Solution Set 2C

Daniel Gardiner

October 28, 2004

Math 23a
Prof. Boller

(C) Let p be a fixed prime number, and let $V = (\mathbb{Z}/p\mathbb{Z})^n$.

1. **How many vectors are in the vector space V?**

   Solution: Since any vector in $(\mathbb{Z}/p\mathbb{Z})^n$ has n co-ordinates and each co-ordinate has p possible values, we conclude that there are p^n vectors in $(\mathbb{Z}/p\mathbb{Z})^n$.

2. **In the case $n = 2$ and arbitrary $p > 2$, show that any vector may be written as a linear combination of the two vectors $(1,2)$ and $(1,1)$.**

   Solution: Since the vector $(1,0) = 2(1,1) - (1,2)$ and the vector $(0,1) = (1,2) - (1,1)$, we can write any $v \in (\mathbb{Z}/p\mathbb{Z})^2 = (a,b)$, with $a, b \in \mathbb{Z}/p\mathbb{Z}$ as follows:
   As $(a,b) = a(1,0) + b(0,1)$, we can substitute for $(1,0)$ and $(0,1)$. Hence,

$$(a,b) = a(1,0) + (b(0,1)$$

$$= a(2(1,1) - (1,2)) + b((1,2) - (1,1))$$
$$= 2a(1,1) - a(1,2) + b(1,2) - b(1,1)$$
$$= (2a - b)(1,1) + (b - a)(1,2).$$

   By assumption, $a, b \in \mathbb{Z}/p\mathbb{Z}$, and $\mathbb{Z}/p\mathbb{Z}$ is a field, so $(2a - b), (b - a) \in \mathbb{Z}/p\mathbb{Z}$. Thus, we have written our generic v as a linear combination of $(1,1)$ and $(1,2)$.

3. **In the case $n = 2$ and $p = 7$, show that the vectors $(1,6)$, $(2,4)$, and $(3,3)$ are not linearly independent.**

Solution: Since, in $(\mathbb{Z}/7\mathbb{Z})^2$, $(3,3) = (1,6)+(2,4)$, we know that $(1,6)+(2,4)-(3,3) = 0$. As there exists a non-trivial linear combination of the three vectors equal to 0 (that is, a linear combination with at least one non-zero scalar), our vectors are not linearly independent.

4. **In the case $n = 2$ and $p = 7$, find an explicit example (writing down all vectors) of a non-trivial subspace (that is, not $\{0\}$, and not V).**

Solution: Consider $W = \{(a,0) | a \in \mathbb{Z}/7\mathbb{Z}\}$. Since W is a subset of $(\mathbb{Z}/7\mathbb{Z})^2$, it suffices to show that W is closed under addition and scalar multiplication.

Taking $(a,0),(b,0) \in W$, we note that $(a,0)+(b,0) = (a+b,0)$. But since $a,b \in \mathbb{Z}/7\mathbb{Z}$, $(a+b) \in \mathbb{Z}/7\mathbb{Z}$; hence $(a+b,0) \in W$.

Likewise, taking $(a,0) \in W$ and $c \in \mathbb{Z}/7\mathbb{Z}$, we find that $c(a,0) = (ca,0)$. But since $a,c \in \mathbb{Z}/7\mathbb{Z}$, $(ca) \in \mathbb{Z}/7\mathbb{Z}$; hence $(ca,0) \in W$.

Thus, W is a subspace of $(\mathbb{Z}/7\mathbb{Z})^2$.