PMAT 315
SOLUTIONS TO ASSIGNMENT 4
WINTER 2005

1. Page 238, #35. *Prove the second isomorphism theorem: If A is an ideal of R and S is a subring of R, then $S+A$ is a subring, A and $S\cap A$ are ideals of $S+A$ and S respectively, and $(S+A)/A \cong A/(S\cap A)$.*

   Solution. It is routine to verify that $S+A$ is a subring of R, and A is an ideal of $S+A$ because it is an ideal or R. Define $\theta : S \to \frac{S+A}{A}$ by $\theta(s) = s+A$. This is an onto ring homomorphism and $\ker\theta = \{s \mid s+A = A\} = S\cap A$.

2. Page 258, #39. *Let R be a commutative ring and consider $f(x) = a_0 + a_1x + \cdots + a_nx^n$ in $R[x]$.*

   (a) *If a_0 is a unit in R and a_i is nilpotent for all $i > 1$, show that $f(x)$ is a unit in $R[x]$.*

   (b) *If $f(x)$ is a unit in $R[x]$, show that a_0 is a unit in R and that a_i is in each prime ideal of R.* [Hint: *See Exercise 37.*]

   Remark: *The intersection of all prime ideals in a commutative ring equals the set of all nilpotents, so each a_i is actually nilpotent.*

   Solution. (a). If $f(x)g(x) = 1$ then $a_0b_0 = 1$ where b_0 is the constant coefficient of $g(x)$. In a commutative ring, if u is a unit and a is a nilpotent then $u^{-1}a$ is also nilpotent so $u + a = u(1 + u^{-1}a)$ is a unit (because $1 + u^{-1}a$ is a unit). If a_0 is a unit and a_i is nilpotent for $i \geq 1$, then a_ix^i is nilpotent for each i, so $a_0 + a_1x$ is a unit; then $(a_0 + a_1x) + a_2x^2$ is a unit; etc.

   (b). Let $f(x)g(x) = 1$ in $R[x]$. If P is a prime ideal of R let $\theta : R \to R/P$ be the coset ring homomorphism. Use the notation of Exercise 37. Then $\overline{f(x)g(x)} = \bar{1}$ in $(R/P)[x]$. But (R/P) is an integral domain (P is prime) so this asserts that $\overline{f(x)}$ is constant in $(R/A)[x]$. If $f(x) = \sum_{i=0}^{n} r_ix^i$, then $\bar{f}[x] = \sum_{i=0}^{n} \bar{r}_ix^i$ being constant means $\overline{a_i} = \bar{0}$ for all $i \geq 1$; that is $a_i \in P$ for all $i \geq 1$. It follows that a_0 is a unit by comparing constant coefficients in $f(x)g(x) = 1$.

3. Page 274, #18b. *If $f(x) = 3x^4 + 2$ in $\mathbb{Z}_{11}[x]$, factor $f(x)$ as a product of irriducible polynomials in $\mathbb{Z}_{11}[x]$.*

   Solution. Since $3^{-1} = 4$ in Z_{11}, write $f(x) = 3(x^4 + 8)$. Hence we factor $x^4 + 8 = x^4 - 3$. One verifies that $x^4 \neq 3$ if $x = 0, 1, 2, 3$, but $4^4 = 16^2 = 5^2 = 3$. Hence $x - 4$ is a factor of $x^4 = 8$, and long division gives $x^4 + 8 = (x - 4)(x^3 + 4x^2 + 5x + 9)$. Now note $7 = -4$ is a root of $x^3 + 4x^2 + 5x + 9$, and long division gives $x^3 + 4x^2 + 5x + 9 = (x + 4)(x^2 + 5)$. Since $x^2 + 5$ has no root in Z_{11}, it is irreducible, and so $3x^4 + 2 = 3(x - 4)(x + 4)(x^2 + 5)$ in $\mathbb{Z}_{11}[x]$ is the desired factorization.

4. Page 285, #10a. *If F is a field, show that* $\dfrac{F[x]}{\langle x^2\rangle} \cong \left\{ \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \mid a, b \in F \right\}$, *a subring of $M_2(F)$.*

   Solution. As in Theorem 2 write $R = F[x]/\langle x^2\rangle = \{a + bt \mid a, b \in F;\ t^2 = 0\}$. Define $\theta : R \to M_2[F]$ by $(a + bt)\theta = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$. This is well defined by Lemma 3 and is clearly a one-to-one homomorphism of additive groups carrying 1 to 1. Finally

   $$[(a + bt)(c + dt)]\theta = \theta[ac + (ad + bc)t] = \begin{bmatrix} ac & ad + bc \\ 0 & ac \end{bmatrix} = \begin{bmatrix} a & b \\ 0 & a \end{bmatrix}\begin{bmatrix} c & d \\ 0 & c \end{bmatrix} = \theta(a + bt) \cdot \theta(c + dt)$$

   so θ is a one-to-one ring homomorphism. Thus $R \cong \theta(R) = \left\{ \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \middle| a, b \in F \right\}$.

5. Page 285, #12. *Let $R = F[x]/\left\langle x^2 - 1\right\rangle = \{a + bt \mid a, b \in F; t^2 = 1\}$. Show that $a + bt$ is a unit in R if and only if $a^2 \neq b^2$.* [Hint: *If $r = a + bt$ let $r^* = a - bt$, and $N(r) = rr^*$. Show that $(rs)^* = r^*s^*$, and hence that $N(rs) = N(r)\,N(s)$ for all $r, s \in R$.*]

   Solution. If $r = a + bt$ let $r^* = a - bt$. Then $(rs)^* = r^*s^*$ is a routine verification, so $N(rs) = (rs)(rs)^* = rsr^*s^* = (rr^*)(ss^*) = N(r)N(s)$. Now $N(r) = rr^* = a^2 - b^2$. So, if $a^2 \neq b^2$, we have $1 = r[\frac{1}{N(r)}r^*]$, so $r^{-1} = \frac{1}{N(r)}r^*$. On the other hand, if r is a unit, say $rs = 1$ for $s \in R$, then $N(r)N(s) = N(rs) = 1$ so $a^2 - b^2 = N(r) \neq 0$.