Midterm Exam #2 - Solutions

1. (a) *(7 points)* True or False? $x^5 + 30x^4 + 60x^2 + 15x + 150$ is irreducible in $\mathbb{Q}[x]$.
   Solution: TRUE - since 3 divides all but the highest coefficient, and 9 doesn't divide the constant term, this is a 3-Eisenstein polynomial, hence irreducible over $\mathbb{Q}$.

   (b) *(7 points)* Write down two rings that have the same cardinality (number of elements) but that are non-isomorphic. Prove they are not isomorphic.
   Solution: Many different solutions! The rings $\mathbb{Z}$ and $\mathbb{Q}$ have the same cardinality, but $\mathbb{Q}$ is a field, and thus certainly not isomorphic to $\mathbb{Z}$ which is not a field. The ring $\mathbb{Z}/n^2\mathbb{Z}$ and the direct product $(\mathbb{Z}/n\mathbb{Z})^2$ have n^2 elements each, but are not even isomorphic as abelian groups, and so they can't be isomorphic as rings. $\mathbb{Z}$ and $2\mathbb{Z}$ have the same cardinality, but $\mathbb{Z}$ has a unity, and $2\mathbb{Z}$ doesn't, so they can't be isomorphic, etc...

   (c) *(7 points)* True or False? There are exactly four groups of order 36.
   Solution: FALSE - By FTFAG, there are exactly 4 *abelian* groups of order 36, namely

$$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \qquad (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/9\mathbb{Z} \qquad \mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/3\mathbb{Z})^2 \quad \text{and} \quad (\mathbb{Z}/2\mathbb{Z})^2 \times (\mathbb{Z}/3\mathbb{Z})^2$$

   But there are some non-abelian groups of order 36 too, for example D_{18}.

   (d) *(7 points)* There is a group G of order $168 = 2^3 \cdot 3 \cdot 7$ with the property that G does not have any non-trivial normal subgroups. (I.e. G is a *simple* group.) What can you say about the number of Sylow-7 subgroups of G?
   Solution: By Sylow's 1st Theorem, there is at least one subgroup of order 7. By Sylow's 3rd Theorem, the number of such subgroups is a divisor of $2^3 \cdot 3$, (i.e. it's 1,2,4,8,3,6,12 or 24), and it's congruent to $1 (\bmod 7)$, (i.e. it's 1,8,15,22,...). Thus it's either 1 or 8. But by Sylow's 2nd (or at least the idea that conjugates of Sylow-p subgroups are again Sylow-p subgroups), and the fact that G is simple, we can't have a unique Sylow-7 subgroup, as it would be normal. So there are 8 Sylow-7 subgroups.

   (e) *(7 points)* Let R be a commutative ring with $1 \in R$. Show that a zero-divisor in R can't have a multiplicative inverse.
   Solution: Suppose $a \in R$ has a multiplicative inverse, x (in particular, $a \neq 0$). And suppose $ab = 0$. Then $b = (xa)b = x(ab) = x0 = 0$. So there is no $b \neq 0$ with $ab = 0$.

2. Let R and S be commutative rings, and let $\phi : R \to S$ be a homomorphism of rings. Let I be an ideal of R.

   (a) *(10 points)* Prove: If ϕ is onto then the image $\phi(I)$ is an ideal in S.
   Solution: A ring homomorphism is a group homomorphism, and an ideal is a subgroup, and the image of a subgroup under a ring homomorphism is a subgroup, so $\phi(I)$ is a subgroup of S. So we only need to show that $\phi(I)$ satisfies 'super-extra closure' under multiplication. Let $y \in \phi(I)$, and let $s \in S$. Then $x = \phi(y)$ for some $x \in I$, and by surjectivity, $s = \phi(r)$ for some $r \in R$. Thus $sy = \phi(r)\phi(x) = \phi(rx)$ by the properties of a ring homomorphism. But I is an ideal and $x \in I$, so $rx \in I$, and therefore $sy \in \phi(I)$. So $\phi(I)$ is super extra-closed under multiplication, and thus an ideal.

