Math 151

Fall 2008

Test 3 - Solutions

1. Consider the group $\mathbb{Z}_6 \times \mathbb{Z}_8$ and its subgroup $< (2,4) >$. Find the order of each of the following:

   (a) the group $\mathbb{Z}_6 \times \mathbb{Z}_8$,
   $|\mathbb{Z}_6 \times \mathbb{Z}_8| = |\mathbb{Z}_6| \cdot |\mathbb{Z}_8| = 6 \cdot 8 = 48.$

   (b) the subgroup $< (2,4) >$,
   $< (2,4) >= \{(0,0),(2,4),(4,0),(0,4),(2,0),(4,4),$ *so* $| < (2,4) > | = 6.$

   (c) the factor group $(\mathbb{Z}_6 \times \mathbb{Z}_8)/ < (2,4) >$.
   $|(\mathbb{Z}_6 \times \mathbb{Z}_8)/ < (2,4) > | = \frac{|\mathbb{Z}_6 \times \mathbb{Z}_8|}{|<(2,4)>|} = \frac{48}{6} = 8.$

2. Find the greatest common divisor of $x^4 + x^3 + 2x^2 + x + 1$ and $x^3 + 2$ over $\mathbb{Z}_3$.
   $x^4 + x^3 + 2x^2 + x + 1 = (x^3 + 2)(x + 1) + (2x^2 + 2x + 2),$
   $x^3 + 2 = (2x^2 + 2x + 2)(2x + 1),$
   so the greatest common divisor is the monic polynomial that is a multiple of $2x^2 + 2x + 2,$ *i.e.* $x^2 + x + 1.$

3. Let $f(x) = x^2 + 100x + n$.

   (a) Give an example of an integer n such that $f(x)$ is reducible over $\mathbb{Q}$. (Show that $f(x)$ is reducible for this value of n.)
   If $n = 0$, *then* $f(x) = x^2 + 100x = x(x + 100)$ *is reducible.*

   (b) Give an example of an integer n such that $f(x)$ is irreducible over $\mathbb{Q}$. (Prove that $f(x)$ is irreducible for this value of n.)
   If $n = 2$, *then* $f(x) = x^2 + 100x + 2$ *is irreducible by Eisenstein's irreducibility criterion (with* $p = 2$*).*

4. Recall that $\mathbb{R}$ is a group (under addition), a ring, and a field. Consider the subset $\mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\}$ of $\mathbb{R}$.

   (a) Is $\mathbb{Z}[\sqrt{5}]$ a subgroup of $\mathbb{R}$? Explain why or why not.
   Yes. It is closed under addition since $(a+b\sqrt{5})+(c+d\sqrt{5}) = (a+c)+(b+d)\sqrt{5}.$ *It contains* $0 = 0+0\sqrt{5}$, *and it is closed under the additive inverses since for any* $a + b\sqrt{5} \in \mathbb{Z}[\sqrt{5}]$, *its additive inverse is* $(-a) + (-b)\sqrt{5} \in \mathbb{Z}[\sqrt{5}]$.

   (b) Is $\mathbb{Z}[\sqrt{5}]$ a subring of $\mathbb{R}$? Explain why or why not.
   Yes. In addition to the properties proved in part (a), the set is closed under multiplication since $(a + b\sqrt{5})(c + d\sqrt{5}) = (ac + 5bd) + (ad + bc)\sqrt{5}$, *and contains* $1 = 1 + 0\sqrt{5}$.

   (c) Is $\mathbb{Z}[\sqrt{5}]$ a subfield of $\mathbb{R}$? Explain why or why not.
   No. The set is not closed under multiplicative inverses, e.g. the multiplicative inverse of $0 + 1\sqrt{5} \in \mathbb{Z}[\sqrt{5}]$ *is* $0 + \frac{1}{5}\sqrt{5} \notin \mathbb{Z}[\sqrt{5}]$.

5. Let R and S be rings, and let $\phi : R \to S$ and $\theta : R \to S$ be ring homomorphisms. Show that $\{r \in R \mid \phi(r) = \theta(r)\}$ is a subring of R.
   Let $K = \{r \in R \mid \phi(r) = \theta(r)\}$. First we will show that K is closed under addition and multiplication. For any $a, b \in K$, we have $\phi(a) = \theta(a)$ and $\phi(b) = \theta(b)$. Then $\phi(a+b) = \phi(a)+\phi(b) = \theta(a)+\theta(b) = \theta(a+b)$ and $\phi(ab) = \phi(a)\phi(b) = \theta(a)\theta(b) = \theta(ab)$, so $a + b, ab \in K$. Next, K contains 0 and 1 since $\phi(0) = 0 = \theta(0)$ and $\phi(1) = 1 = \theta(1)$. Finally, K is closed under additive inverses since for any $a \in K$, $\phi(-a) = -\phi(a) = -\theta(a) = \theta(-a)$, so $-a \in K$. Thus K is a subring of R.

Optional Give an example of a non-commutative ring with exactly 10000 elements. (One point will be given for an example of a non-commutative ring of any finite order.)

$Mat_{2\times 2}(\mathbb{Z}_{10})$ is a ring with 10^4 elements. It is non-commutative because e.g.
$\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 0 & 0 \end{bmatrix}$ *and* $\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$.