MATH 251: ABSTRACT ALGEBRA I
EXAM #3

Problem 1. Let F be a field. For a polynomial $f(x) = \sum_{i=0}^{n} a_i x^i \in F[x]$, we denote by

$$f'(x) = \sum_{i=1}^{n} i a_i x^{i-1} = a_1 + 2a_2 x + \cdots + n a_n x^{n-1}$$

the formal derivative of f.

(a) Let

$$I = \{f(x) \in F[x] : f(1) = f'(1) = 0\}.$$

Show that I is an ideal of $F[x]$.

(b) Let

$$J = \{f(x) \in F[x] : f(1) = f'(0) = 0\}.$$

Is J an ideal of $F[x]$? Prove or disprove.

Solution. A subset $I \subset R = F[x]$ is an ideal if I is a subgroup under $+$ and is closed under multiplication by R.

For (a), we clearly have $0 \in I$ so that $I \neq \emptyset$; if $f, g \in I$ then $(f+g)(1) = f(1) + g(1) = 0$ and $(f+g)'(1) = f'(1) + g'(1) = 0$ so $f+g \in I$, and if $f \in I$ then $(-f)(1) = -f(1) = 0$ and $(-f)'(1) = -f'(1) = 0$ so $-f \in I$, hence I is a subgroup under $+$. Next, if $f \in I$ and $p \in R$, then $(pf)(1) = p(1)f(1) = 0$ and

$$(pf)'(1) = (p'f + pf')(1) = p'(1)f(1) + p(1)f'(1) = 0 + 0 = 0.$$

Thus I is an ideal. Indeed, I is the principal ideal generated by $(x-1)^2$.

For (b), we note that J is not an ideal: we have $x^2 - 1 \in J$ but $x^3 - x = x(x^2-1) \notin J$.

Problem 2. Determine explicitly if the matrix

$$A = \begin{pmatrix} 1 & 5 \\ 3 & 2 \end{pmatrix} \in M_2(\mathbb{Z}/26\mathbb{Z})$$

is a zerodivisor.

Solution. The matrix A is a zerodivisor. One can do this by solving linear equations over $\mathbb{Z}/26\mathbb{Z}$ directly, but here is another approach. We note that for $a, b, c, d \in R$ for any ring R, we have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} D & 0 \\ 0 & D \end{pmatrix}$$

where $D = \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$. We compute that $\det(A) = 2 - 15 = -13 \equiv 13 \pmod{26}$, when

$$A \begin{pmatrix} 4 & -10 \\ -6 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

From this argument, it is easy to see that $A \in M_2(R)^\times$ if and only if $\det(A) \in R^\times$, and otherwise $A \in M_2(R)$ is a zerodivisor if and only if $\det(A)$ is a zerodivisor.

Problem 3. Let R be a ring.

(a) Let $a \in R$ and suppose that $a^n \in R^\times$ for some $n \in \mathbb{Z}_{>0}$. Show that $a \in R^\times$.

(b) Suppose that $a^2 = 1$ for all $a \in R$ with $a \neq 0$. Show that R is a field.

Date: 14 December 2007.

Solution. Part (a) is easy: if $a^n u = ua^n = 1$, then $a(a^{n-1}u) = (ua^{n-1})a = 1$; by the uniqueness of left and right inverse, we have $a \in R^\times$. (You may assume this, but for completeness: If $ab = ca = 1$ in a ring R, then $b = c$. Indeed, since $ab = 1$, we have $b = cab = c$.)

For part (b), we note that by part (a) every $a \in R \setminus \{0\}$ is a unit, so we need only show that R is commutative. Let $a, b \in R$, then by hypothesis $(ab)^2 = abab = 1$; then multiplying by a, b on the left and right, respectively, we have $a^2bab^2 = ba = ab$, so R is a field. Such fields exist, e.g. $R = \mathbb{Z}/2\mathbb{Z}$ and $R = \mathbb{Z}/3\mathbb{Z}$.

Problem 4. Let R be an integral domain, and let $a, b \in R$. Prove that $(a) = (b)$ if and only if $a = ub$ for some $u \in R^\times$.

Solution. We recall that $(a) \subset (b)$ if and only if $b \in (a)$ if and only if $b = ra$ for some $r \in R$. Thus $(a) = (b)$ if and only if $b = ra$ and $a = sb$ for some $r, s \in R$. Putting these equations together, we obtain $b = (rs)b$, or $b(1 - rs) = 0$. But since R is an integral domain, this implies that either $b = 0$ or $rs = 1$; in the former case, we then have $(b) = (0) = (a)$ so $a = 1b = 0$ in which case the result is trivially true, and in the latter case we have $a = sb$ where now $s \in R^\times$ as claimed.

Problem 5. Show that the ideal of $\mathbb{Z}[i]$ generated by $2 + i$ is maximal.

Solution. An ideal I of a commutative ring R is maximal if and only if R/I is a field. We prove that in fact $\mathbb{Z}[i]/(2 + i) \cong \mathbb{Z}/5\mathbb{Z}$, which is a field since 5 is prime. We examine the set of cosets $S = \mathbb{Z}[i]/(2 + i)$ and ask ourselves: what are the possible remainders? What does it mean to consider elements of $\mathbb{Z}[i]$ "modulo the ideal $(2 + i)$"? Note that if $a + bi + (2 + i) \in S$, then $a + bi = a + bi - b(2 + i) = a - 2b$ so $a + bi + (2 + i) = a - 2b + (2 + i)$; but also, $(2 + i)(2 - i) = N(2 + i) = 5$, so we may reduce $a - 2b$ modulo 5 as well. Therefore we define a map

$$\mathbb{Z}[i] \to \mathbb{Z}/5\mathbb{Z}$$
$$a + bi \mapsto (a - 2b) \bmod 5.$$

Check that this map is a ring homomorphism. It is obviously surjective, and its kernel by the above is the ideal $(2 + i)$. The result then follows.

Alternatively, one can "divide" an element $a + bi$ by $2 + i$, i.e. solve the equation $(x + yi)(2 + i) = a + bi$; one obtains

$$x = \frac{2a + b}{5}, \quad y = \frac{-a + 2b}{5},$$

and so $x, y \in \mathbb{Z}$ if and only if $a \equiv 2b \pmod 5$ (equivalently, $2a \equiv -b \pmod 5$). (This also reproves that the kernel of the above map is the ideal $2 + i$.) Now consider an ideal $I \subsetneq J \subsetneq \mathbb{Z}[i]$ and $a + bi \in J$, then $N(a + bi) = c \in J$. If $\gcd(c, 5) = 1$, then $1 \in J$ so $J = \mathbb{Z}[i]$, a contradiction. Therefore $c = a^2 + b^2$ must be a multiple of 5, which can happen if and only if $a \equiv 2b \pmod 5$ by a direct calculation, which is again a contradiction.