Name: Anton Bernshteyn

No calculators, books, notes, &c. are allowed. Please justify all your answers.

Good luck!
Problem 1. (25 pts.)

Recall that if $A$ is a set and $f : S \to T$ is a function, then $f^A : S^A \to T^A$ is the function given by

$$f^A(g) := f \circ g \quad \text{for all } g \in S^A,$$

while $A^f : A^T \to A^S$ is the function given by

$$A^f(g) := g \circ f \quad \text{for all } g \in A^T.$$

Now, given two functions $f : S \to T$ and $h : A \to B$, define $f^h : S^B \to T^A$ by

$$f^h(g) := f \circ g \circ h \quad \text{for all } g \in S^B.$$

Show that $f^h = T^h \circ f^B = f^A \circ S^h$.

First, we check that the three functions $f^h$, $T^h \circ f^B$, and $f^A \circ S^h$ have the same domain and range, which is easiest to see on the following diagram:

Now, for each $g \in S^B$, we compute:

$$(f^A \circ S^h)(g) = f^A(S^h(g)) = f^A(g \circ h) = f \circ (g \circ h) = f^h(g);$$

$$(T^h \circ f^B)(g) = T^h(f^B(g)) = T^h(f \circ g) = (f \circ g) \circ h = f^h(g),$$

as desired.
Problem 2. (5+10+10+5 pts.)

Let $\ast$ be an associative binary operation on a set $X$. Suppose that $u \in X$ is a **left identity** for $\ast$, i.e., $u \ast x = x$ for all $x \in X$. Suppose also that each $x \in X$ has a **left inverse**, i.e., there is some element $x' \in X$ with $x' \ast x = u$.

(a) Show that for all $x, y, z \in X$, if $x \ast y = x \ast z$, then $y = z$.

(b) Conclude that for all $x \in X$, $x \ast u = x$; in other words, $u$ is an identity of $\ast$.

(c) Show that if $x \in X$ and $x'$ is a left inverse of $x$, then $x \ast x' = u$.

(d) Conclude that $(X, \ast)$ is a group.

(a) Suppose $x \ast y = x \ast z$ and let $x'$ be a left inverse of $x$. Then

$$y = u \ast y = (x' \ast x) \ast y = x' \ast (x \ast y) = x' \ast (x \ast z) = (x' \ast x) \ast z = u \ast z = z.$$

(b) Let $x'$ be a left inverse of $x$. We have

$$x' \ast (x \ast u) = (x' \ast x) \ast u = u \ast u = u = x' \ast x.$$

Applying the result of part (a) with

- $x'$ in place of $x$,
- $x \ast u$ in place of $y$, and
- $x$ in place of $z$,

we obtain $x \ast u = x$, as desired.

(c) Using the result of part (b), we can write

$$x' \ast (x \ast x') = (x' \ast x) \ast x' = u \ast x' = x' = x' \ast u.$$

Applying the result of part (a) with

- $x'$ in place of $x$,
- $x \ast x'$ in place of $y$, and
- $u$ in place of $z$,

we obtain $x \ast x' = u$, as desired.

(d) Part (b) shows that $u$ is an identity for $\ast$, while part (c) shows that every element of $X$ has an inverse under $\ast$, so $(X, \ast)$ satisfies the definition of a group.
Problem 3. (25 pts.)

Let $G$ be a group. Show that the function $\varphi : G \to G$ given by $\varphi(g) := g^{-1}$ for all $g \in G$ is a group homomorphism if and only if $G$ is Abelian.

For $g, h \in G$, we have

$$\varphi(gh) = (gh)^{-1} = h^{-1}g^{-1} \quad \text{and} \quad \varphi(g)\varphi(h) = g^{-1}h^{-1}. $$

Therefore, $\varphi$ is a homomorphism if and only if

$$h^{-1}g^{-1} = g^{-1}h^{-1} \quad \text{for all } g, h \in G. \quad (\ast)$$

Clearly, $(\ast)$ holds if $G$ is Abelian. Conversely, if $(\ast)$ holds, then for any $a, b \in G$, we can apply $(\ast)$ with $h = a^{-1}$ and $g = b^{-1}$ (and hence $h^{-1} = a$ and $g^{-1} = b$) to get $ab = ba$, as desired.
Problem 4. (5+20 pts.)

Let $G$ be a group. A set $S \subseteq G$ is **multiplicatively closed** if for all $a, b \in S$, we have $ab \in S$. By definition, every subgroup of $G$ is multiplicatively closed.

(a) Give an example of a group $G$ and a nonempty multiplicatively closed subset $S \subseteq G$ such that $S$ is not a subgroup of $G$.

(b) Show that if the group $G$ is finite, then every nonempty multiplicatively closed subset of $G$ is a subgroup of $G$.

(a) One can take, say, $G = \mathbb{Z}$ (with addition) and $S = \mathbb{N}^+$. The sum of any two positive integers is still positive, but $\mathbb{N}^+$ is not a subgroup of $\mathbb{Z}$ (for instance, 0, the identity of $\mathbb{Z}$, is not in $\mathbb{N}^+$).

(b) Suppose $G$ is a finite group with identity $e$ and $S \subseteq G$ is a nonempty multiplicatively closed subset. To argue that $S$ is a subgroup, we need to show that $e \in S$ and that for each $a \in S$, $a^{-1} \in S$.

Take any $a \in S$ (here we are using that $S \neq \varnothing$). Since $S$ is multiplicatively closed, we have

$$a^n = a \cdot a \cdot \cdots a \in S \quad \text{for all } n \in \mathbb{N}^+.$$ 

Since $G$ is finite, the elements $a, a^2, a^3, \ldots$ cannot be all distinct, so there are some $n, m \in \mathbb{N}^+$ with $n < m$ and $a^n = a^m$. Set $k := m - n$. Then $k \in \mathbb{N}^+$ and $a^k = a^n \cdot (a^m)^{-1} = a^n \cdot (a^n)^{-1} = e$, which shows that $e \in S$. Furthermore, if $a \neq e$, then $k \geq 2$ (because $a^1 = a \neq e$) and $a \cdot a^{k-1} = e$, i.e., $a^{-1} = a^{k-1} \in S$. Since $e^{-1} = e \in S$, the proof is complete.

Remark. The smallest $k \in \mathbb{N}^+$ such that $a^k = e$ is called the **order** of $a$ and is denoted by $|a|$. 
This page is intentionally left blank for use as scrap paper. If you want your work on this page to be graded, please indicate so clearly (including the problem number).
This page is intentionally left blank for use as scrap paper. If you want your work on this page to be graded, please indicate so clearly (including the problem number).
This page is intentionally left blank for use as scrap paper. If you want your work on this page to be graded, please indicate so clearly (including the problem number).
This page is intentionally left blank for use as scrap paper. If you want your work on this page to be graded, please indicate so clearly (including the problem number).
This page is intentionally left blank for use as scrap paper. If you want your work on this page to be graded, please indicate so clearly (including the problem number).