Math 3124 Final Exam Solutions

May 13, 2004

1. (5 pts each) Let G be a group. For an element $x \in G$ define the map $\sigma_x : G \to G$ by

$$\sigma_x(g) = xgx^{-1}.$$

(a) Prove that σ_x is an automorphism of G.

Let $g, h \in G$. Then

$$\sigma_x(gh) = xghx^{-1} = xgx^{-1}\, xhx^{-1} = \sigma_x(g)\sigma_x(h).$$

So σ_x is a homomorphism. Notice that

$$\sigma_{x^{-1}} \circ \sigma_x(g) = x^{-1}(xgx^{-1})x = g \qquad \forall\, g \in G$$
$$\sigma_x \circ \sigma_{x^{-1}}(g) = x(x^{-1}gx)x^{-1} = g \qquad \forall\, g \in G.$$

So $\sigma_{x^{-1}}$ is inverse of σ_x, hence σ_x is an isomorphism. As $\sigma_x : G \to G$, it is an automorphism of G.

Remark: you can also do this by showing that σ_x is one-to-one and onto.

(b) Let $\alpha : G \to \mathrm{Aut}(G)$ be the map $\alpha(g) = \sigma_g$. Prove that α is a homomorphism.

We need to show $\alpha(xy) = \alpha(x)\alpha(y)$ for all $x, y \in G$, that is $\sigma_{xy} = \sigma_x \circ \sigma_y$. Clearly, σ_{xy} and $\sigma_x \circ \sigma_y$ have the same domains and codomains. For any $g \in G$,

$$\sigma_{xy}(g) = (xy)g(xy)^{-1} = xygy^{-1}x = \sigma_x \circ \sigma_y(g).$$

Remark: Remember you show two maps are equal by showing they have the same domains and codomains, and they map everything in this domain to the same element in the codomain. Most of you got the idea here, the biggest problem was getting the notation right. One example of broken notation is $\alpha(xy) = \sigma_{xy}(g)$, where the LHS is a map $G \to G$ and the RHS is an element of G.

(c) Prove that $\mathrm{im}(\alpha)$ is a normal subgroup of $\mathrm{Aut}(G)$.

By Theorem 18.2.(d), $\mathrm{im}(\alpha)$ is a subgroup of $\mathrm{Aut}(G)$. To show that it is a normal subgroup, we need to verify that for all $x \in G$ and all $\beta \in \mathrm{Aut}(G)$, $\beta \circ \sigma_x \circ \beta^{-1} \in \mathrm{im}(\alpha)$. For all $g \in G$,

$$\beta \circ \sigma_x \circ \beta^{-1}(g) = \beta(\sigma_x(\beta^{-1}(g))) = \beta(x\beta^{-1}(g)x^{-1}) = \beta(x)g\beta(x)^{-1} = \sigma_{\beta(x)}(g).$$

So $\beta \circ \sigma_x \circ \beta^{-1} = \sigma_{\beta(x)} \in \mathrm{im}(\alpha)$.

Remark: Here some of you assumed that all elements in $\mathrm{Aut}(G)$ looked like σ_x for some $x \in G$. In general, this is not true. Those elements of $\mathrm{Aut}(G)$ that look like conjugation by an element of G are called inner automorphisms, while those that don't are called outer automorphisms. So here you showed that the inner automorphisms form a normal subgroup of the automorphisms.
Another problem was that some of you forgot that in order to prove something is a normal subgroup, you need to first prove that it's a subgroup.

(d) Recall the definition of the center of G from Exercise 7.24:

$$Z(G) = \{g \in G \mid gh = hg \ \forall\, h \in G\}.$$

Prove that $Z(G)$ is a normal subgroup of G and

$$G/Z(G) \cong \mathrm{im}(\alpha).$$

We will prove that $\ker(\alpha) = Z(G)$. If $x \in G$ then

$$x \in \ker(\alpha) \iff \sigma_x = \iota_G \iff \sigma_x(g) = g \quad \forall\, g \in G \iff$$

$$xgx^{-1} = g \quad \forall\, g \in G \iff xg = gx \quad \forall\, g \in G \iff x \in Z(G).$$

