Math 561/661 **Fall 2021**
Homework 4 **Drew Armstrong**

---

1. Equivalence Relation = Partition. Given a set S, a *relation* on S is just a subset $\mathscr{R} \subseteq S^2$ of ordered pairs. We usually write $a \sim b$[1] instead of $(a, b) \in \mathscr{R}$, and say "a is related to b". We further say that $\mathscr{R}$ is an *equivalence relation* if for all $a, b, c \in S$ we have

- $a \sim a$
- $a \sim b \;\Rightarrow\; b \sim a$
- $a \sim b$ and $b \sim c \;\Rightarrow\; a \sim c$

On the other hand, we define a *partition* of the set S as a set of subsets $X_i \subseteq S$ with the following properties:

- $S = \cup_i X_i$
- $X_i \cap X_j = \emptyset$ for all $i \neq j$

Prove that these two concepts are equivalent. [Hint: Given an equivalence $\sim$ and an element $a \in S$ let $[a] = \{b \in S : a \sim b\} \subseteq S$ denote the *equivalence class of* a and let $S/\!\sim$ denote the set of equivalence classes. Conversely, given a partition $X_i \subseteq S$ write $a \sim b$ to denote the fact that $a, b \in S$ are members of the same part X_i.]

2. The Group of Units.

(a) Given a ring R we define the set of units $R^\times = \{u \in R : \exists v \in R, uv = 1\}$. Prove that this set satisfies the following three properties:
- $1 \in R^\times$
- $u \in R^\times \;\Rightarrow\; u^{-1} \in R^\times$
- $u, v \in R^\times \;\Rightarrow\; uv \in R^\times$

We say that the structure $(R^\times, \cdot, 1)$ is a *group*, called the *group of units* of R.

(b) Prove that the group of units of the ring $\mathbb{Z}/n\mathbb{Z}$ is given by

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{a \in \mathbb{Z}/n\mathbb{Z} : \gcd(a, n) = 1\}.$$

We will write $\phi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$ to denote the size of this group. [Hint: If $\gcd(a, n) = d \geq 2$, say $a = dk$ and $n = d\ell$, show that $a\ell \equiv 0 \bmod n$ and use this to show that a is not a unit mod n. Conversely, if $\gcd(a, n) = 1$, use the Vector Euclidean Algorithm to show that a is a unit mod n.]

3. The Euler-Fermat Theorem. Let $(G, \cdot, 1)$ be an *abelian group*. That is, let G be a set with a binary operation $\cdot : G \times G \to G$ and a special element $1 \in G$ satisfying the following axioms:

- $ab = ba$
- $a(bc) = (ab)c$
- $1a = a$
- $\forall a \in G, \exists b \in G, ab = 1$

(a) For all $a, b, c \in G$ prove that $ab = ac$ implies $b = c$.

(b) For any element $a \in G$ we define the function $\mu_a : G \to G$ by $b \mapsto ab$. Use part (a) to show that this function is injective.

---

[1]There are limited number of appropriate symbols for relations and sometimes we run out.

(c) If $G = \{a_1, a_2, \dots, a_m\}$ is a finite set then the function μ_a must also be surjective, so

$$\prod_{b \in G} b = \prod_{b \in G} \mu_a(b)$$
$$a_1 a_2 a_3 \cdots a_m = (aa_1)(aa_2) \cdots (aa_m).$$

Use this to prove that $a^m = 1$.[2]

(d) The group of units $(\mathbb{Z}/n\mathbb{Z})^\times$ is an example of an abelian group. Apply the result from part (c) to prove Euler's Theorem:

$$a^{\phi(n)} \equiv 1 \bmod n \qquad \text{for all integers } a \text{ satisfying } \gcd(a, n) = 1.$$

(e) If $p \in \mathbb{Z}$ is prime, use the result from part (d) to prove Fermat's Little Theorem:

$$a^{p-1} \equiv 1 \bmod p \qquad \text{for all integers } a \text{ satisfying } p \nmid a.$$

[2]The notation a^m means $a \cdot a \cdot a \cdots a$ (m times).