Math 113 — Problem Set 10 — William Guss

(P174. 6) Compute $(-3,5)(2,-4) \in \mathbb{Z}_4 \times \mathbb{Z}_{11}$

Proof. The product is as follows. First $-3 \times 2 \mod 4 = -6 \mod 4 = 2$. Then $5 \times -4 = -20 \mod 11 = -22 + 2 = 2 \mod 11$. Thus the product is $(2,2)$. $\square$

(P175. 12) Decide whether or not the indicated operations of addition and multiplicatioin are defined on the set and givea ring structure. Then describe the ring, if $S = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$ with usual addition and multiplication.

Proof. First $(a+b\sqrt{2})+(c+d\sqrt{2}) = a+c+(b+d)\sqrt{2} \in S$. Then since $+$ is the usual addition on $\mathbb{R}$, it is Abelian. Furthermore $0 = 0+0\sqrt{2} \in S$ and by the inheritied additio operation $a+b\sqrt{2}+0 = a+b\sqrt{2}$. Lastly there are addative inverses, let $a + b\sqrt{2} \in S$ then claim that $(-a) + (-b)\sqrt{2}$ is its inverse; namely, $a+b\sqrt{2}+(-a)+(-b)\sqrt{2} = (a-a)+(b-b)\sqrt{2} = 0+0\sqrt{2} = 0$. Thus $\langle S, + \rangle$ is a commutative group.

Next $(a + b\sqrt{2}) \times (c + d\sqrt{2}) = ac + ad\sqrt{2} + bc\sqrt{2} + 2db = (ac + 2db) + (ac + ad)\sqrt{2} \in S$ and thus S is closed under multiplication. Note we used that $\times$ is distributed as inherited by the ring $\langle \mathbb{R}, +, \times \rangle$Furthermore $1 \in S$ and $1(a + b\sqrt{2}) = 1a + 1b\sqrt{2} = a + b\sqrt{2} \in S$ so there is a unital element. Again since $\langle \mathbb{R}, \times \rangle$ is a commutative group then $\times$ is commutative on S.

Now S is a commutative unital subring of $\mathbb{R}$. Now to find multiplictive inverses, observe the following

$$\frac{1}{a+b\sqrt{2}} = \frac{1}{a+b\sqrt{2}} \frac{\overline{a+b\sqrt{2}}}{\overline{a+b\sqrt{2}}} = \frac{\overline{a+b\sqrt{2}}}{a^2-2b^2} = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2} \in S$$

and this solution is algebraically unique since we inherit the operations of $\mathbb{R}$. Thus $\langle S, +, \times \rangle$ is a field. $\square$

(P182. 2) Solve the equation $3x = 2$ in the field
(a) $\mathbb{Z}_7$.

Proof. We must find x so that $x \mod 7 = 2$ and $3|x$. First $3 \times 1 = 3 \mod 7 = 3$, then $3 \times 3 = 9 \mod 7 = 2$, thus $x = 2$ in $\mathbb{Z}_7$. $\square$

(b) $\mathbb{Z}_{23}$

Proof. We msut find x so that $x \mod 23 = 2$ and $3|x$. Take $x = 16$, then $3x = 48$. Finally $23 \times 2 = 46$ so $48 \mod 46 = 2$ and $3x = 2$. We could have found this by showing that $3y = 1$ if $y = 3^{-1}$ and thus $3 \times 8 = 24 \mod 23 = 1$ so $y = 8$. Then $3x \equiv 2$ is solved by $x \equiv y3x \equiv y \times 2 = 16$. $\square$

(P182. 3) Find all solutions of the equation $x^2 + 2x + 2 = 0$ in $\mathbb{Z}_6$.

Proof. First $\mathbb{Z}_6$ is not a field since $2 \times 3 = 6 \equiv 0$ so $\mathbb{Z}_6$ is not an integral domain. We factor the polynomial however and get $(x+1)(x+1) = -1 \mod 6 = 5 \in \mathbb{Z}_6$. Thus we find all y so that $y^2 = 5$, or equivalently we must find all y so that $y^2 + 1 = 0$. We get initially that

$$\begin{aligned} 0 + 1 &= 1 \\ 1 + 1 &= 2 \\ 4 + 1 &= 5 \\ 9 + 1 &= 10 \equiv 4 \\ 16 + 1 &= 17 \equiv 5 \\ 25 + 1 &= 26 \equiv 2 \end{aligned}$$

Thus there are no such solutions. This problem illustrates that $\mathbb{Z}^6$ does not have a square root of -1. For the grader the following is an exact verification.

$$\begin{aligned} 0^2 + 0 + 2 &= 2 \\ 1^2 + 2 + 2 &= 5 \\ 2^2 + 4 + 2 = 8 + 2 &= 10 \equiv 4 \\ 3^2 + 6 + 2 = 9 + 8 &= 17 \equiv 5 \\ 4^2 + 8 + 2 = 16 + 10 &= 26 \equiv 2 \\ 5^2 + 10 + 2 = 25 + 12 &= 37 \equiv 1 \end{aligned}$$

$\square$

(P182. 14) Show that the matrix $A = \begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix}$ is a divisior of zero in $M_2(\mathbb{Z})$.

Proof. We need to show that $AB = 0$ in $M_2(\mathbb{Z})$. Then we must solve specifically

$$AB = \begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = 0$$

As a system of equations we get

$$a + 2c = 0b + 2d = 02a + 4c = 02b + 4d = 0$$

which is then just

$$a + 2c = 0b + 2d = 0$$

So take $a = -2, c = 1$ and $b = -2, d = 1$. Thus

$$\begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix} \begin{bmatrix} -2 & -2 \\ 1 & 1 \end{bmatrix} = 0$$

Next we must show that $CA = 0$. Since $A = (1, 2) \otimes (1, 2)$, $A^T = A$ and thus $(AB)^T = 0^T = 0 = B^T A^T = B^T A$; therefore $CA = 0$ with $C = B^T \neq 0$. Therefore A is a divisor of 0 since it is a left and right divisor of 0. $\square$