Exercise 11

Rings: definitions, units, zero divisors, polynomial rings

1. Show that the matrices $M(n \times n, \mathbb{C})$ form a noncommutative ring. What are the units of $M(n \times n, \mathbb{C})$? What are the zero divisors?
Solution The matrices $M(n \times n, \mathbb{C})$ form a non-commutative ring: Indeed $(M(n \times n, \mathbb{C}), +)$ is a vector space isomorphic to $\mathbb{C}^{n^2}$, in particular it is an abelian group. The zero matrix is its identity element. It follows from the rule of matrix multiplication that the matrix multiplication is associative, and it has an identity 1 that corresponds to the matrix having ones on the diagonal. Since the multiplication is not commutative, the ring of matrices is non-commutative. Moreover it is proven in linear algebra that the distributive law holds for sum and product of matrices.

   An *unit* in $M(n \times n, \mathbb{C})$ is a matrix admitting a multiplicative inverse. In particular $GL_n(\mathbb{C})$ is, by definition, the subgroup of $M(n \times n, \mathbb{C})$ made of units.

   We will prove that the (left) *zero divisors* in $M(n \times n, \mathbb{C})$ are the nonzero matrices with determinant equal to zero. Indeed, if the determinant of M is different from zero, then there exist a matrix N such that $NM = 1$, in particular it is not possible that there exists a non zero matrix R such that $MR = 0$: in fact in that case we would have $R = (NM)R = N(MR) = N0 = 0$. On the other hand let us assume that $det(M) = 0$. Since every matrix is conjugate to an upper-triangular matrix, there exist an invertible matrix X such that $XMX^{-1} = T$ where T is a upper triangular matrix. Since the determinant is invariant under conjugation at least one of the diagonal elements of T is equal to 0, and we can assume (up to choosing X properly) that $T_{11} = 0$. Let us denote by E the elementary matrix whose unique non-zero entry is $E_{11} = 1$. An easy computation shows that $TE = 0$. Since E is not the zero matrix, also $Y = X^{-1}EX$ is not zero, moreover $MY = X^{-1}(XMX^{-1})EX = X^{-1}TEX = X^{-1}0X = 0$. This shows that every matrix M with $det(M) = 0$ is a left zero divisor. Similarly (choosing X so that XMX^{-1} is upper triangular with $T_{nn} = 0$, and considering the elementary matrix F with $F_{nn} = 1$) it is possible to show that any noninvertible matrix is also a right zero divisor.

   The same result is true for the ring of real matrice $M(n \times n, \mathbb{R})$ even if it is slightly harder to prove. Let M be a real matrix with zero determinant. By the real Jordan theorem there exist a real invertible matrix X such that XMX^{-1} has a block structure $\left[\begin{smallmatrix} A & 0 \\ 0 & B \end{smallmatrix}\right]$ where B is stricty upper triangular: the block B corresponds to the endomorphism induced by M on the generalized eigenspace for the eigenvector 0. Once this is settled we can apply the same argument as for the complex case.

2. Let us set $\alpha = \sqrt{2}$, $\beta = \sqrt{3}$, $\gamma = \alpha + \beta$.

   (a) Show that γ is an algebraic number.
   Solution Since $\gamma = \sqrt{2}+\sqrt{3}$ we have $\gamma^2 = 5+2\sqrt{6}$, in particular $(\gamma^2-5)^2 = 24$ that in turns implies $\gamma^4 - 10\gamma^2 + 1 = 0$. This shows that γ is an algebraic number.