Clearly, $Z(G) \subseteq G$. Since $Z(G)$ is the kernel of a homomorphism, it is a normal subgroup of G. Now by the corollary to the Fundamental Homomorphism Theorem proved in class

$$G/Z(G) = G/\ker(\alpha) \cong \mathrm{im}(\alpha).$$

Remark: Once you show $Z(G) = \ker(\alpha)$, you get for free that $Z(G)$ is a normal subgroup. There is no reason to waste time and effort proving this first, then showing that $Z(G) = \ker(\alpha)$.
To show $Z(G) = \ker(\alpha)$, it is not enough to prove that α maps every element of $Z(G)$ to ι_G. This only proves $\mathbb{Z}(G) \subseteq \ker(\alpha)$. You also need $\ker(\alpha) \subseteq Z(G)$. Or you can just prove both inclusions at the same time, as above.
Some of you tried to reprove the FHT here. There is no need to do that, you know the theorem, use it.

2. Let G be a group. Define the map $\sigma_x : G \to G$ as in the previous problem. Define the following operation on the set $G \times G$:

$$(x,\, y) * (s,\, t) = (x\sigma_y(s),\, yt).$$

(a) (10 pts) Prove that $G \times G$ is a group with respect to this operation.

Since $\sigma_s(y) \in G$, $(x\sigma_y(s),\, yt) \in G \times G$, so G is indeed closed under $*$.
The element (e, e) works as an identity:

$$(e,e)(x,y) = (e\sigma_e(x), ey) = (x,y) \qquad \forall\, (x,y) \in G \times G$$
$$(x,y)(e,e) = (x\sigma_y(e), ye) = (xyey^{-1}, y) = (x,y) \qquad \forall\, (x,y) \in G \times G$$

To find the inverse of (x, y)

$$(x,\, y) * (s,\, t) = (e, e)$$
$$(x\sigma_y(t),\, yt) = (e, e),$$

so

$$yt = e \implies t = y^{-1}$$
$$x\sigma_y(s) = e \implies \sigma_y(s) = x^{-1} \implies s = \sigma_{y^{-1}}(x^{-1}) = y^{-1}x^{-1}y,$$

where $\sigma_{y^{-1}}$ appears because it is the inverse of σ_y. Hence $(\sigma_{y^{-1}}(x^{-1}), y^{-1})$ is the right inverse of (x, y). Let us show it also works as a left inverse:

$$(\sigma_{y^{-1}}(x^{-1}),\, y^{-1}) * (x,\, y) = (\sigma_{y^{-1}}(x^{-1})\sigma_{y^{-1}}(x), y^{-1}y) = (\sigma_{y^{-1}}(x^{-1}x), e) = (e, e).$$

Finally, for associativity, let $(x,y),(s,t),(a,b) \in G \times G$.

$$\begin{aligned}((x,y)*(s,t))*(a,b) &= (x\sigma_y(s), yt)*(a,b) = (x\sigma_y(s)\sigma_{yt}(a), ytb)\\ (x,y)*((s,t)*(a,b)) &= (x,y)*(s\sigma_t(a), tb) = (x\sigma_y(s\sigma_t(a)), ytb)\\ &= (x\sigma_y(s)\sigma_y(\sigma_t(a)), ysb) = (x\sigma_y(s)\sigma_{yt}(a), ysb) \qquad \surd\end{aligned}$$

where we shrewdly used the fact that σ_y is a homomorphism from 1.(a) and that $\sigma_y \circ \sigma_t = \sigma_{yt}$ from 1.(b).

Remark: Most of you did these computations directly by expanding out what the σ's do. I did it this way for two reasons. One is to show the connection with problem 1, and the other is because there is a deeper principle behind all this. What I gave you here is an example of a semidirect product, which is something Durbin talks about on p. 111, although he never mentions the word. He calls it an extension.
Here is what a semidirect product is. Take two groups G and H, and a homomorphism $\alpha : H \to \mathrm{Aut}(G)$. Now define the following operation on $G \times H$:

$$(g,h)*(g',h') = (g\alpha(h)(g'), hh'),$$

where $\alpha(h)(g')$ means take the map in $\mathrm{Aut}(G)$ that α sends h to and apply it to g'. You can prove this gives a group structure on $G \times H$ much the same way as above. (Why not try?) This group is denoted $G \ltimes H$.

