Algebra Problems

Many more problems are scattered around in various seminar handouts,
— some examples: "Wilson's theorem...", "...the Cauchy equation" —
either explicitly stated as HW, or just indicated by phrases
such as (Why?) or "Hint" or "It is easy to see that..."

In the following problems, G is a nonempty set with an associative binary operation $\cdot$ (a so-called semigroup), that is, $\cdot : G \times G \to G$ satisfies $(\forall a, b, c \in G)(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

As customary, we will often write ab for $a \cdot b$. All quantifiers below refer to the universe G, that is, we simply write $(\forall x)$ and $(\exists x)$ for $(\forall x \in G)$ and $(\exists x \in G)$.

Recall that $(G, \cdot)$ is a group if the following two additional properties hold:

(ii) G contains an identity [for $\cdot$]: $(\exists e)(\forall g) ge = g = eg$ [two-sided identity],

(iii) every element of G has an inverse: $(\forall g)(\exists h) gh = e = hg$ [two-sided inverse].

Problem 1. Prove that right identity and right inverses are sufficient, that is,

> *If there is an element $e \in G$ such that $(\forall g) ge = g$ and $(\forall g)(\exists h) gh = e$,*
> *then $(G, \cdot)$ is a group [that is, conditions (ii) and (iii) hold].*

[Hint: Firstly, left multiply $gh = e$ with h to show that a right inverse is a left inverse too. Then, right-multiply $gh = e$ with g to show that e is a left identity too, and hence unique.]

Clearly, all linear equations are solvable in a group: $(\forall a, b)(\exists x) ax = b$ and $(\forall a, b)(\exists y) ya = b$. The following problem states the converse.

Problem 2. Show that if all linear equations are solvable in G then $(G, \cdot)$ is a group:

> *If (iv) $(\forall a, b)(\exists x) ax = b$, and (v) $(\forall a, b)(\exists y) ya = b$, then $(G, \cdot)$ is a group.*

While the one-sided versions of (ii) and (iii) are sufficient to guarantee that G is a group under $\cdot$, the one-sided condition (iv) alone - without the matching (v) - is not sufficient:

Problem 3. Find a set G with an associative binary operation $\cdot : G \times G \to G$ such that the operation $\cdot$ satisfies (iv) yet $(G, \cdot)$ is not a group.

Problem 4. If in a non-trivial group all elements other than the identity have the same finite order p, then p is prime. [G is non-trivial means $o(G) > 1$; G has at least two elements.]

The following corollary is a special case of the theorem in the LBB that a field is a vector space over any of its subfields.

Corollary. If in a non-trivial additive Abelian group G all non-zero elements have the same finite order p, then p is prime and G is a vector space over $\mathbb{Z}_p$ with the natural scalar multiplication $kg = \underbrace{g + g + \ldots + g}_{k}$ for $k = 0, 1, \ldots, p - 1$.