ALGEBRA I

We use the following standard notation: $\mathbb{Z}$ is the ring of integers, $\mathbb{Q}$ is the field of rational numbers, $\mathbb{R}$ is the field of real numbers, $\mathbb{C}$ is the field of complex numbers, and $\mathbb{F}_q$ is the finite field with q elements (where $q = p^e$ for some prime p and $e \geq 1$).

(1) Let N be a positive integer with prime factorization $p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ (where the p_i's are distinct prime numbers, and the exponents e_i are positive). How many solutions to the equation $x^2 = x$ are there in the ring $\mathbb{Z}/N\mathbb{Z}$?

Solution: By the Chinese remainder theorem, we have $\mathbb{Z}/N\mathbb{Z} \cong \prod_{i=1}^{k} \mathbb{Z}/p_k^{e_k}$. Let x in $\mathbb{Z}/N\mathbb{Z}$ correspond to $(x_1, x_2, \ldots, x_k)$ in the product. Then $x^2 = x$ if and only $x_i^2 = x_i$ for each i. So our challenge is to compute the number of solutions to $x^2 = x$ in $\mathbb{Z}/p^e\mathbb{Z}$.

We claim there are exactly two solutions: 0 and 1. Indeed, if $x^2 \equiv x \bmod p^e$, then $x(1-x) \equiv 0 \bmod p^e$. But $x + (1-x) = 1$, so it is impossible that both x and $1-x$ are divisible by p, and we must either have $x \equiv 0 \bmod p^e$ or $1 - x \equiv 0 \bmod p^e$.

So there are 2 solutions to $x^2 = x$ in $\mathbb{Z}/p^e\mathbb{Z}$, and thus 2^k solutions in $\mathbb{Z}/N\mathbb{Z}$.

(2) An element x of a ring is called **nilpotent** if there is a positive integer N with $x^N = 0$. Show that, in a commutative ring, the set of nilpotent elements form an ideal.

Solution: We must check two things: That a sum of two nilpotent elements is nilpotent, and that the product of a nilpotent element with an arbitrary element is nilpotent. For the first, let $x_1^{N_1} = x_2^{N_2} = 0$. Then we have $(x_1+x_2)^{N_1+N_2} = \sum_{k=0}^{N_1+N_2} \binom{N_1+N_2}{k} x_1^k x_2^{N_1+N_2-k}$. For each term in this sum, either $k \geq N_1$ or $N_1 + N_2 - k \geq N_2$, so each summand is 0 and we deduce that $x_1 + x_2$ is nilpotent. For the second, if $x^N = 0$ then $(ax)^N = a^N x^N = 0$ as well.

(3) (a) Let $A = \{(x, y, z) \in \mathbb{Z}^3 : x \equiv y \equiv z \bmod 3\}$. Give three vectors $\vec{u}_1$, $\vec{u}_2$, $\vec{u}_3$ such that $A = \mathbb{Z}\vec{u}_1 \oplus \mathbb{Z}\vec{u}_2 \oplus \mathbb{Z}\vec{u}_2$.

(b) Let $B = \{(x, y, z) \in \mathbb{Z}^3 : x + y + z \equiv 0 \bmod 3\}$. Give three vectors $\vec{v}_1$, $\vec{v}_2$, $\vec{v}_3$ such that $B = \mathbb{Z}\vec{v}_1 \oplus \mathbb{Z}\vec{v}_2 \oplus \mathbb{Z}\vec{v}_2$.

Date: Aug 2021.

(c) Describe the abelian group B/A explicitly as a product of one or more cyclic groups.

Solution:

(a) We claim that $(1,1,1)$, $(3,0,0)$ and $(0,3,0)$ is one such list. Clearly, each of these vectors is in A, and the vectors are clearly linearly independent, so we just need to show that every vector in A is an integer linear combination of these. Suppose that (x,y,z) is in A. Then $(x,y,z) = (x-z, y-z, 0) + z(1,1,1) = \frac{x-z}{3}(1,0,0) + \frac{y-z}{3}(0,1,0) + z(1,1,1)$. We have shown that every vector in A is an integer linear combination of $(1,1,1)$, $(3,0,0)$ and $(0,3,0)$.

