Homework #12 (week of 11/08–11/12)

Due Friday, 11/12/04 in class

Let $G$ be a group and $a, b \in G$. Recall that the powers $a^n$ are defined by

$$a^n = \begin{cases} 
  e & : n = 0; \\
  a^{n-1}a & : n > 0; \\
  (a^{-1})^{-n} & : n < 0.
\end{cases}$$

Recall that the exponent laws $a^{m+n} = a^m a^n$, $(a^m)^n = a^{mn}$ for all $m, n \in \mathbb{Z}$. If $a$ and $b$ commute, that is $ab = ba$, then $(ab)^m = a^m b^m$ for all $m \in \mathbb{Z}$ as well.

Let $R$ be a ring and $a, b \in R$. Then $R$ is a group under addition. Recall that the additive analog $n \cdot a$ of powers is defined by

$$n \cdot a = \begin{cases} 
  0 & : n = 0; \\
  (n - 1) \cdot a + a & : n > 0; \\
  (-n) \cdot (-a) & : n < 0.
\end{cases}$$

The additive versions of the exponent laws above are $(m + n) \cdot a = m \cdot a + n \cdot a$, $mn \cdot a = m \cdot (n \cdot a)$, and $m \cdot (a + b) = m \cdot a + m \cdot b$, for all $m, n \in \mathbb{Z}$. The latter holds since addition in $R$ is commutative.

Suppose further that $R$ has a unity 1. We define powers for non-negative integers as above by

$$a^n = \begin{cases} 
  1 & : n = 0; \\
  a^{(n-1)}a & : n > 0.
\end{cases}$$

Unless $a$ has a multiplicative inverse negative powers of $a$ are not defined. The exponent laws $a^{m+n} = a^m a^n$ and $(a^m)^n = a^{mn}$ hold for all $m, n \geq 0$. If $ab = ba$ then $(ab)^m = a^m b^m$ for all $m \geq 0$ holds as well.

There is a formula which relates the operation $n \cdot a$ with multiplication in $R$, namely

$$n \cdot (ab) = (n \cdot a)b = a(n \cdot b)$$

for all $n \in \mathbb{Z}$.

You may use all of the preceding formulas without proof in the exercises below.
1. Let $R$ be a finite ring with unity $1$.

   a) Let $a \in R$ be not zero. Show that there is a non-zero $b \in R$ such that $ab = 0 = ba$ or $ab = 1 = ba$. [Hint: Consider the list $1 = a^0, a = a^1, a^2, a^3, \ldots$. Since $R$ is finite $a^\ell = a^m$ for some $0 \leq \ell < m$.]

   Let $R = \mathbb{Z}_{12}$.

   b) For all non-zero $a \in \mathbb{Z}_{12}$ find a non-zero $b \in \mathbb{Z}_{12}$ such that $ab = 0 = ba$ or $ab = 1 = ba$ and indicate which is the case.

   c) Let $R^\times$ be the (abelian) group of units of $R$ under multiplication. Write down a Cayley Table for $R^\times$.

   d) Find positive integers $1 < n_1, \ldots, n_r$ such that $R^\times \cong \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_r}$, and $n_1|n_2, \ldots, n_{r-1}|n_r$.

2. Let $d$ be a positive rational number and $\sqrt{d}$ be its positive real square root. Show that

   $$\mathbb{Q}[\sqrt{d}] = \{r + s\sqrt{d} | r, s \in \mathbb{Q}\}$$

   is a subfield of $\mathbb{R}$. [Hint: Consider two cases: $\sqrt{d}$ rational and $\sqrt{d}$ not rational.]

3. Let $R = \mathbb{Z}_6$. Find a polynomial of the form $X^2 + cX$, where $c \in \mathbb{Z}_6$, which has more than two roots in $\mathbb{Z}_6$.

4. Let $R$ be a commutative ring with unity and suppose that every polynomial of the form $f(X) = a_0 + a_1X + \cdots + a_nX^n \in R[X]$, where $a_n \neq 0$, has at most $n$ roots in $R$. Show that $R$ must be an integral domain. [Hint: See the preceding problem.]

5. Let $R$ be a ring and $a, b \in R$ commute (that is $ab = ba$). Show that

   $$(a + b)^n = \sum_{\ell=0}^{n} \binom{n}{\ell} a^{n-\ell} b^\ell$$
holds for all $n \geq 1$. [Hint: Look up a proof of the Binomial Theorem for numbers $a$ and $b$. You may use the generalized distributive laws

$$a(b_1 + \cdots + b_r) = ab_1 + \cdots + ab_r \quad \text{and} \quad (a_1 + \cdots + a_r)b = a_1 b + \cdots + a_r b$$

for all $a, b_1, \ldots, b_r, b, a_1, \ldots, a_r \in R$ which follow by induction from the distributive laws. ]