Algebra 1 QR Solutions — August 2023

Problem 1. Let $\mathbb{F}_p$ be the field with p elements and let U be a two dimensional vector space over $\mathbb{F}_p$. How many distinct tensors of the form $u \otimes v$ are there in $U \otimes U$?

Solution. If $u, u', v, v' \in U$ are non-zero then

$$u \otimes v = u' \otimes v' \iff u = \alpha u' \text{ and } v = \alpha^{-1} v'$$

for scalar some α. To see this, first suppose that u and v are linearly independent, and thus a basis for U. Then $u \otimes u$, $u \otimes v$, $v \otimes u$, and $v \otimes v$ are a basis for $U \otimes U$. Writing u' and v' in the (u, v) basis and computing $u' \otimes v'$ leads to the result. The case where u and v are dependent is similar (use an auxiliary third vector to make a basis). We thus see that the map $(u, v) \mapsto u \otimes v$ (on non-zero vectors) is $(p-1)$-to-1, and so we obtain $(p^2-1)^2/(p-1)$ distinct tensors. The final answer is one more than this since the zero vector is also of the form $u \otimes v$ (take $u = v = 0$).

Problem 2. Let V be a real vector space of finite dimension n and let $\langle\ ,\ \rangle$ be a non-degenerate symmetric bilinear form on V. Suppose that there is a basis e_1, e_2, $\ldots$, e_n of V such that $\langle e_i, e_i \rangle$ is positive for all $1 \le i \le n$. What are the possible signatures of $\langle\ ,\ \rangle$?

Solution. The signature cannot be $(0, n)$, i.e., the form cannot be negative definite, since there are vectors with positive norm. Every other signature is possible. To see this, consider the vector space $U = \mathbb{R}^n$ equipped with the standard form of signature (r, s), with $r > 0$; that is, $e_1, \ldots, e_n$ are orthogonal and $\langle e_i, e_i \rangle$ is 1 if $1 \le i \le r$, and -1 if $i > r$. Let $v_i = e_i$ for $1 \le i \le r$, and $v_i = 2e_1 + e_i$ for $i > r$. Then $v_1, \ldots, v_n$ is a basis of U, and each v_i has positive norm.

Problem 3. Let $\mathbb{Z}[i]$ be the subring of the complex numbers generated by i (a square root of -1). Up to isomorphism, how many $\mathbb{Z}[i]$-modules are there with 25 elements? You may use without proof that $\mathbb{Z}[i]$ is a principal ideal domain (PID), and we helpfully point out that $5 = (2+i)(2-i)$ is the prime factorization of 5.

Solution. If M is a finite $\mathbb{Z}[i]$-module then the structure theorem tells us that

$$M = \mathbb{Z}[i]/(\pi_1^{e_1}) \oplus \cdots \oplus \mathbb{Z}[i]/(\pi_n^{e_n}),$$

where $\pi_1, \ldots, \pi_r$ are prime elements. This decomposition is unique up to re-ordering and changing the π_j's by units. Now suppose that M has 25 elements. Then $25 \cdot M = 0$, and so we must have $\pi_j \mid 25$ for each j. Since $5 = (2+i)(2-i)$ is the prime factorization of 5, it follows that we must have $\pi_j = 2+i$ or $\pi_j = 2-i$ for each j. Since $\mathbb{Z}[i]/(2+i)$ has 5 elements and $\mathbb{Z}[i]/(2+i)^2$ has 25 elements (and similarly for $2-i$), we see that the possibilities for M are

$$\mathbb{Z}[i]/(2+i) \oplus \mathbb{Z}[i]/(2+i), \quad \mathbb{Z}[i]/(2+i) \oplus \mathbb{Z}[i]/(2-i), \quad \mathbb{Z}[i]/(2-i) \oplus \mathbb{Z}[i]/(2-i)$$

$$\mathbb{Z}[i]/(2+i)^2, \quad \mathbb{Z}[i]/(2-i)^2$$

So there are 5 modules with 25 elements, up to isomorphism.

Problem 4. Let A be an $n \times n$ matrix of complex numbers and suppose that the characteristic polynomial of A is $(t-1)^k t^{n-k}$. Show that there is a polynomial $f(x)$ in $\mathbb{C}[x]$ such that $f(A)$ also has characteristic polynomial $(t-1)^k t^{n-k}$, and $f(A)^2 = f(A)$.

Solution. Using Jordan normal form, we see that A can be conjugated into block form

$$\begin{pmatrix} 1+X & 0 \\ 0 & Y \end{pmatrix},$$

where the top left block is $k \times k$, and X and Y are strictly upper triangular (and thus nilpotent). We have

$$A^n = \begin{pmatrix} 1+X' & 0 \\ 0 & 0 \end{pmatrix}$$

where X' is also strictly upper triangular. We thus have

$$(1-A^n)^n = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

Thus $1-(1-A^n)^n$ is idempotent and has the same characteristic polynomial as A.

Problem 5. Let $\mathbb{Q}(x)$ be the field of rational functions in x with coefficients in $\mathbb{Q}$. Let R be the subring of $\mathbb{Q}(x)$ consisting of functions of the form $\frac{f(x)}{g(x)}$ for f, $g \in \mathbb{Z}[x]$ and $g(0) = 1$. Show that the ideal xR is prime, but not maximal, in R.

Solution. There is a well-defined ring homomorphism $\phi\colon R \to \mathbb{Z}$ given by evaluation at 0, i.e., $\phi(f/g) = f(0)$ (choosing g so that $g(0) = 1$). We claim that $\ker(\phi) = xR$. Since ϕ is surjective and $R/\ker(\phi) = \mathbb{Z}$ is a domain and not a field, this will prove that xR is prime and not maximal.

It is clear that $x \in \ker(\phi)$, and so $xR \subset \ker(\phi)$. Now suppose that $f/g \in \ker(\phi)$, where $g(0) = 1$. Then $f(0) = 0$, and so x divides f in $\mathbb{Z}[x]$, and so we can write $f = xf'$ for some $f' \in \mathbb{Z}[x]$. Thus $f/g = x(f'/g)$ belongs to xR, as required.