MODERN ALGEBRA II SPRING 2013: SECOND PROBLEM SET

1. (i) Show that $(\mathbb{Z}[i])^*$, the multiplicative group of units in $\mathbb{Z}[i]$, is equal to $\{\pm 1, \pm i\}$. In particular, every element in the (finite) group $(\mathbb{Z}[i])^*$ has order at most 4.

   (ii) In the ring $\mathbb{Z}[\sqrt{2}]$, show that $1+\sqrt{2}$ is a unit by explicitly finding an inverse for $1+\sqrt{2}$ in $\mathbb{Z}[\sqrt{2}]$. However, by viewing $1+\sqrt{2}$ as a real number, show that no positive power of $1+\sqrt{2}$ is equal to 1 and hence that $(\mathbb{Z}[\sqrt{2}])^*$ contains an element of infinite order.

2. Let p be a prime number.

   (a) If k is an integer with $1 \leq k \leq p-1$, show that p divides the binomial coefficient $\binom{p}{k}$.

   (b) Let R be a ring of characteristic p (recall that this means that $p \cdot r = 0$ for all $r \in R$. Show that, for all $r, s \in R$, $(r+s)^p = r^p + s^p$. (Use the binomial theorem from the last problem set.)

   (c) If R is a ring of characteristic p, show that the function $F\colon R \to R$ defined by $F(r) = r^p$ is a homomorphism (the *Frobenius homomorphism*). If R is an integral domain, show that F is injective.

   (d) Let $R = \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$. Show that $F\colon \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ is the identity. (Note: you will need to use a standard number theory fact which we proved last semester.)

   (e) Let $R = (\mathbb{Z}/p\mathbb{Z})[x] = \mathbb{F}_p[x]$. Show that $F\colon R \to R$ is injective but not surjective and describe the image of F.

   The Frobenius homomorphism is very important in the study of finite fields, and it will reappear later.

3. Recall that an element r of a ring R is *nilpotent* if there exists a positive integer N such that $r^N = 0$. (The possibility that $r = 0$, i.e. that $N = 1$, is allowed.)

   (a) Show that, if r is nilpotent and $s \in R$, then sr is nilpotent.

   (b) Show that, if $r, s \in R$ and r and s are both nilpotent, then $r+s$ is also nilpotent (i.e. the sum of two nilpotent elements is again nilpotent. (The binomial theorem again.) (Note: this does not necessarily hold in a non-commutative ring, for example, in $\mathbb{M}_2(\mathbb{R})$ both $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ are nilpotent, but their sum is invertible.)

(c) Show that, if r is nilpotent, then $1+r$ is a unit. (Hint: geometric series.) More generally, if u is a unit in R and r is nilpotent, then $u+r$ is a unit.

(d) If r is a nilpotent element of R, then the polynomial $1+rx$ is a unit in $R[x]$. Hence, if R is not an integral domain, then it is possible for $(R[x])^*$ to be larger than R^*.

4. Let n be a positive integer. What are all of the (nonzero) divisors of zero in $\mathbb{Z}/n\mathbb{Z}$? What are all of the nilpotent elements in $\mathbb{Z}/n\mathbb{Z}$ (i.e. those elements $a \in \mathbb{Z}/n\mathbb{Z}$ such that $a^N = 0$ for some $N > 0$)?

5. Let $\mathbb{Q}(i) = \{a+bi : a, b \in \mathbb{Q}\}$ be the subring of $\mathbb{C}$ given by the image of $\mathrm{ev}_i \colon \mathbb{Q}[x] \to \mathbb{C}$. Show that $\mathbb{Q}(i)$ is a field, not just an integral domain, by showing that, if a, b are not both 0, then $a+bi$ has a multiplicative inverse. (This is the usual trick of "rationalizing the denominator" of $1/(a+bi)$.) Similarly, show that the subring $\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} : a, b \in \mathbb{Q}\}$ of $\mathbb{R}$ is a field.

6. Let $a, b, c \in \mathbb{Q}$, not all zero. We would like to show that $\mathbb{Q}(\sqrt[3]{2})$ is a field by rationalizing the denominator in an expression of the form $\dfrac{1}{a+b\sqrt[3]{2}+c(\sqrt[3]{2})^2}$. Show that this can be done by multiplying by

$$1 = \frac{(a^2-2bc)+(-ab+2c^2)\sqrt[3]{2}+(b^2-ac)(\sqrt[3]{2})^2}{(a^2-2bc)+(-ab+2c^2)\sqrt[3]{2}+(b^2-ac)(\sqrt[3]{2})^2},$$

by checking that

$$(a+b\sqrt[3]{2}+c(\sqrt[3]{2})^2)((a^2-2bc)+(-ab+2c^2)\sqrt[3]{2}+(b^2-ac)(\sqrt[3]{2})^2))$$

is in fact a rational number, in fact it is $a^3+2b^3+4c^3-6abc$, which is nonzero if not all of a, b, c are zero (you do **not** need to prove that this expression is nonzero). How could you hope to guess such a formula? We will see a few different ways to find this formula over the course of the semester.