(b) (5 pts) Let $e \in G$ be the identity and

$$H = \{(g,\, e) \mid g \in G\}.$$

Prove that H is a normal subgroup of $G \times G$.

Again, the slick way to do this is to show H is the kernel of a homomorphism. Let $\theta : G \times G \to G \times G$ be defined as

$$\theta(x,y) = (e,y).$$

It is easy to see that this is a homomorphism. Let $(x,y),(s,t) \in G \times G$:

$$\theta(x,y)\theta(s,t) = (e,s)*(e,t) = (e\sigma_s(e), st) = (e,st) = \theta((x,y)*(s,t)).$$

That $\ker(\theta) = H$ is obvious. So H is a normal subgroup of G.

Remark: You can also do the proof directly, but don't forget to prove that H is a subgroup.

3. (5 pts each) Let G be a group. Define the map $\sigma_x : G \to G$ as in Problem 1.
   (a) Let $g \in G$ be fixed. For $x, y \in G$, define the relation $\sim_g$ as $x \sim_g y$ iff $\sigma_x(g) = \sigma_y(g)$. Show that $\sim_g$ is an equivalence relation on G.

For all $x \in G$, $\sigma_x(g) = \sigma_x(g)$, so $x \sim_g x$. Hence $\sim_g$ is reflexive. If $x \sim_g y$, then $\sigma_x(g) = \sigma_y(g) \implies \sigma_y(g) = \sigma_x(g) \implies y \sim_g x$. Hence $\sim_g$ is symmetric. Let $x \sim_g y$ and $y \sim_g z$. Then $\sigma_x(g) = \sigma_y(g)$ and $\sigma_y(g) = \sigma_z(g)$, so $\sigma_x(g) = \sigma_z(g)$, and hence $x \sim_g z$. Hence $\sim_g$ is transitive. Really, $\sim_g$ is an equivalence relation because $=$ is.

Remark: You never need to use what the σ's really do. In fact, let S and T be sets, and M the set of maps $S \to T$. Pick an element $s \in S$ and define $\sim_s$ on M by $\alpha \sim_s \beta$ if $\alpha(s) = \beta(s)$. This is an equivalence relation on M by the same proof as above.

(b) Recall the definition of the centralizer of $g \in G$ from Exercise 7.23:

$$C(g) = \{h \in G \mid hg = gh\}.$$

We already know this is a subgroup of G, so we can look at its left cosets. Prove that the left cosets of $C(g)$ are the equivalence classes of $\sim_g$.

Notice that

$$\sigma_x(g) = \sigma_y(g) \iff xyx^{-1} = ygy^{-1} \iff gx^{-1}y = x^{-1}yg \iff$$

$$x^{-1}y \in C(g) \iff xC(g) = yC(g).$$

In fact, $\sim_g$ is the same equivalence relation as $x \sim y$ iff $x^{-1}y \in C(g)$, whose equivalence classes we know: they are the left cosets of $C(g)$.

Remark: A frequent mistake here was to prove only half of the statement by showing that two elements from the same left coset of $C(g)$ are also equivalent under $\sim_g$. But all this shows is that the left cosets are contained in the equivalence classes of $\sim_g$. For that matter, if $\sim_g$ were the equivalence under which any two elements of G are equivalent, this argument would still work. Make sure you understand that the equivalence class of a doesn't only consist of elements that are equivalent to a but it consists of <u>all</u> elements.

4. (5 pts each) Let $\sigma, \phi \in S_n$.
   (a) Suppose $\sigma = (a_1\ a_2 \dots a_k)$. Prove that

$$\phi \circ \sigma \circ \phi^{-1} = (\phi(a_1)\ \phi(a_2) \dots \phi(a_k)).$$

The domains and the codomains of the maps on the LHS and the RHS are the same: $I_n = \{1, 2, \dots, n\}$. To show that the maps are the same, we need to prove that they send every element of the domain to the same element in the codomain. Let $S = \{\phi(a_1), \phi(a_2), \dots, \phi(a_k)\} \subseteq I_n$.
Let $m \in I_n$. If $m \in S$, then $m = \phi(a_j)$ for some $1 \le j \le k$. Then

$$(\phi(a_1)\ \phi(a_2) \dots \phi(a_k))(m) = \begin{cases} \phi(a_{j+1} & \text{if } j < k \\ \phi(a_1) & \text{if } j = k \end{cases},$$

and

$$\phi \circ \sigma \circ \phi^{-1}(m) = \phi \circ \sigma \circ \phi^{-1}(\phi(a_j)) = \phi \circ \sigma(a_j) = \begin{cases} \phi(a_{j+1} & \text{if } j < k \\ \phi(a_1) & \text{if } j = k \end{cases}.$$

