Introduction to Algebra

Shu Sasaki

21st March 2024

5 Polynomials

5.1 Defining polynomials

Definition. Let R be a ring. A polynomial f in one variable X with coefficients in R is:

$$f = c_nX^n + c_{n-1}X^{n-1} + \cdots + c_1X + c$$

where $c_n, c_{n-1}, \ldots, c_1, c$ are elements of R which are often referred to as the coefficients of f.

The set of all polynomials in one variable X with coefficients in R will be denoted by $R[X]$.

Definition. The degree, denoted deg(f), of a non-zero polynomial f (in one variable X) is the largest integer n for which its coefficient 'c_n' of X^n is non-zero.

Definition. A non-zero polynomial $f = c_nX^n + c_{n-1}X^{n-1} + \cdots + c_1X + c$ of degree n is called monic if the leading coefficient $c_n = 1$. The zero polynomial is defined to be monic.

5.2 Polynomial rings

Theorem 25. If R is a ring, then so is $R[X]$ in terms of addition

$$(f+g)(X) = f(X) + g(X) = \sum_n (c_n(f) + c_n(g))X^n$$

and multiplication

$$(fg)(X) = f(X)g(X) = \sum_n \left(\sum_r c_r(f)c_{n-r}(g) \right) X^n.$$

If R is a ring with identity, then so is $R[X]$. If R is commutative, then so is $R[X]$.

Proof.

- (R+0) Since $c_n(f)$ and $c_n(g)$ are both elements of R, it follows from (R+0) for $(R, +, \times)$ that $c_n(f) + c_n(g)$ is an element of R. Therefore $\sum_n (c_n(f) + c_n(g))X^n \in R[X]$.

- (R+1) Since $c_n(f) + (c_n(g) + c_n(\gamma)) = (c_n(f) + c_n(g)) + c_n(\gamma)$ by (R+1) for $(R, +, \times)$,

$$\sum_n c_n(f)X^n + \sum_n (c_n(g) + c_n(\gamma))X^n = \sum_n (c_n(f) + (c_n(g) + c_n(\gamma)))X^n$$

equals

$$\sum_n ((c_n(f) + c_n(g)) + c_n(\gamma))X^n = \sum_n (c_n(f) + c_n(g))X^n + \sum_n c_n(\gamma)X^n.$$

- (R+2) $0 = \sum_n 0X^n = \cdots 0X^n + \cdots + 0X + 0$ is the identity. For every n,

$$c_n(f) + 0 = 0 + c_n(f) = c_n(f)$$

holds by (R+2) for $(R, +, \times)$. Therefore $\sum_n c_n(f)X^n + 0 = 0 + \sum_n c_n(f)X^n = \sum_n c_n(f)X^n$.

- (R+3) If $f = \sum_n c_n(f)X^n$, the inverse is $\sum_n(-c_n(f))X^n$. This is because for every $n \geqslant 0$

$$c_n(f) + (-c_n(f)) = (-c_n(f)) + c_n(f) = 0$$

holds by (R+3) for $(R, +, \times)$.

- (R+4) By (R+4) for $(R, +, \times)$, we have $c_n(f) + c_n(g) = c_n(g) + c_n(f)$ and therefore

$$\sum_n c_n(f)X^n + \sum_n c_n(g)X^n = \sum_n (c_n(f) + c_n(g))X^n$$

equals

$$\sum_n (c_n(g) + c_n(f))X^n = \sum_n c_n(g)X^n + \sum_n c_n(f)X^n.$$

- (R×0) Fix n. It follows from (R×0) for $(R, +, \times)$ that $c_r(f)c_{n-r}(g) \in R$ for every $0 \leqslant r \leqslant n$. By (R+0) for $(R, +, \times)$, we may then deduce that the coefficient $c_n(fg) = \sum_r c_r(f)c_{n-r}(g)$ of X^n lies in R and therefore that $\sum_n(\sum_r c_r(f)c_{n-r}(g))X^n \in R[X]$.

- (R×1) To prove $f(g\gamma) = (fg)\gamma$, it suffices to compare the coefficients of X^n. The coefficient of X^n on the LHS is

$$\sum_r c_r(f)c_{n-r}(g\gamma) = \sum_r c_r(f)\left(\sum_s c_s(g)c_{(n-r)-s}(\gamma)\right) = \sum c_p(f)c_q(g)c_r(\gamma)$$

where the rightmost sum ranges over the set of all non-negative integers p, q and r satisfying $p + q + r = n$, while the coefficient on the RHS is

$$\sum_r c_r(fg)c_{n-r}(\gamma) = \sum_r \left(\sum_s c_s(f)c_{r-s}(g)\right) c_{n-r}(\gamma) = \sum c_p(f)c_q(g)c_r(\gamma).$$

