MODERN ALGEBRA II SPRING 2012: FIRST PROBLEM SET

1. (i) Let $R = \mathbb{Z}[\frac{1}{2}]$ be the set of all rational numbers of the form $a/2^n$, where $a \in \mathbb{Z}$ and $n \in \mathbb{Z}$, $n \geq 0$. Show that R is a subring of $\mathbb{Q}$ containing $\mathbb{Z}$ and $\frac{1}{2}$. (Note: In fact, R is the smallest subring of $\mathbb{Q}$ with this property. Also, in the statement and proof, you can replace 2 with any positive integer d.)

   (ii) Let $S = \mathbb{Z}_{(2)}$ be the set of all rational numbers of the form a/b, where $a, b \in \mathbb{Z}$ and 2 does not divide b. Show that S is a subring of $\mathbb{Q}$ containing $\mathbb{Z}$ which does not contain $\frac{1}{2}$. (Note: In fact, S is the largest subring of $\mathbb{Q}$ with this property. Also, in the statement and proof, you can replace 2 with any prime number p.)

2. Let R be a ring and let $r \in R$. Given $n \in \mathbb{N}$, define $r^n = \underbrace{r \cdot \cdots \cdot r}_{n \text{ times}}$. By convention, if R has unity 1, set $r^0 = 1$. (However, the expression r^n, for $n < 0$, can only be defined in r is a unit.) Show (informally) that $r^n \cdot r^m = r^{n+m}$ and that $(r^n)^m = r^{nm}$.

3. (i) Let R be a ring. Given $n \in \mathbb{Z}$ and $r \in R$, then, as is the usual notation for abelian groups, $n \cdot r$ is the element $\underbrace{r + \cdots + r}_{n \text{ times}}$, if $n > 0$. Similarly for $n < 0$, $n = -m$, $n \cdot r = m \cdot (-r)$, and for $n = 0$, $0 \cdot r = 0$ in the usual way. Show that, for all $n \in \mathbb{Z}$ and $r, s \in R$, $(n \cdot r)s = r(n \cdot s) = n \cdot (rs)$ and that, for all $n, m \in \mathbb{Z}$, $n \cdot (m \cdot r) = (nm) \cdot r$. (For the first property, just check it for $n > 0$ by induction on n. You don't need to check the second property; it is one of the "laws of exponents" for an abelian group and doesn't have anything to do with R being a ring.)

   (ii) Let R be a ring with unity and define $f \colon \mathbb{Z} \to R$ by $f(n) = n \cdot 1$. Show that f is a (ring) homomorphism, that it is the unique homomorphism from $\mathbb{Z}$ to R (with our conventions on homomorphisms from a ring with unity to another ring with unity) and that its image is the cyclic subgroup generated by 1.

4. Let R be a commutative ring. Show:

   (a) For all $r, s \in R$, $(r + s)(r - s) = r^2 - s^2$. Is this statement true if R is not commutative?

(b) For all $r, s \in R$, $(r+s)^2 = r^2 + 2 \cdot rs + s^2$. How should the statement read if R is not commutative?

(c) Generalizing (b), argue (informally if need be) that, for all $r, s \in R$ and $n \in \mathbb{N}$, $(r+s)^n = \displaystyle\sum_{i=0}^{n} \binom{n}{i} \cdot r^i s^{n-i}$.

5. Let $\mathbb{H}$ denote the quaternions: $\mathbb{H} = \mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}k$. Recall that $i^2 = j^2 = k^2 = -1$ and $ij = k = -ji$, $jk = i = -kj$, $ki = j = -ik$.

   (a) Given $\alpha = x_0 + x_1 i + x_2 j + x_3 k \in \mathbb{H}$, define the *conjugate* $\bar{\alpha}$ via:

   $$\bar{\alpha} = x_0 - x_1 i - x_2 j - x_3 k.$$

   With some care due to the fact that multiplication of quaternions is not commutative, show that

   $$\alpha \cdot \bar{\alpha} = x_0^2 + x_1^2 + x_2^2 + x_3^2 = |\alpha|^2,$$

   and conclude that, if $\alpha \neq 0$, then $\bar{\alpha}/|\alpha|^2$ is a multiplicative inverse for α.

   (b) Let $\alpha = x_1 i + x_2 j + x_3 k \in \mathbb{H}$. Compute α^2. Conclude that there are an infinite number of $\alpha \in \mathbb{H}$ such that $\alpha^2 = -1$.

6. Let R be a ring, not necessarily commutative or with unity. Define the *center* $Z(R)$ to be the set

   $$\{r \in R : rs = sr \text{ for all } s \in R.\}$$

   Show that $Z(R)$ is a subring of R. Show that, if R has a unity 1, then $1 \in Z(R)$. Show that the center $Z(\mathbb{H})$ of the quaternions is just $\mathbb{R} \subseteq \mathbb{H}$.

   (Note: using some linear algebra, it is possible to show that the center of $M_n(\mathbb{R})$ is the subring $\{t\,\mathrm{Id} : t \in \mathbb{R}\}$ of all scalar multiples of the identity matrix; this subring is isomorphic to $\mathbb{R}$.)