   (b) Is $\mathbb{Q}[\alpha, \beta] = \mathbb{Q}[\gamma]$ as subrings of $\mathbb{R}$?
   Solution Since $\gamma = \alpha + \beta$, we have that $\mathbb{Q}[\gamma] \subseteq \mathbb{Q}[\alpha, \beta]$ as a subring of $\mathbb{R}$. In order to show the reverse inequality, it is enough to check that α belongs to $\mathbb{Q}[\gamma]$. It is easy to compute that $\gamma^3 = 11\sqrt{2} + 9\sqrt{3}$. In particular $\alpha = (\gamma^3 - 9\gamma)/2$ and hence belongs to $\mathbb{Q}[\gamma]$. Since $\beta = \gamma - \alpha$, β belongs to $\mathbb{Q}[\gamma]$ as well.

   (c) Is $\mathbb{Z}[\alpha, \beta] = \mathbb{Z}[\gamma]$? *Hint:* you can use the equation determined in (a) to show that every element of $\mathbb{Z}[\gamma]$ can be written as an integer combination of $1, \gamma, \gamma^2, \gamma^3$.
   Solution We will show that $\mathbb{Z}[\gamma]$ is contained properly in $\mathbb{Z}[\alpha, \beta]$ since α doesn't belong to $\mathbb{Z}[\gamma]$ (notice that in part (b) we had to divide by 2). Indeed since $\gamma^4 = 10\gamma^2 - 1$, any element in $\mathbb{Z}[\gamma]$ can be written as $a+b\gamma+c\gamma^2+d\gamma^3$ for some integer numbers a, b, c, d. In particular, since $\gamma = \sqrt{2}+\sqrt{3}$, $\gamma^2 = 5+2\sqrt{6}$, and $\gamma^3 = 11\sqrt{2} + 9\sqrt{3}$ we get that every element in $\mathbb{Z}[\gamma]$ can be written as $(a + 5c) + (b + 11d)\sqrt{2} + (b + 9d)\sqrt{3} + 2c\sqrt{6}$. Let us now assume by contradiction that $\sqrt{2}$ has this form, since $\sqrt{2}, \sqrt{3}, \sqrt{6}$ are irrational and all their ratios are irrational, an integer combination can be zero if and only if all the coefficients are zero, but this is not possible since we would get that $b+9d = 0$ and $b + 11d = 1$.

3. (a) Let R be a finite ring. Show that every $x \in R$ is either 0, a zero divisor, or invertible.
   Solution Let us fix a finite ring R and an element $x \in R$ and consider the function

$$\begin{array}{rccc} f_x: & R & \to & R \\ & r & \mapsto & xr. \end{array}$$

   Let us first assume that f_x is not injective, then there are two different elements a, b with $xa = xb$. Using the distributive law we get that $x(a - b) = 0$, in particular, since $a - b$ is different from zero by assumption on a, b, we get that x is a zero divisor.

   We are left to deal with the case in which f_x is an injective function, since R is finite, this implies that f_x must be surjective. Hence 1 is in the image of the function, in particular there exists an element $y \in R$ such that $xy = 1$, hence x is invertible.

   (b) Give an example of a ring R that contains an element that is not a zero divisor and is not invertible.

Solution Let us consider the ring $\mathbb{Z}$ of integer numbers. Since $\mathbb{Z}$ is a domain of integrity, there are no zero divisors, but no element, apart from 1 and -1 admit a multiplicative inverse.

(c) Give an example of an infinite ring that is not an integral domain.
Solution The diagonal matrices with real coefficients are a commutative subring of $M(n \times n, \mathbb{R})$ that contain zero divisors (all the non invertible diagonal matrices).

4. Let R_1 and R_2 be rings, show that $R_1 \times R_2$ is a ring. Show that if $R_1 \times R_2$ is an integral domain, then at least one of the two rings R_1, R_2 is the zero ring.
Solution The set $R_1 \times R_2$ with operations $(a, b) + (c, d) = (a + b, c + d)$ and $(a, b) \times (c, d) = (a \times c, b \times d)$ is a ring since R_1 and R_2 are: indeed the product of two abelian groups is an abelian group (with zero the pair $(0, 0)$), the multiplication on $R_1 \times R_2$ is associative since it is associative the multiplication on each factor, the identity of the multiplication is the pair $(1, 1)$. The distributive law holds since it holds on each factor.

