Algebra I QR August 2024

Problem 1. Let R be a commutative ring with 1. Let $R^\star \subset R$ be the set of invertible elements and $\mathfrak{m} := R \setminus R^\star$.
(1) Show that if $\mathfrak{m}$ is an abelian group, then it is the unique maximal ideal of R.
(2) Conversely, suppose that R has a unique maximal ideal. Show that this maximal ideal is equal to $\mathfrak{m}$.

Solution.

(1) Clearly no element of $R^\star$ can lie in a proper ideal of R. Thus, it suffices to show that $\mathfrak{m}$ is an ideal. If $\mathfrak{m}$ is an abelian group, we must check that it is closed under multiplication by arbitrary $r \in R$. Suppose $m \in \mathfrak{m}$. If $rm = u \in R^\star$, then $(u^{-1}r)m = 1$ would imply that m is invertible, a contradiction. Thus $rm \in \mathfrak{m}$, and $\mathfrak{m}$ is an ideal.

(2) It suffices to show that every $m \in \mathfrak{m}$ lies in the unique maximal ideal I. The principal ideal $\langle m \rangle$ generated by m is not the whole ring R since $1 \notin \langle m \rangle$. But $m \in \langle m \rangle \subset I$, and thus $\mathfrak{m} \subset I$.

Problem 2. Let V denote the vector space of real polynomials ax^2+bx+c of degree less than or equal to 2. Define

$$(p(x), q(x)) = (p(x)q(x))'|_{x=0}.$$

Here $f(x)'$ denotes the derivative of f. Check that $(.,.)$ is a symmetric bilinear form, find its signature, and find an orthogonal basis for $(.,.)$.

Solution. For polynomials $p(x), q(x), r(x) \in V$ and scalars $a, b \in \mathbb{R}$, we have

$$\begin{aligned}(p(x), aq(x)+br(x)) &= (ap(x)q(x)+bp(x)r(x))'|_{x=0}\\ &= a(p(x)q(x))'|_{x=0} + b(p(x)r(x))'|_{x=0}\\ &= a(p(x),q(x)) + b(p(x),r(x))\end{aligned}$$

using linearity of the derivative and of $|_{x=0}$, and

$$(p(x), q(x)) = (p(x)q(x))'|_{x=0} = (q(x)p(x))'|_{x=0} = (q(x), p(x)).$$

Thus $(.,.)$ is a symmetric bilinear form.

Calculating the values of the bilinear form on the ordered basis $\{1, x, x^2\}$, we obtain the matrix

$$\begin{bmatrix}0 & 1 & 0\\ 1 & 0 & 0\\ 0 & 0 & 0\end{bmatrix}$$

which has eigenvalues $1, -1, 0$. Thus the signature of $(.,.)$ is $(1,1,1)$. By direct computation, the polynomials $\{1-x, 1+x, x^2\}$ give an orthogonal basis.

Problem 3. How many elements does each of the following groups have?

(1) $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/20\mathbb{Z})$

(2) $(\mathbb{Z}/3\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Q}$

(3) $(\mathbb{Z} \times \mathbb{Z})/M$, where M is the subgroup of $\mathbb{Z} \times \mathbb{Z}$ generated by $(3, 2)$ and $(2, 5)$

Solution.

(1) The generator of $\mathbb{Z}/6\mathbb{Z}$ can be sent to 0 or 10 in $\mathbb{Z}/20\mathbb{Z}$, and thus

$$|\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/20\mathbb{Z})| = 2.$$

(2) We compute in $\mathbb{Z}/3\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}$ that

$$a \otimes (p/q) = a \otimes (3p/3q) = 3a \otimes (p/3q) = 0 \otimes (p/3q)$$

Thus $\mathbb{Z}/3\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}$ is the trivial group with one element.

(3) $(\mathbb{Z} \times \mathbb{Z})/M$ has order 11 which is the absolute value of the determinant of

$$\begin{bmatrix} 3 & 2 \\ 2 & 5 \end{bmatrix}$$

Problem 4.

(1) Let $\mathbb{F}_2$ denote the field with two elements. For $(a, b) \in \mathbb{F}_2 \times \mathbb{F}_2$, define the ring

$$R_{a,b} := \mathbb{F}_2[x]/(x^2 + ax + b).$$

For which distinct pairs (a, b) and (c, d) do we have a ring isomorphism $R_{a,b} \cong R_{c,d}$? Which of these rings are fields? Which of these rings are integral domains?

(2) For each of the rings in (1), list all the prime ideals.

Solution.