If $m \notin S$, then

$$(\phi(a_1)\ \phi(a_2) \dots \phi(a_k))(m) = m,$$

and since $\phi^{-1}(m) \notin \{a_1, a_2, \dots, a_n\}$,

$$\phi \circ \sigma \circ \phi^{-1}(m) = \phi(\sigma(\phi^{-1}(m))) = \phi(\phi^{-1}(m)) = m.$$

So the LHS and the RHS are indeed the same map.

Remark: There is no reason to assume that every element of the domain is of the form $\phi(a_j)$ for some $1 \le j \le k$, this is why the second check needs to be done. A common mistake I saw is the notation $m \in \sigma$. Since σ is a map and not a set, you cannot talk about something being an element of σ. If you want to talk about m being a number which σ sends to a different number, you can say $\sigma(m) \neq m$.

(b) Now suppose $\sigma = (a_1\ a_2 \dots a_k)\,(b_1\ b_2 \dots b_m)$. Prove that

$$\phi \circ \sigma \circ \phi^{-1} = (\phi(a_1)\ \phi(a_2) \dots \phi(a_k))\,(\phi(b_1)\ \phi(b_2) \dots \phi(b_m)).$$

Just like in problem 1.(a),

$$\begin{aligned}\phi \circ \sigma \circ \phi^{-1} &= \phi(a_1\ a_2 \dots a_k)\,(b_1\ b_2 \dots b_m)\phi^{-1} \\ &= \phi(a_1\ a_2 \dots a_k)\phi^{-1}\,\phi(b_1\ b_2 \dots b_m)\phi^{-1}(\phi(a_1) \\ &= \phi(a_2) \dots \phi(a_k))\,(\phi(b_1)\ \phi(b_2) \dots \phi(b_m)).\end{aligned}$$

Remark: Observe that conjugation by ϕ in S_n is a special case of the map introduced in problem 1, and this part is just a restatement that conjugation by ϕ is a homomorphism. There is no need to assume that the two cycles of σ are disjoint, and this is not given anyway.

(c) Recall that the cycle structure of σ is defined as the partition $n = n_1 + n_2 + \cdots n_j$ whose parts are the lengths of the disjoint cycles of σ. Conclude from the above that the cycle structure of $\phi \circ \sigma \circ \phi^{-1}$ is the same as the cycle structure of σ. In other words the cycle structure is invariant under conjugation in S_n.

Since ϕ is a one-to-one map, it send disjoint sets to disjoint sets. Therefore it sends the disjoint cycles of σ to disjoint cycles. It is clear from part (a) that the lengths of the cycles are preserved. The cycle structure of a permutation is the lengths of all the disjoint cycles. Hence the cycle structures of σ and $\phi \circ \sigma \circ \phi^{-1}$ are the same.

Remark: The observation that disjoint cycles remain disjoint after conjugating by ϕ is crucial.

5. (5 pts each) Let R be a ring. Define the center of R as

$$Z(R) = \{x \in R \mid xr = rx\ \forall\, r \in R\}.$$

(a) Prove that $Z(R)$ is a subring of R.

Clearly, $Z(R) \subseteq R$. Since $0r = 0 = r0$ for all $r \in R$, $0 \in Z(R)$, so $Z(R)$ is nonempty. Let $x, y \in Z(R)$. Then

$$(x+y)r = xr + yr = rx + ry = r(x+y) \qquad \forall\, r \in R,$$

so $x + y \in Z(R)$. Also

$$(xy)r = x(yr) = x(ry) = (xr)y = (rx)y = r(xy) \qquad \forall\, r \in R,$$

so $xy \in Z(R)$.
Let $x \in R$. Then

$$(-x)r = -(xr) = -(rx) = r(-x) \qquad \forall\, r \in R,$$

so $-x \in Z(R)$.
By Theorem 25.2, $Z(R)$ is a subring of R.

