HOMEWORK 1

YOUR NAME

Due date: Monday of Week 5

Problem 1. *Let $X = \mathbb{Z} \times (\mathbb{Z} - \{0\})$. Consider the relation R on X defined by*

$$R = \{((a,b),(c,d)) \in X \times X : ad = bc\}.$$

Show that R is an equivalence relation. (Actually X/R is the set of rational numbers. Think about why this is so.)

Problem 2. *Show that the set $F = \left\{a + b\sqrt{2} : a, b \in \mathbb{Q}\right\}$ with the usual addition and multiplication is a field.*

Problem 3. *In this problem, we construct a field $(F, +, \times)$ which has 4 elements. Denote the 4 elements by $\{0, 1, \alpha, \beta\}$, where 0 is the identity of the abelian group $(F, +)$, 1 is the identity element of the abelian group $(F - \{0\}, \times)$, α, β are the other two elements in F. Fill the following tables of the binary operations and check that F together with these two binary operations is indeed a field. (You only need to write up the details that every element in $F - \{0\}$ has an inverse.)*

$+$	0	1	α	β
0				
1				
α				
β				

$\times$	0	1	α	β
0				
1				
α				
β				

Problem 4. *In this problem, we construct a field $(F, +, \cdot)$ which has 9 elements. Let $\mathbb{F}_3 = \{0, 1, 2\}$ be the finite field with 3 elements with the usual notation. This means that 0 is the additive identity, 1 is the multiplicative identity and $2 = 1 + 1$. Let α be an extra element, which is not in $\mathbb{F}_3$ but $\alpha^2 = 2$ (where the 2 in α^2 means $\alpha^2 = \alpha \cdot \alpha$ and 2 on the right side denotes the element " 2" in $\mathbb{F}_3$). Consider the set $F = \{a\alpha + b | a, b \in \mathbb{F}_3\}$. Define addition and multiplication on F in the usual sense. Namely,*

$$(a_1\alpha + b_1) + (a_2\alpha + b_2) = (a_1 + a_2)\alpha + (a_2 + b_2),$$
$$(a_1\alpha + b_1) \cdot (a_2\alpha + b_2) = (a_1b_2 + a_2b_1)\alpha + (2a_1a_2 + b_1b_2),$$

for $a_1, a_2, b_1, b_2 \in \mathbb{F}_3$. Show that $(F, +, \cdot)$ is a field. This is a field with 9 elements.

(Using similar method, try to construct a field with 25 elements.)

1. A little arithmetic of integers

Let $\mathbb{N}$ be the set of natural numbers, namely, $\mathbb{N} = \{0, 1, 2, \dots\}$. Let $S \subset \mathbb{N}$ be a subset. An element $a \in S$ is called a minimal element of S, if for any $b \in S$, there exists another element $c \in \mathbb{N}$ such that $b = a + c$. One important property of $\mathbb{N}$ is given in the following

Theorem 1. *Any non-empty subset S of $\mathbb{N}$ contains a minimal element. Moreover, this minimal element is unique.*

Problem 5. *Prove Theorem 1 by induction.*

Hint: For $n \in \mathbb{N}$, consider the statement $P(n)$: any subset S which contains n has a minimal element. Show that the statement $P(n)$ is true for any $n \in \mathbb{N}$ by induction.

Problem 6. *Given $a, b \in \mathbb{N}$ with $b \neq 0$. Show that there exists $q, r \in \mathbb{N}$ with $0 \leq r < b$ such that $a = bq + r$.*

Hint: Consider the set $S = \{a - bq \mid q \in \mathbb{N} \text{ and } a - bq \in \mathbb{N}\}$. Use Theorem 1.

Recall that an integer $p \in \mathbb{N}$ is called prime, if $p \neq 0, 1$ and if $q|p$ (which means $p = qb$ for some $b \in \mathbb{N}$) for $q \in \mathbb{N}$, then $q = 1$ or $q = p$.

Problem 7. *Let p be a prime integer and $a \in \mathbb{N}$ with $1 \leq a < p$. Show that there exists integers $x, y \in \mathbb{Z}$ such that $ax + py = 1$. Conclude that $\mathbb{Z}/p\mathbb{Z}$ is a field.*

Hint: Consider the set $S = \{ax + py \mid x, y \in \mathbb{Z}, ax + py > 0\} \subset \mathbb{N}$.

Problem 8. *Let $p = 31$ and $a = 13$. Find an element $x \in \mathbb{Z}/p\mathbb{Z}$ such that $ax = 1$ in $\mathbb{Z}/p\mathbb{Z}$.*

You should learn this in elementary school.