Math 113 Midterm #2 solutions

(1) True or false:

(a) If R is an integral domain with quotient field Q then the quotient field of $R[x]$ is isomorphic to $Q[x]$.

(b) The group $\mathbb{Z}_4 \times \mathbb{Z}_{18}$ is isomorphic to the group $\mathbb{Z}_2 \times \mathbb{Z}_{36}$.

(a) False. $Q[x]$ is not a field because x has no multiplicative inverse. Degree is additive under multiplication of polynomials, so there is no way to multiply the degree 1 polynomial x by another polynomial to get the degree 0 polynomial 1.

(b) True. Since 2 and 9 are relatively prime, $\mathbb{Z}_2 \times \mathbb{Z}_9 \simeq \mathbb{Z}_{18}$. Since 4 and 9 are relatively prime, $\mathbb{Z}_4 \times \mathbb{Z}_9 \simeq \mathbb{Z}_{36}$. Thus both groups are isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9$.

(2) Let G be a group. Consider the "diagonal"

$$H = \{(x,x) \mid x \in G\} \subset G \times G.$$

H is a subgroup of $G \times G$; you don't have to prove this.

(a) Show that H is a normal subgroup of $G \times G$ if and only if G is abelian.

(b) Assuming G is abelian, show that $(G \times G)/H \simeq G$.

(a) If G is abelian, then for $(x,x) \in H$ and $(g_1,g_2) \in G \times G$, we have $(g_1,g_2)(x,x)(g_1,g_2)^{-1} = (g_1 x g_1^{-1}, g_2 x g_2^{-1}) = (x,x) \in H$, so H is normal. Conversely if H is normal, then for any $x,y \in G$ we must have $(x,e)(y,y)(x,e)^{-1} \in H$, which means that $xyx^{-1} = y$, so $xy = yx$, so G is abelian.

(b) Define $\phi : G \times G \to G$ by $\phi(x,y) = xy^{-1}$. Since G is abelian, ϕ is a homomorphism: $\phi((x_1,y_1)(x_2,y_2)) = \phi(x_1x_2, y_1y_2) = x_1x_2y_2^{-1}y_1^{-1} = x_1y_1^{-1}x_2y_2^{-1} = \phi(x_1,y_1)\phi(x_2,y_2)$. Now $\mathrm{Ker}(\phi) = \{(x,y) \mid xy^{-1} = e\} = \{(x,y) \mid x = y\} = H$, and ϕ is surjective since for any $x \in G$ we have $x = \phi(x,e)$. So by the fundamental homomorphism theorem, $(G \times G)/H \simeq G$.

(3a) Find all solutions to the equation $x^2 - 1 = 0$ in $\mathbb{Z}_{35}$.

(3b) Show that if $p > 2$ is prime then either $2^{(p-1)/2} + 1$ or $2^{(p-1)/2} - 1$ is a multiple of p.

(a) We have $x^2 - 1 = (x+1)(x-1)$. This is zero when $x = 1$ or $x = -1$. It is also zero when $x+1$ and $x-1$ are two numbers whose product is a multiple of 35, i.e. when one is a multiple of 5 and the other is a multiple of 7. Listing the multiples of 5 and 7 from 0 to 35, we see that the solutions we get this way are $x = 6$ and $x = -6$.

(b) By Lagrange's theorem, the order of 2 in the group $\mathbb{Z}_p^*$ must divide the order of the group, namely $p-1$, so $2^{p-1} \equiv 1 \mod p$. Thus $2^{(p-1)/2}$ is a solution to the equation $x^2 - 1 = 0$ in $\mathbb{Z}_p$. Since $\mathbb{Z}_p$ is a field this equation only has the two solutions $x = 1$ and $x = -1$. Instead of the last two sentences, one can also observe that p divides the product $2^{p-1} - 1 = (2^{(p-1)/2} + 1)(2^{(p-1)/2} - 1)$, so since p is prime p must divide one of the two factors.

(4a) Find the quotient and the remainder when x^3+8x^2+7x-1 is divided by $4x - 1$ in $\mathbb{Z}_{11}[x]$.

(4b) Prove the "remainder theorem": if F is a field, $p \in F[x]$, and $\alpha \in F$, then $p(\alpha)$ is the remainder when p is divided by $x - \alpha$. (Here $p(\alpha)$ denotes the image of p under the evaluation homomorphism $i_\alpha : F[x] \to F$.)

(a) Doing long division of polynomials we find that $q = 3x^2 + 10$ and $r = 9$. In doing this division, a key point is that in $\mathbb{Z}_{11}$, division by 4 is the same as multiplication by 3.

(b) By the division theorem we can write $p = (x-\alpha)q+r$ where $q, r \in F[x]$ and $\deg(r) < \deg(x-\alpha)$, that is $\deg(r) = 0$, so r is a constant polynomial and can be regarded as an element of F. Applying the evaluation homomorphism i_α, we have $p(\alpha) = i_\alpha(p) = i_\alpha(x - \alpha)i_\alpha(q) + i_\alpha(r)$. Now $i_\alpha(x - \alpha) = 0$ and $i_\alpha(r) = r$. Putting this into the previous equation completes the proof.

(5) True or false:

(a) The quotient group $(\mathbb{Z} \times \mathbb{Z})/\langle(2, 4)\rangle$ is isomorphic to $\mathbb{Z}$.

(b) There exists a nonzero homomorphism from the group $\mathbb{Z}_{33}$ to the group $\mathbb{Z}_{20}$.

(a) False. This quotient group cannot be isomorphic to $\mathbb{Z}$ because it contains an element of order 2, namely the coset $(1, 2) + \langle(2, 4)\rangle$. This coset has order 2 because $(1, 2)^2 = (2, 4)$ is an element of the subgroup $\langle(2, 4)\rangle$.

(b) False. Let $\phi : \mathbb{Z}_{33} \to \mathbb{Z}_{20}$ be a homomorphism. The fundamental homomorphism theorem says that $\mathbb{Z}_{33}/\operatorname{Ker}(\phi) \simeq \operatorname{Im}(\phi)$. Since the left side is the quotient of $\mathbb{Z}_{33}$ by a subgroup, its order must divide 33. Since the right side is a subgroup of $\mathbb{Z}_{20}$, its order must divide 20. Since the greatest common divisor of 33 and 20 is 1, both sides must be one element groups, which means that ϕ is the zero homomorphism.