Let us now assume that $R_1 \times R_2$ is an integral domain, and let us consider the product $(1, 0) \times (0, 1) = (1 \times 0, 0 \times 1) = (0, 0)$. Since by assumption $R_1 \times R_2$ is an integral domain, at least one between $(1, 0)$ and $(0, 1)$ must be the zero element $(0, 0)$. This implies that at least one of the two rings R_1, R_2 is the zero ring.

5. For the following (commutative) rings determine the zero divisors and the units, say if they are integral domains:

(a) $\mathbb{Z}/m\mathbb{Z}$ with the product induced by the product of $\mathbb{Z}$.
Solution Let us assume that the prime decomposition of m is $p_1 \dots p_k$. Let us assume that a number n that is not a multiple of m, is not coprime with m. This means that at least one prime factor of m, p_i appears in the prime decomposition of n. Since n is not a multiple of m its class in $\mathbb{Z}/m\mathbb{Z}$ is not zero. Moreover the product $p = p_1 \dots \hat{p}_i \dots p_k$ is not a multiple of m, in particular its class in $\mathbb{Z}/m\mathbb{Z}$ is non zero. Moreover pn is a multiple of m. This shows that the class of n is a zero divisor in $\mathbb{Z}/m\mathbb{Z}$.

Viceversa if n is coprime with m, the Chinese Remainder theorem implies that there are integers a, b with $1 = am + bn$. This implies that $\overline{n}$ is invertible in $\mathbb{Z}/m\mathbb{Z}$ with inverse $\overline{b}$.

In particular if m is prime every nonzero element in $\mathbb{Z}/m\mathbb{Z}$ is invertible. In this case $\mathbb{Z}/m\mathbb{Z}$ is a field.

(b) the set $F = C([0, 1], \mathbb{R})$ of continuous functions of the interval $[0, 1]$ with pointwise addition and multiplication.
Solution The functions that do not attain the value zero are precisely the units in the ring $F = C([0, 1], \mathbb{R})$: indeed if $f(x)$ is different from zero for every x, we can define the function g by setting $g(x) = 1/f(x)$, and we get

that $(f \times g)(x) = f(x)/f(x) = 1$ and the constant function 1 is the unit of F. Viceversa if f is invertible with inverse x, then, for every $x \in [0,1]$, we have $1 = f(x)g(x)$ hence in particular $f(x)$ is different from 0.

For every proper open sub-interval I of $[0,1]$ there exists a continuous function g_I that is identically zero outside I and has a positive value in I. Moreover given a continuous function f on $[0,1]$ we denote by Z_f the closed subset of $[0,1]$ defined by $Z_f = \{x \in [0,1] | f(x) = 0\}$.

We claim that the set of zero divisors of F consists of those functions f such that Z_f contains an open interval K. Indeed those functions are zero divisors: $f \times g_K$ is identically zero. Viceversa let f be a zero divisor. By definition there exist a continuous function h that is not identically zero and with $f(x)h(x) = 0$ for every $x \in [0,1]$. Let y be a point with $h(y)$ different from 0. Since h is continuous there exists an open interval I containing y such that $h(t) \neq 0$ for every t in I. Since $f(x)h(x) = 0$, the interval I must be contained in Z_f, and this concludes the proof.

In particular in the ring $C([0,1], \mathbb{R})$ there are elements that are not invertible and not zero divisors: for example the function $f(x) = x - 1/2$.

(c) The subring R of $M(2 \times 2, \mathbb{R})$ consisting of matrices of the form $\begin{bmatrix} a & b \\ 0 & a \end{bmatrix}$, with a, b in $\mathbb{R}$.

