MATH 113 - WORKSHEET 5
WEDNESDAY 7/24

In problems (1)-(3), let $(A, +)$ be an abelian group. An *endomorphism* of A is a group homomorphism $\phi : A \to A$. Let $\mathrm{End}(A) = \mathrm{Hom}(A, A)$ be the set of endomorphisms of A.

Given two endomorphisms of A, ϕ and ψ, we can add them to obtain a new function $(\phi + \psi) : A \to A$, given by $(\phi + \psi)(a) = \phi(a) + \psi(a)$.

As usual, we can also compose them to obtain a new function $(\phi \circ \psi) : A \to A$.

(1) Show that $(\mathrm{End}(A), +)$ is an abelian group. Here $+$ is addition of functions as defined above. This includes checking that if $\phi, \psi \in \mathrm{End}(A)$, then $(\phi + \psi) \in \mathrm{End}(A)$.

(2) Given the result of Problem (1), show that $(\mathrm{End}(A), +, \circ)$ is a ring with unity.

Note that this ring is not commutative in general, since function composition is not commutative in general.

(3) Given a ring with unity R, let $A(R) = (R, +)$ be the abelian group of R under addition. Note that *as sets*, $A(R) = R$. Given $r \in R$, show that $\lambda_r : A(R) \to A(R)$, defined by $\lambda_r(a) = ra$, is an endomorphism.

Given the result of Problem (2), show that the map $\phi : R \to \mathrm{End}(A(R))$ given by $\phi(r) = \lambda_r$ is a one-to-one ring homomorphism.

This result is the analogue of Cayley's theorem for rings. Cayley's theorem states that every group embeds into the permutation group of some set (in fact, its own underlying set). We have shown that every ring with unity embeds into the endomorphism ring of some abelian group (in fact, its own underlying abelian group).

(4) Let R be a ring with unity, and let $U(R) = \{r \in R \mid r \text{ is a unit}\}$. Show that $(U(R), \cdot)$ is a group. This includes showing that $U(R)$ is closed under multiplication.

If F is a field, conclude that $F^* = F \setminus \{0\}$ is an abelian group.

The group $U(R)$ is called the *group of units* of R and is sometimes denoted $R^\times$.

(5) Consider the field $\mathbb{Z}_p$, p prime. Use Problem (4) (i.e. the fact that $\mathbb{Z}_p^*$ is a group) to show that for all $a \in \mathbb{Z}_p^*$, $a^{p-1} = \overline{1}$, and $a^p = a$.

This result (and its restatement in (6)) is called *Fermat's little theorem*.

(6) Let p be a prime number. Use Problem (5) to show that if $a \in \mathbb{Z}$, with $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$ and $a^p \equiv a \pmod{p}$.

Use this result to compute the remainder of $3^{6000002}$ when divided by 7.