(b) Find the center of $M_2(\mathbb{Z})$, the ring of 2×2 matrices with integer entries. (Hint: Let E_{ij} be a matrix whose (i,j)-entry is 1, and all other entries are 0. Try multiplying a generic matrix by such matrices on both left and right.)

Let

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z})$$

be a generic matrix. If M is in the center, then it must commute with all other matrices. In particular,

$$\begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = ME_{1,1} = E_{1,1}M = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$$

which implies $b = c = 0$. Also

$$\begin{pmatrix} 0 & a \\ 0 & c \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = ME_{1,2} = E_{1,2}M = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix}$$

which further implies $a = d$. So $Z(M_2(\mathbb{Z}))$ can only contain scalar matrices. But any scalar matrix commutes with any other matrix:

$$\begin{aligned} \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} x & y \\ z & w \end{pmatrix} &= a \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x & y \\ z & w \end{pmatrix} = a \begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} x & y \\ z & w \end{pmatrix} a \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}. \end{aligned}$$

So

$$Z(M_2(\mathbb{Z})) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in R \right\}.$$

Remark: This observation remains true $M_n(\mathbb{Z})$, and also holds in $M_n(\mathbb{Q})$, $M_n(\mathbb{R})$, $M_n(\mathbb{C})$ and in fact any $M_n(R)$ where R is a commutative ring. The center of $M_n(R)$ where R is a noncommutative ring is more complicated and depends on R as well.

6. (10 pts) Let $\mathbb{Z}_n$ be the ring as in Example 24.2. Prove that $\overline{k} \in \mathbb{Z}_n$ is a zero divisor if and only if $\gcd(k, n) \neq 1$. Conclude that $\mathbb{Z}_p$ is an integral domain.

Since $\mathbb{Z}_n$ is a commutative ring, we don't have to worry about which side we multiply on to get $\overline{0}$.

Suppose $\gcd(k, n) = 1$. Let $\overline{m} \in \mathbb{Z}_n$ be such that $\overline{k}\overline{m} = \overline{0}$, that is $n|km$. By Lemma 13.1, $n|m$, so $\overline{m} = \overline{0}$. That is $\overline{k}$ is not a zero divisor.

Conversely, suppose $\gcd(k, n) = d \neq 1$. If $d = n$, then $n|k$, so $\overline{k} = \overline{0}$, which is usually not considered a zero divisor, so the statement was sloppy, it would have been better to say $\overline{k} \in \mathbb{Z}_n$ is a zero divisor or $\overline{0}$ iff $\gcd(k, n) \neq 1$. (Thanks to Golnar for noticing this.) Otherwise $d < n$. Let $a = k/d$ and $b = n/d$. Since $1 < d$, $b < n$, so $\overline{b} \neq \overline{0}$. Now

$$\overline{kb} = \overline{kb} = \overline{\left(k\frac{n}{d}\right)} = \overline{\left(\frac{k}{d}n\right)} = \overline{an} = \overline{0},$$

so $\overline{k}$ is indeed a zero divisor.

Remark: In your homework (12.21), you proved that $\mathbb{Z}_{(n)} = \{\overline{k} | k \in Z \text{ and } \gcd(k, n) = 1\}$ is a group under multiplication. So every such $\overline{k}$ has an inverse in $\mathbb{Z}_{(n)} \subseteq \mathbb{Z}_n$. But an invertible element of a ring cannot be a zero divisor. For let R be a ring and $x, y \in R$, where x is invertible. If $xy = 0$, then $y = (x^{-1}x)y = x^{-1}(xy) = 0$. So this could also serve as the proof of the first half.

7. (15 pts) Let $k_1, k_2, \ldots, k_n \in \mathbb{Z}^* = \mathbb{Z}\backslash\{0\}$. Define the *greatest common divisor* of $k_1, k_2, \ldots, k_n$ as the number $d \in \mathbb{Z}^+$ such that

1. $d|k_i$ for all $1 \leq i \leq n$,
2. if $c|k_i$ for all $1 \leq i \leq n$, then $c|d$.

Denote this by $\gcd(k_1, k_2, \ldots, k_n)$.