   (b) *(10 points)* Give an example to show that the statement in (a) is not true if we omit the assumption that ϕ is onto.
   Solution: Lots of possible examples. Let $\phi : \mathbb{Z} \to \mathbb{Q}$ have $\phi(n) = n$. It's easy to see that NONE of the ideals of $\mathbb{Z}$, except $\{0\}$, get mapped to ideals in $\mathbb{Q}$, since $\mathbb{Q}$ is a field and has no non-trivial ideals. In particular $2\mathbb{Z}$ is an ideal of $\mathbb{Z}$, but $\phi(2\mathbb{Z}) = \{2n \,|\, n \in \mathbb{Z}\} \subset \mathbb{Q}$ is not an ideal of $\mathbb{Q}$, since $2 \in \phi(2\mathbb{Z})$, but $1 = (1/2) \cdot 2 \notin \phi(2\mathbb{Z})$.

3. Let G be a finite group, and let H be a subgroup of G.

   (a) *(5 points)* What is the definition of 'G acts on a set S'?
   Solution: A group action of G on S is a mapping $G \times S \to S$ with the two properties **(1.)** $(e, s) = s$ for all $s \in S$ and **(2.)** $(g_1, (g_2, s)) = (g_1 g_2, s)$ for all $g_1, g_2 \in G$ and $s \in S$.

   (b) *(5 points)* Define 'the normalizer of H in G'.
   Solution: The normalizer of H in G is $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$. It is the largest subgroup of G in which H is normal.

   (c) *(15 points)* Suppose p is the *smallest* prime divisor of $|G|$, and suppose that $|G|/|H| = p$. Prove that H is a normal subgroup of G. [Hint: Let the group H on the set G/H by multiplication, and examine the sizes of the orbits.]
   Solution: Let H act on the set of cosets G/H by multiplication, i.e. $(h, xH) = (hx)H$. Notice that $\text{Orb}(eH) = \{heH \mid h \in H\} = \{eH\}$, so there is at least one single element orbit. The orbits of this action partition the set G/H, which has p elements, so we get

$$p = \sum_{\text{orbits } \mathcal{O}} |\mathcal{O}| \quad = \quad 1 + \sum_{\text{other orbits } \mathcal{O}} |\mathcal{O}|$$

   But we know that for any orbit $|\text{Orb}(xH)| = |H|/|\text{Stab}(xH)|$, so the number of elements of the orbit is a divisor of $|H|$, and thus a divisor of $|G|$. p is the smallest such divisor, other than 1, but the terms in the sum above clearly need to be smaller than p, since they are all positive and sum to p. So all the orbits must have size 1. So for any $x \in G$, we have

$$\{xH\} = \text{Orb}(xH) = \{hxH \mid h \in H\} \quad \text{i.e.} \quad hxH = xH \text{ for all } h \in H$$

   This last condition says $x^{-1}hx \in H$ for all $h \in H$, and since x was arbitrary above, we have shown that $x^{-1}Hx \subset H$ for all $x \in G$, hence $H \lhd G$

4. Let R be a commutative ring with unity. A proper ideal $I \subset R$ is called *prime* if it satisfies the condition: for all $a, b \in R - I$, we have $ab \in R - I$

   (a) *(15 points)* Show that an ideal $I \subset R$ is prime if and only if the quotient ring R/I is an integral domain with unity, $1 \neq 0$.
   Suppose I is prime. Then $1 \notin I$ (otherwise $I = R$ is not proper) and the coset $1 + I$ is the unity in R/I. Let $a + I$ and $b + I$ be non-zero cosets (i.e. not equal to $0 + I$ as cosets). Then $a, b \in R - I$, and so $ab \notin I$, therefore $ab + I \neq 0 + I$. Therefore, there are no non-zero elements in R/I whose product is zero, and so R/I is an integral domain. Now assume R/I is an integral domain with unity. Then $1 + I \neq 0 + I$, so $1 \neq I$ and I is a proper ideal. Furthermore, for any $a, b \in R - I$, $a + I$ and $b + I$ are non-zero in the quotient, so their product is non-zero too, since R/I is an integral domain. So $ab + I \neq 0 + I$ and thus $ab \in R - I$. So $a, b \in R - I$ implies $ab \in R - I$ and therefore I is prime.

   (b) *(5 points)* Show that every maximal ideal of R is a prime ideal of R.
   If I is a maximal ideal, then R/I is a field, which is an integral domain with unity, so I is a prime ideal by (a).