \ldots, a_n \rangle$ is principal by induction on n. If $n = 1$, it is clear. If $n > 1$ let $\langle a_1, \ldots, a_{n-1} \rangle = \langle b \rangle$ by induction. Then $\langle a_1, \ldots, a_n \rangle = \langle b, a_n \rangle$ and this is principal because R is a Bézout domain. Now let $\langle a_1, \ldots, a_n \rangle = \langle d \rangle$. Then $d|a_i$ for all i because $a_i \in \langle d \rangle$; and if $k|a_i$ for all i. Then $k|d$ because $d = r_1a_1 + \cdots + r_na_n$ for $r_i \in R$. So $d = \gcd(a_1, \ldots, a_n)$.

4. §5.2, # 31: Let $a = bc$ in a PID R where $gcd(b,c) \sim 1$. Show that $\frac{R}{\langle a \rangle} \cong \frac{R}{\langle b \rangle} \times \frac{R}{\langle c \rangle}$. [*Hint*: Chinese remainder theorem and Theorem 8 §3.4.]

   Solution: Write $B = \langle b \rangle$ and $C = \langle c \rangle$. By Theorem 8 §3.4, it suffices to show that $B \cap C = \langle a \rangle$ and $B + C = R$. Now $\gcd(b,c) = 1$ means that $1 = rb + sc$ for some r, $s = R$. Thus $1 \in B + C$, so $B + C = R$. It is clear that $\langle a \rangle = \langle bc \rangle \subseteq B \cap C$. If $x \in B \cap C$ then $b|x$ and $c|x$, say $x = b'b = c'c$. Then $1 = rb + sc$ gives $x = rbx + scx = rb(c'c) + scb'b = (rc' + sb')bc = (rc' + sb')a \in \langle a \rangle$.

5. §7.1, # 10 If $e \in R$ satisfies $e^2 = e$, show that $R = Re \oplus R(1-e)$.

   # 11: If $R = A \oplus B$ where A and B are left ideals, show that there exists $e^2 = e \in R$ such that $A = Re$ and $B = R(1-e)$. [*Hint*: Let $1 = e + f$, $e \in A$, $f \in B$. If $a \in A$ show that $a - ae = af \in A \cap B = 0$, and conclude that $e^2 = e$.]

   Solution: 10. We have $R = Re + R(1-e)$ because $r = re + r(1-e)$ for all $r \in R$. If $r \in Re \cap R(1-e)$, then $r = se$ and $r = t(1-e)$ with $s, t \in R$. Hence $re = se^2 = se = r$, so $r = re = t(1-e)e = t(e - e^2) = 0$. Hence $Re \cap R(1-e) = 0$.

   11. As in the Hint, let $1 = e + f$ where $e \in A$ and $f \in B$. If $a \in A$ then $a - ae = af \in A \cap B = 0$ because $a - ae \in A$ and $af \in B$ (using the fact that A and B are left ideals). Hence $a = ae$ for all $a \in A$ so, since $e \in A$, we obtain $e^2 = e$ and $A \subseteq Re$. But $Re \subseteq A$ because A is a left ideal and $e \in A$, so $A = Re$. Now observe that $f = 1 - e$ satisfies $f^2 = f$, so $B = Rf = R(1-e)$ follows in the same way.