Prove that such a number exists, is unique, and is an integer linear combination of $k_1, k_2, \ldots, k_n$. (Hint: you don't have to do this from scratch, you may use what you know about the greatest common divisor of two integers.)

Let

$$\begin{aligned} d_2 &= \gcd(k_1, k_2) \\ d_3 &= \gcd(d_2, k_3) \\ &\vdots \\ d_n &= \gcd(d_{n-1}, k_n) \end{aligned}$$

Now d_n is clearly a positive integer and $d_n|d_{n-1}|d_{n-2}|\cdots|d_2$, so $d_n|k_i$ for $1 \leq i \leq n$. Since d_1 is a linear combination of k_1 and k_2, d_3 is a linear combination of k_1, k_2, k_3, and so on. By induction, d_n is a linear combination of $k_1, k_2, \ldots, k_n$.

Suppose $c|k_i$ for all $1 \leq i \leq n$. Then c divides any linear combination of the k's, so in particular, $c|d_n$. Hence $d = d_n$ is a greatest common divisor of $k_1, k_2, \ldots, k_n$.

Now suppose d' is also a greatest common divisor of $k_1, k_2, \ldots, k_n$. Then by property 2, $d|d'$ and $d'|d$, and since they are both positive, $d = d'$.

Remark: You can also prove this by the same argument we first gave for the existence of the gcd of two nonzero integers. You could do it using the Euclidean algorithm too, but the notation would be messy. The common mistake among those that gave a similar proof as above was to say that since the gcd of two numbers is unique, therefore by following the above recursive algorithm, the gcd of n numbers is also unique. This is not logically sound. Surely, the algorithm will yield a unique number, which turns out to be a gcd. But how do you know that someone else can't come up with a different algorithm that yields a different gcd of the n numbers?

8. (5 pts each) Let $\alpha : G \to H$ be a group homomorphism with $K = \ker(\alpha)$. Let N be a normal subgroup of G such that $N \subseteq K$. Define $\theta : G/N \to H$ as

$$\theta(Ng) = \alpha(g).$$

(a) Prove that θ is well-defined.

Let $x, y \in G$. Suppose $Nx = Ny$. Then $x^{-1}y \in N \subseteq K$, so

$$\alpha(x^{-1}y) = e_h \implies \alpha(x)^{-1}\alpha(y) = e_H \implies \alpha(x) = \alpha(y) \implies \theta(Nx) = \theta(Ny).$$

So θ is well-defined.

Remark: θ is of course also a homomorphism, but you were not asked to prove this.

(b) Let $\pi : G \to G/N$ be the canonical projection ($\pi(g) = Ng$). Show that $\alpha = \theta \circ \pi$. When this happens, we say α factors through G/N.

First notice that $\theta \circ \pi : G \to H$, so the domains and the codomains match. Now for any $g \in G$,

$$\theta \circ \pi(g) = \theta(Ng) = \alpha(g).$$

So $\theta \circ \pi = \alpha$.

9. (5 pts each) **Extra credit problem.** Let R be a ring.
   (a) Prove that $(a+b)(a-b) = a^2 - b^2$ for all $a, b \in R$ iff R is commutative.

   First, notice $(a+b)(a-b) = a^2 + ba - ab - b^2$. Now for all $a, b \in R$,

   $$a^2 + ba - ab - b^2 = a^2 - b^2 \iff ba - ab = 0 \iff ba = ab.$$

   The latter is the definition of commutative ring, so R is commutative iff $(a+b)(a-b) = a^2 - b^2$ for all $a, b \in R$.

   (b) Prove that $(a+b)^2 = a^2 + 2ab + b^2$ for all $a, b \in R$ iff R is commutative.

   First, notice $(a+b)^2 = (a+b)(a+b) = a^2 + ba + ab + b^2$. Now for all $a, b \in R$,

   $$a^2 + ba + ab + b^2 = a^2 + 2ab + b^2 \iff ba + ab = ab + ab \iff ba = ab.$$

   The latter is the definition of commutative ring, so R is commutative iff $(a+b)^2 = a^2 + 2ab + b^2$ for all $a, b \in R$.

   Remark: $2ab$ in the above expression doesn't mean multiply 2 by a then by b. For that matter, the ring may not have an element $2 = 1 + 1$. But $2ab$ always makes sense as $ab + ab$.