Solution Let R be the subring of $M(2 \times 2, \mathbb{R})$ consisting of matrices of the form $\begin{bmatrix} a & b \\ 0 & a \end{bmatrix}$, with a, b in $\mathbb{R}$. We claim that an element is invertible if and only if a is different from zero, and is a zero divisor if a is equal to zero and b is different from 0.

Indeed if a is different from zero, the matrix $M^{-1} = \begin{bmatrix} a^{-1} & -a^{-2}b \\ 0 & a^{-1} \end{bmatrix}$ is a multiplicative inverse of the matrix $M = \begin{bmatrix} a & b \\ 0 & a \end{bmatrix}$. In particular M is invertible.

Viceversa if $a = 0$ we have that $M = \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix}$ is a zero divisor since M is different from 0 but $M^2 = MM = 0$.

6. Let R be a (commutative) ring, and let us consider the polynomial ring $R[x]$.

(a) Show that if R is an integral domain then the same is true for $R[x]$.

Solution Recall that the degree $deg(f)$ of an element f of $R[x]$ is defined to be the biggest n such that the coefficient of x^n in f is different from zero. We will first show the following

Lemma: Let R be an integral domain, then $deg(fg) = deg(f) + deg(g)$ in $R[x]$.

Proof Infact let $f = \sum_{i=0}^{deg(f)} f_i x^i$ and let $g = \sum_{i=0}^{deg(g)} g_i x^i$. Then the biggest n such that the coefficient of x^n in fg is different from zero is smaller or

equal to $deg(f) + deg(g)$, moreover the coefficient of $x^{deg(f)+deg(g)}$ is equal, by the multiplication rule in a polynomial ring, to $c = f_{deg(f)}g_{deg(g)}$. Since by assumption $f_{deg(f)}$ and $g_{deg(g)}$ are non zero, and R is an integral domain, then also c is nonzero, and this implies that $deg(fg) = deg(f) + deg(g)$.

By the lemma if R is an integral domain, for every $f, g \in R[x]$ different from 0 the degree of fg is bigger or equal than the degree of f. Let us now chose two elements f, g such that $fg = 0$. The degree of f and g must be zero, hence both f and g must belong to R. Since R is a domain of integrity then $fg = 0$ implies that either f or g is zero, hence there are no zero divisor in $R[x]$. Let f be a unit of $R[x]$. By definition there exists g in $R[x]$ with $fg = 1$. Since the degree is monotone because R is a domain of integrity, we get that $deg(f) = deg(g) = 0$, hence f and g belong to R and are units of R.

(b) Prove that if R is an integral domain, then the set of units of $R[x]$ coincides with the set of units of R.
Solution Let f be a unit of $R[x]$. By definition there exists g in $R[x]$ with $fg = 1$. Since the degree is monotone because R is a domain of integrity, we get that $deg(f) = deg(g) = 0$, hence f and g belong to R and are units of R.

(c) Show that $1 + 5X$ is invertible in $\mathbb{Z}/25\mathbb{Z}[x]$.
Solution Indeed $(1 + \overline{5}X)(1 - \overline{5}X) = 1 + \overline{25}X = 1$. In particular $1 + \overline{5}X$ is invertible in $\mathbb{Z}/25\mathbb{Z}[x]$.

7. For which positive n does $x^2 + x + 1$ divide $x^4 + 3x^3 + x^2 + 7x + 5$ in $\mathbb{Z}/n\mathbb{Z}[x]$?
Solution The algorithm for division of polynomials in $\mathbb{Z}[x]$ gives

$$x^4 + 3x^3 + x^2 + 7x + 5 = (x^2 + x + 1)(x^2 + 2x - 2) + 7x + 7$$

in particular we get, in $\mathbb{Z}/n\mathbb{Z}$, that $x^2 + x + 1$ divides $x^4 + 3x^3 + x^2 + 7x + 5$ if and only if the remainder $7x + 7$ is zero in $\mathbb{Z}/n\mathbb{Z}$, and this last statement is true if and only if $n = 7$.