(b) We claim that $(1,1,1)$, $(1,-1,0)$, $(0,1,-1)$ is one such list. Clearly, each of these vectors is in B, and the vectors are clearly linearly independent, so we just much show that every vector in B is an integer linear combination of these. Suppose that (x,y,z) is in B. Then $(x+y+z)/3$ is an integer, and we see that $(u,v,w) := (x,y,z) - (x+y+z)/3(1,1,1)$ is also in B. This latter vector has $u+v+w = 0$, so $(u,v,w) = u(1,-1,0) - w(0,1,-1)$. We have shown that every vector in B is an integer linear combination of $(1,1,1)$, $(1,-1,0)$ and $(0,1,-1)$.

(c) We claim that $B/A \cong \mathbb{Z}/3\mathbb{Z}$. There are many ways to do this computation; here is one of them. Let $\vec{u}_1 = (1,1,1)$, $\vec{u}_2 = (3,0,0)$ and $\vec{u}_3 = (0,3,0)$ be the basis of A and let $\vec{v}_1 = (1,1,1)$, $\vec{v}_2 = (1,-1,0)$ and $\vec{v}_3 = (0,1,-1)$ be the basis of B. We compute the change of basis matrix between the $\vec{u}$'s and the $\vec{v}$'s, namely, $\vec{u}_1 = \vec{v}_1$, $\vec{u}_2 = \vec{v}_1 + 2\vec{v}_2 + \vec{v}_3$ and $\vec{u}_3 = \vec{v}_1 - \vec{v}_2 + \vec{v}_3$. So B/A is isomorphic to the cokernel of the matrix $\begin{bmatrix} 1 & 1 & 1 \\ 0 & 2 & -1 \\ 0 & 1 & 1 \end{bmatrix}$. The invariant factors of this matrix are $(3,1,1)$, so $B/A \cong \mathbb{Z}/3\mathbb{Z}$.

(4) Let V be a finite dimensional vector space over a field k. Let $T : V \to V$ be a k-linear map of rank r. Calculate the rank of $\bigwedge^n T : \bigwedge^n V \to \bigwedge^n V$ for all n.

Solution: We claim that $\bigwedge^n T$ has rank $\binom{r}{n}$. Choose a basis $e_{r+1}, e_{r+2}, \ldots, e_N$ for $\mathrm{Ker}(T)$ and complete it to a basis $e_1, e_2, \ldots, e_N$ for V. Put $f_i = T(e_i)$. Since $\mathrm{Span}(e_1, \ldots, e_r)$ is transverse to $\mathrm{Span}(e_{r+1}, e_{r+2}, \ldots, e_N) = \mathrm{Ker}(T)$, the vectors $T(e_1), T(e_2), \ldots, T(e_r)$ are linearly independent. Put $f_i = T(e_i)$ for $1 \leq i \leq r$ and compute $f_1, f_2, \ldots, f_r$ to a basis $f_1, f_2, \ldots, f_N$ of V.

So

$$T(e_i) = \begin{cases} f_i & i \leq r \\ 0 & i > r \end{cases}.$$

Then

$$T(e_{i_1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_n}) = \begin{cases} f_{i_1} \wedge f_{i_2} \wedge \cdots \wedge f_{i_n} & i_1, i_2, \ldots, i_n \leq r \\ 0 & \text{otherwise} \end{cases}.$$

So, if we write $\bigwedge^n T$ using the basis $e_{i_1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_n}$ for the source and $f_{i_1} \wedge f_{i_2} \wedge \cdots \wedge f_{i_n}$ for the target, we get a diagonal matrix. The nonzero diagonal entries come from $\{i_1, \ldots, i_n\}$ a subset of $\{1, 2, \ldots, r\}$, so there are $\binom{r}{n}$ nonzero entries on the diagonal and the matrix has rank $\binom{r}{n}$.

(5) Show that $\mathbb{Z}[x]$ and $\mathbb{Z}[x, x^{-1}]$ are not isomorphic as rings.

Problem: There are many ways to do this, but probably the easiest is to note that they have non-isomorphic unit groups: The units of $\mathbb{Z}[x]$ are ± 1, whereas the units of $\mathbb{Z}[x, x^{-1}]$ are $\{\pm x^n\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$.