10. (5 pts each) **Extra credit problem.** Let $m, n \in \mathbb{Z}$ be relatively prime.
   (a) Let and $a, b \in \mathbb{Z}$. Show that there exists $x \in \mathbb{Z}$ such that

   $$\begin{aligned} x &\equiv a \mod m \\ x &\equiv b \mod n. \end{aligned}$$

   So we are looking for x such that $x = sm + a = tn + b$ for some $s, t \in Z$. Hence $sm - tn = b - a$. We know there exist $q, r \in \mathbb{Z}$ such that $qm + rn = 1$. Let $s = (b-a)q$ and $t = (a-b)r$. Then

   $$sm - nt = (b-a)qm - (a-b)rn = (b-a)(qm + rn) = b - a \implies sm + a = tn + b.$$

   Now let $x = sm + a = tn + b$.

   (b) Now suppose that $0 \leq a < m$ and $0 \leq b < n$. Show that there exists a unique $0 \leq x < mn$ such that

   $$\begin{aligned} x &\equiv a \mod m \\ x &\equiv b \mod n. \end{aligned}$$

   Do the same thing as in part (a) to come up with $y = sm + a = tn + b$. Now use the Division Algorithm to write $y = z(mn) + x$ with $x, z \in \mathbb{Z}$ and $0 \leq x < mn$. This x clearly satisfies the requirements.
   Suppose $0 \leq x' < mn$ also satisfies the congruences. Then $-mn < x - x' < mn$. Also, $m | x - x'$ and $n | x - x'$ and hence $\operatorname{lcm}(m, n) | x - x'$. But $\gcd(m, n) = 1$ implies $\operatorname{lcm}(m, n) = mn$, so $mn | x - x'$, and therefore $x - x' = 0$. That is $x = x'$.

   Remark: This is a special case of the Chinese Remainder Theorem.

11. (5 pts each) **Extra credit problem.** Let R be a ring with at least two elements. Suppose that for any nonzero $r \in R$ there exists a unique $s \in R$ such that $rsr = r$. Prove the following

(a) R has no zero divisors.

Let $r, x \in R$ with $r \neq 0$. Suppose $rx = 0$ or $xr = 0$. In either case, find the s as above and write

$$r = rsr = rsr - \underbrace{rxr}_{=0} = r(s - x)r.$$

But s was supposed to be the unique element in R which satisfies $rsr = r$, so $s - x = s$ and hence $x = 0$. So r cannot be a zero divisor. We can do this for any $r \neq 0$, so R has no zero divisors.

(b) $srs = s$.

$$rs = (rsr)s = r(srs) \implies rs - r(srs) = 0 \implies r(s - srs) = 0.$$

Since $r \neq 0$ and r cannot be a zero divisor, $s - srs = 0$ and hence $s = srs$.

(c) R has a multiplicative identity.

Let $x \in R$ be any element. Look at

$$rx = rsrx \implies rx - rsrx = 0 \implies r(x - srx) = 0.$$

Since $r \neq 0$ cannot be a zero divisor, $x - srx = 0$ and $x = srx$. On the other side,

$$xs = xsrs \implies xs - xsrs = 0 \implies (x - xsr)s = 0.$$

Since $s \neq 0$ cannot be a zero divisor, $x - xsr = 0$ and $x = xsr$. So sr works as both a left and a right identity. So we can denote sr by 1.

(d) Every nonzero element of R has a multiplicative inverse, that is R is a division ring.

Let $x \in R$ be any nonzero element. We know there exists $y \in R$ such that $xyx = x$. Hence

$$xyx = x \implies xyx - x = 0 \implies x(yx - 1) = 0.$$

Since x cannot be a zero divisor $yx - 1 = 0$ and $yx = 1$. Similarly,

$$xyx = x \implies xyx - x = 0 \implies (xy - 1)x = 0.$$

Since x cannot be a zero divisor $yx - 1 = 0$ and $yx = 1$. So y is a two-sided inverse of x.

Remark: If we had know at the beginning that R contains a 1 and cancelation lkaws hold for left and right multiplication, the statements would have been trivial to prove. But neither of these is required for a ring. In fact, since the existence of cancelation laws is equivalent to not having zero divisors, these are exactly what had to be proved.