(1) Of the four monic quadratic polynomials $x^2, x^2 + 1, x^2 + x, x^2 + x + 1$ in $\mathbb{F}_2[x]$, only $x^2 + x + 1$ is irreducible. Thus $(x^2 + x + 1) \subset \mathbb{F}_2[x]$ is a maximal ideal and $R_{1,1} = \mathbb{F}_2[x]/(x^2+x+1)$ is a field (the field $\mathbb{F}_4$ with 4 elements). It is also an integral domain. None of the other three rings are fields or integral domains, and in particular are not isomorphic to $R_{1,1}$.

The two rings $R_{0,0} = \mathbb{F}_2[x]/(x^2)$ and $R_{1,0} = \mathbb{F}_2[x]/(x^2 + 1)$ are isomorphic under the ring map $x \mapsto x + 1$. The ring $R_{0,1} = \mathbb{F}_2[x]/(x^2 + x)$ is not isomorphic to $R_{0,0}$ (and thus not isomorphic to $R_{1,0}$). This is because $R_{0,0}$ contains a nonzero element x which squares to 0, but $R_{0,1}$ does not:

$$1^2 = 1, \qquad x^2 = x, \qquad (x + 1)^2 = x + 1, \qquad \text{in } R_{0,1}.$$

Thus the four rings give exactly three isomorphism classes. Exactly one of the four rings is a field and it is also the only integral domain.

(2) Since $R_{1,1} = \mathbb{F}_4$ is a field, it has a unique prime ideal (0).

In the ring $R_{0,0}$, the elements $1, 1 + x$ generate the unit ideal. The zero ideal (0) is not prime. Thus the only prime ideal is $(x) = \{0, x\}$. Similarly the only prime ideal in $R_{1,0}$ is $(x + 1)$.

In the ring $R_{0,1}$, the element 1 generates the unit ideal. The zero ideal (0) is not prime. The other two ideals are $(x) = \{0, x\}$ and $(1 + x) = \{0, 1 + x\}$ which are both prime.

Problem 5. Let F be a field and V be a vector space of dimension n over F. For $1 \leq k \leq n$, consider the set

$$X_k := \{(W, U) \mid W, U \subset V \text{ and } \dim(W) = k = \dim(U)\}$$

of ordered pairs of k-dimensional subspaces of V.
(1) The diagonal action of $\mathrm{GL}_n(F)$ on X_k is given by $g \cdot (W, U) = (g \cdot W, g \cdot U)$, for $g \in \mathrm{GL}_n(F)$. How many orbits are there of the diagonal action of $\mathrm{GL}_n(F)$ on X_k?
(2) Suppose that $F = \mathbb{F}_q$ is a finite field with q elements. What is the cardinality of X_k?

Solution.
(1) Let $Z = W \cap U$ and $r := \dim(Z)$. Then $\dim(W + U) = 2k - r \leq n$. Thus $\max(0, 2k - n) \leq r \leq k$, and it is clear that r is an invariant of the action of $\mathrm{GL}_n(F)$ on X_k. We claim that the orbits of the diagonal action of $\mathrm{GL}_n(F)$ are classified by possible values of r. Thus there are $\min(k + 1, n - k + 1)$ orbits.

Let $a_1, \ldots, a_r$ be a basis of Z, and extend this to bases $a_1, \ldots, a_r, b_1, \ldots, b_{k-r}$ (resp. $a_1, \ldots, a_r, b'_1, \ldots, b'_{k-r}$) of W (resp. U). Then $a_1, \ldots, a_r, b_1, \ldots, b_{k-r}, b'_1, \ldots, b'_{k-r}$ is a basis of $W + U$, and it can be extended to a basis of V. Since $\mathrm{GL}_n(F)$ acts transitively on bases of V, it follows that all pairs (W, U) with the same value of $r = \dim(W \cap U)$ form a single orbit.
(2) First we count the number of independent sets of vectors $B = \{b_1, \ldots, b_k\}$ of size k. We first choose a nonzero vector $b_1 \in V$ in $q^n - 1$ ways, then pick b_2 linearly independent to b_1 in $q^n - q$ ways, and so on. Thus the number of such sets of independent vectors is equal to

$$(q^n - 1)(q^n - q) \cdots (q^n - q^{k-1}).$$

Each such B spans a subspace W of dimension k, and by the same counting argument, each W arises from

$$(q^k - 1)(q^k - q) \cdots (q^k - q^{k-1})$$

such sets B. So the number of possible choices for W is equal to

$$\frac{(q^n - 1)(q^n - q) \cdots (q^n - q^{k-1})}{(q^k - 1)(q^k - q) \cdots (q^k - q^{k-1})} = \frac{(q^n - 1)(q^{n-1} - 1) \cdots (q^{n-k+1} - 1)}{(q^k - 1)(q^{k-1} - 1) \cdots (q - 1)}.$$

The cardinality of X_k is the square of this number.