- (R×+) To prove $f(g + \gamma) = fg + f\gamma$, it suffices to compare the coefficient of X^n. The coefficient on the LHS is

$$\sum_r c_r(f)c_{n-r}(g + \gamma) = \sum_r c_r(f)\left(c_{n-r}(g) + c_{n-r}(\gamma)\right)$$

which is equal, by (R+×) for $(R, +, \times)$, to

$$\sum_r c_r(f)c_{n-r}(g) + c_r(f)c_{n-r}(\gamma) = \left(\sum_r c_r(f)c_{n-r}(g)\right) + \left(\sum_r c_r(f)c_{n-r}(\gamma)\right) = c_n(fg) + c_n(f\gamma).$$

- (R+×) A proof of $(g + \gamma)f = gf + \gamma f$ is similar to (R×+) and is left as an exercise. We make appeal to (R+×) for $(R, +, \times)$ instead.

• $R[X]$ is commutative when R is. If $(R, +, \times)$ is commutative, $c_r(f)c_{n-r}(g) = c_{n-r}(g)c_r(f)$ and therefore

$$c_n(fg) = \sum_r c_r(f)c_{n-r}(g) = \sum_r c_{n-r}(g)c_r(f) = \sum_s c_s(g)c_{n-s}(f) = c_n(gf).$$

• $R[X]$ has a multiplicative unit if R does. Let 1 be the multiplicative unit R has and, by slight abuse of notation, let 1 again denote the polynomial $1 = \cdots + 0X^n + \cdots + 0X + 1$ of degree 0 with constant term 1, i.e. the polynomial 1 with $c_n(1) = 0$ for every $n \geqslant 1$ and $c(1) = 1$. To establish $f \times 1 = 1 \times f = 1$, we compare the coefficients of X^n for every $n \geqslant 0$. For $n \geqslant 1$, we have

$$c_n(f \times 1) = \sum_r c_r(f)c_{n-r}(1) = 0 + \cdots + 0 + c_n(f)c(1) = c_n(f) \times 1 = c_n(f)$$

by Proposition 16, (R+2) for $(R, +, \times)$ and the fact that 1 is the multiplicative identity. Similarly,

$$c_n(1 \times f) = \sum_r c_r(1)c_{n-r}(f) = c(1)c_n(f) + 0 + \cdots + 0 = c_n(f).$$

For $n = 0$, we have

$$c(f)c(1) = c(f) \times 1 = c(f)$$

and

$$c(1)c(f) = 1 \times c(f) = c(f).$$

□

Proposition 26. If $(R, +, \times)$ is a ring with identity 1, then $R[X]$ is not a division ring.

Proof. Suppose, firstly, that R consists only of one element– the element is necessarily the additive identity 0 of R. It then follows that $R[X] = \{0\}$, as f with $c_n(f) = 0$ for every n is necessarily the 'polynomial' 0. However, this forces $R[X]$ not to be a division ring as the condition $1 \neq 0$ does not hold.

Having dealt with the case that R consists of one element, we may assume now that $R \neq \{0\}$. In this case, there exists a non-zero element c in R. Consider the polynomial cX of degree 1. It suffices to prove that cX does not have multiplicative inverse (if $R[X]$ were a division ring, then any element would have multiplicative inverse). If cX had a multiplicative inverse, then there should be a polynomial $f = c_n(f)X^n + \cdots + c_1(f)X + c(f)$ such that $f \times cX = 1$. However,

$$f \times cX = (cc_n(f))X^n + \cdots + (cc_1(f))X^2 + (cc(f))X$$

and comparing the constant terms, we deduce that $1 = 0$. However, this would have implied that $R = \{0\}$ which we know should not occur. □

Remark. By definition, $\deg(f)\deg(g) \geqslant \deg(fg)$. Let $f = \sum_n c_n(f)X^n$ and $g = \sum_n c_n(g)X^n$. By definition, $c_n(f) =$ for every $n \geqslant \deg(f)$ while $c_n(f)$ is non-zero when $n = \deg(f)$. Similarly for g. Since

$$fg = \sum_n \left(\sum_r c_r(f)c_{n-r}(g) \right) X^n = c(f)c(g) + (c(f)c_1(g) + c_1(f)c(g))\, X + \cdots + c_{\deg(f)}c_{\deg(g)}X^{\deg(f)+\deg(g)},$$

we see that $\deg(fg) \leqslant \deg(f) + \deg(g)$ where the equality holds exactly when $c_{\deg(f)}c_{\deg(g)}$ is non-zero. For example, if $R = \mathbb{Z}_6$ and $c_{\deg(f)} = [2]$ and $c_{\deg(g)} = [3]$, then $c_{\deg(f)}c_{\deg(g)} = [2][3] = [6] = [0]$ and therefore $\deg(fg) < \deg(f) + \deg(g)$.

Remark (non-examinable). If R is a ring with the property– if any pair of elements a and b of R are non-zero, then their product ab is again non-zero– then $\deg(fg) = \deg(f) + \deg(g)$ always holds. A commutative ring with this property is called an *integral domain*. One of the most important example of an integral domain is $\mathbb{Z}$. Another important example is a field. And it is for this reason, we shall specialised the coefficient ring to be a field from now on.

Proposition 27. Let $(F, +, \times)$ be a field. The units $F[X]^\times$ of $F[X]$ are $F^\times = F - \{0\}$.

Proof. Let f be a unit in $F[X]$. Then there exists a polynomial g in $F[X]$ such that $fg = gf = 1$. By the remark above, $\deg(f) + \deg(g) = \deg(fg) = \deg(1) = 0$. Therefore $\deg(f) = \deg(g) = 0$, i.e. f and g are non-zero constants in F whose product is 1, in other words, f and g are units in F. □

Remark (non-examinable) The assertion of Proposition 27 holds with an integral domain in place of F. If R is (merely) a commutative ring with identity, then the units are the group of polynomials f with the property that $c(f) \in R^\times$ and $c_n(f)$ is nilpotent (i.e. its sufficiently large power is 0) for every $n \geqslant 1$. See for example https://kconrad.math.uconn.edu/blurbs/ringtheory/polynomial-properties.pdf for a proof (and much more).

5.3 Polynomial division

Theorem 28 (Division algorithm in the context of the polynomial ring $F[X]$). Let F be a field. Let f and g be two polynomials in $F[X]$ and assume, in particular, that g is non-zero. Then there exists polynomials q and r in $F[X]$ such that

$$f = gq + r$$

where either $r = 0$ or $\deg(r) < \deg(g)$.

Proof. We prove the theorem by induction on the degree of f.

- Suppose $\deg(f) < \deg(f)$. Then

$$f = g \cdot 0 + f$$

(i.e. $q = 0$ and $r = f$) holds.

- Suppose, for any polynomial f' of degree $< \deg(f)$, the assertion of the theorem holds (with the same g!), i.e., there exists q' and r' in $F[X]$ such that

$$f' = gq' + r'$$

where r' is either 0 or $\deg(r') < \deg(g)$. The goal is to show for f (of degree $\deg(f)$!) there are q and r as above. By the case already dealt with above, we may assume

$$\deg(f) \geqslant \deg(g)$$

and let

$$f' = f'(X) = f(X) - \frac{c_{\deg(f)}(f)}{c_{\deg(g)}(g)} X^{\deg(f)-\deg(g)} g(X).$$

Then $c_n(f') = 0$ for every $n > \deg(f)$ and

$$c_{\deg(f)}(f') = c_{\deg(f)}(f) - \frac{c_{\deg(f)}(f)}{c_{\deg(g)}(g)} c_{\deg(g)}(g) = 0.$$

Therefore $\deg(f') < \deg(f)$. By the inductive hypothesis, there exists q' and r' in $F[X]$ such that

$$f' = q'g + r'$$

where $r' = 0$ or $\deg(r') < \deg(g)$. It therefore follows from the definition of f' that

$$f = \left(q' + \frac{c_{\deg(f)}(f)}{c_{\deg(g)}(g)} X^{\deg(f)-\deg(g)}\right) g + r'$$

as desired. □

5.4 Roots and factors

Definition. Let f and g be polynomials in $F[X]$. We say that g divides f, or g is a factor of f, if there exists a polynomial q in $F[X]$ such that $f = gq$.

Remark. One needs to be careful when it come to polynomial division. Suppose g divides f. Then, for every unit γ in $F[X]$, the product $g\gamma$ also divides f! By Proposition 27, we know that $F[X]^\times = F - \{0\}$, hence this assertions amounts to saying that if g divides f, then any non-zero constant multiple of g also divides f.

The divisibility of a polynomial depends on F:

Examples.

$X + \sqrt{-1}$ divides $X^2 + 1$ in $\mathbb{C}[X]$. Indeed, $(X+\sqrt{-1})(X-\sqrt{-1}) = X^2 - (\sqrt{-1})^2 = X^2 + 1$.

On the other hand, no non-trivial polynomial in $\mathbb{Q}[X]$ divides $f(X) = X^2 + 1$ in $\mathbb{Q}[X]$! Firstly, any degree 0 polynomial in $\mathbb{Q}[X]$ divides $f(X)$ because a polynomial in $\mathbb{Q}$ of degree 0 is nothing other than an element c of $\mathbb{Q} - \{0\}$, hence $f = c(c^{-1}f)$. Similarly, the only degree 2 polynomial of degree 2 that divides f is f itself. Indeed, if g of degree 2 divides f, then there exists γ in $\mathbb{Q}[X]$ such that $g\gamma = f$. Since $\deg(g) + \deg(\gamma) = \deg(f)$, then $\deg(\gamma) = 0$, i.e. γ is an element of $\mathbb{Q} - \{0\}$. Therefore, g is forced to be $\gamma^{-1}f$. To see that no polynomial of degree 1 in $\mathbb{Q}[X]$ divides f, it suffices to establish that $X^2 + 1$ does not factorises as the product $(X + a)(X + b)$ of degree one polynomials, i.e. there are no rational numbers a and b such that $a + b = 0$ and $ab = 1$ (by comparing the coefficients). Suppose for contradiction that it does. It then follows from $a + b = 0$ that $b = -a$ and substituting this into $ab = 1$, we get $-a^2 = 1$. Since $-a^2 \leqslant 0$, this is a contradiction.

Corollary 29. Let F be a field. Let f in $F[X]$ and α be an element of F. Then there exists q in $F[X]$ and r in F such that

$$f = (X - \alpha)q + r.$$

Proof. This follows from the theorem with $g = X - \alpha$. □

Corollary 30. Let f in $F[X]$ and α in F. The remainder of f when divided by $(X - \alpha)$ is $f(\alpha)$. In particular, $f(\alpha) = 0$ if and only if $X - \alpha$ is a factor of $f(X)$ in $F[X]$.

Proof. It follows from the corollary (by letting $X = \alpha$) that $f(\alpha) = r$. If $f(\alpha) = 0$, it therefore follows from the corollary that $f = (X - \alpha)q$ and $X - \alpha$ is a factor of f. Conversely, if $X - \alpha$ is a factor of f, there exists q in $F[X]$ such that $f = (X - \alpha)q$. Letting $X = \alpha$, we deduce that $f(\alpha) = 0$. □

We may use the corollary to check if a given polynomial factorises or not factorises at all.

Example. Consider $f(X) = X^2 + 3$ in $\mathbb{F}_7[X]$. Then $X - 2$ divides $X^2 + 3$, Indeed,

$$[2]^2 + [3] = [4] + [3] = [7] = [0],$$

i.e. $f([2]) = [0]$. In fact, $X + 2$ also divides f as

$$[-2]^2 + [3] = [4] + [3] = [7] = [0],$$

i.e. $f([-2]) = f(-[2]) = [0]$.

Example. The polynomial $f(X) = X^2 + 2$ is irreducible in $\mathbb{F}_5[X]$, i.e. no non-trivial polynomial in $\mathbb{F}_5[X]$ divides f. To see this, we observe that no polynomial of the form $X - \alpha$ divides f in $\mathbb{F}_5[X]$. By Corollary 30, this is equivalent to checking that no α in $\mathbb{F}_5$ satisfy $f(\alpha) = 0$. Indeed,

α	[0]	[1]	[2]	[3]	[4]
$f(\alpha)$	[2]	[3]	[1]	[1]	[3]

Definition. Let N be a non-negative integer. An element α in F is a root of multiplicity N of a polynomial f in $F[X]$, if $(X - \alpha)^N$ is the highest power of $(X - \alpha)$ that divides $f(X)$.

5.5 The fundamental theorem of algebra

Definition. Let F be a field. We say that α is a root, or zero, of the polynomial $f(X) = c_n X^n + \cdots + c_1 X + c$ in $F[X]$ if $f(\alpha) = 0$, i.e. $c_n \alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_1 X + c = 0$.

Theorem 31.(The Fundamental Theorem of Algebra) Let $n \geq 1$. Let $c, c_1, \ldots, c_n$ be complex numbers, where c_n is assumed to be non-zero. Then the polynomial $c_n X^n + \cdots + c$ has at least one root inside $\mathbb{C}$.

Theorem 32.(The Fundamental Theorem of Algebra with multiplicities) Let $n \geq 1$. Let $c, c_1, \ldots, c_n$ be complex numbers, where c_n is assumed to be non-zero. Then the polynomial $f(X) = c_n X^n +$

$\cdots + c$ has exactly n roots in $\mathbb{C}$ counted with multiplicities, i.e. there exist complex numbers $\alpha_1, \ldots, \alpha_n$ such that

$$f(X) = c_n(X - \alpha_n)(X - \alpha_{n-1}) \cdots (X - \alpha_1).$$

These theorems are proved, for example, by complex analysis! Needless to say, proofs are non-examinable (and I won't even try to spell them out either!). