Math 127
Homework Problem Set 1

Problem 1. (i) Let $\mathbb{F}$ be a field. Consider $a, b, c \in \mathbb{F}$ and show the following:

$$-a = (-1) \cdot a\,, \qquad -(b \cdot c) = (-b) \cdot c = b \cdot (-c)\,.$$

(Note that here e.g. $-a$ denotes the additive inverse of a, while -1 denotes the additive inverse of the multiplicative identity 1, and $(-1) \cdot a$ means the product of -1 and a; similarly $-(b \cdot c)$ stands for the additive inverse of the product $b \cdot c$, while $(-b) \cdot c$ denotes the product of $-b$ and c.)

(ii) Let $\mathbb{F}$ be a field, and let x be a non-zero element of $\mathbb{F}$ (recall that we know then that x has a multiplicative inverse, which we denote by x^{-1}). Show that $-x$ has a multiplicative inverse too, and that

$$(-x)^{-1} = -(x^{-1})\,.$$

(iii) Let $m > 1$ be a positive integer (not necessarily a prime), and consider the ring $\mathbb{Z}_m$. Let $[k], [l]$ be two invertible elements of $\mathbb{Z}_m$. Show that their product $[k] \cdot [l]$ is also invertible, and that

$$\big([k] \cdot [l]\big)^{-1} = [k]^{-1} \cdot [l]^{-1}\,.$$

Problem 2. (*Cancellation laws for addition and multiplication*) Let $\mathbb{F}$ be a field, and let a, b, c be elements of $\mathbb{F}$. Show the following.
(i) (*Cancellation law for addition*) If $a + b = a + c$, then $b = c$.
(ii) (*Cancellation law for multiplication*) If $ab = ac$ and moreover $a \neq 0$, then $b = c$.

Remark. One of the purposes of the following problem is to test your understanding of certain mathematical statements and certain logical implications we have discussed in class.

Problem 3. (i) & (ii) Recall the Proposition we saw in the Lecture 3 slides (right after the definition of a 'field', see slide 5 in that slide presentation).

Determine which, if any, of the two parts of the Proposition would still hold true if we replaced the field $\mathbb{F}$ in the statement of the Proposition by an (arbitrary) commutative ring $\mathcal{R}$, and which part(s) would not necessarily be true anymore.

Justify your answers fully (that is, if, say, Part (i) remains true in every commutative ring $\mathcal{R}$ as well, then give a proof for this; otherwise verify that Part (i) doesn't necessarily hold true in a commutative ring $\mathcal{R}$ *(what proof approach do you need to use in the latter case?)*).

(iii) Let $\mathcal{R}$ be a commutative ring, and suppose z, w are elements of $\mathcal{R}$ such that $zw = 0$ and $z \neq 0$. Show that w is **not** invertible (that is, it does not have a multiplicative inverse).

Practice Exercise. Ask yourself the analogous question regarding the Cancellation Laws for Addition and Multiplication: would any of the two laws continue to hold true in commutative rings as well? Is any of them not necessarily true anymore? Justify your answers fully.

Problem 4. Let $\mathbb{Q}(\sqrt{17})$ be the following subset of $\mathbb{R}$: it is the set of numbers of the form $a+b\sqrt{17}$ where $a, b \in \mathbb{Q}$, with usual addition and multiplication (note that all these numbers are real numbers, so we can add or multiply any two of them in the standard way).

(i) First check that $\mathbb{Q}(\sqrt{17})$ is closed under the addition and under the multiplication in $\mathbb{R}$. That is, if $x, y \in \mathbb{Q}(\sqrt{17})$, then $x+y$ is also an element of $\mathbb{Q}(\sqrt{17})$, and so is $x \cdot y$.

Note that this will imply that the triple of the set $\mathbb{Q}(\sqrt{17})$, together with the usual operations of addition and multiplication of real numbers when restricted to elements of $\mathbb{Q}(\sqrt{17})$, is of the type required in the definition of a 'field'.

(ii) Prove that $\mathbb{Q}(\sqrt{17})$ with these operations is a field (which will also give us that it is a subfield of $\mathbb{R}$).

Problem 5. Exactly one of the following two structures is a field.

1. The set $\mathbb{Z}_3^2$ (that is, the set of ordered pairs (a, b) with both a and b in $\mathbb{Z}_3$) together with coordinate-wise addition, and multiplication defined according to the formula $(a, b)(c, d) \stackrel{\text{def}}{=\!=} (ac-bd, ad+bc)$ (note that the operations on the right-hand side are the standard operations in $\mathbb{Z}_3$).
2. The set $\mathbb{Z}_5^2$ with addition and multiplication defined in the same way as above.

(i) Determine which one is the field, and (ii) verify that the other one **is a commutative ring**, but **is not a field**. Justify your answer fully.

[*Hint.* You may wish to find first what the multiplicative identity in each case should be.]

Problem 6. (i) For every non-zero element of $\mathbb{Z}_{13}$, find its multiplicative inverse.

(ii) Only one of $\mathbb{Z}_{37}$, $\mathbb{Z}_{39}$ and $\mathbb{Z}_{41}$ is **not** a field. Determine which one and justify why it is not a field (by showing that it does not satisfy all the necessary axioms).

[*Clarification.* In both parts here, it is understood that the operations of addition and of multiplication are the standard ones, as we defined them in class.

Problem 7. (a) *(Practice question)* Consider the complex numbers $z = 3+4\mathbf{i}$ and $w = 2-3\mathbf{i}$.

Simplify the following expressions in $\mathbb{C}$ by writing them in the form $a+b\mathbf{i}$ with $a, b \in \mathbb{R}$: $z+w$, zw, z/w, $z \cdot \overline{w}$.

Determine also $\operatorname{Re} z$, $\operatorname{Im} z$, $|z|$, and $\arg(z)$.

(b) Find a complex number y such that $y^2 = \overline{-3-4\mathbf{i}}$.

(c) *(Practice question)* Simplify the following expression in $\mathbb{Z}_{11}$ by expressing your answer as an integer in the range -5 to 5:

$$\frac{(2+22-5)(3^2+6)}{4}\,.$$

(d) Find all solutions, if any, to each of these equations in $\mathbb{Z}_{13}$, expressing the answers as integers in the range -6 to 6: (i) 3x=5; (ii) $x^2 = 1$; (iii) $x^2 = -1$.

(e) Find all solutions, if any, to each of these equations in $\mathbb{Z}_{16}$, expressing the answers as integers in the range 0 to 15: (i) $x^2 = 0$; (ii) $x^2 = 1$; (iii) $12x = 7$; (iv) $12x = 4$.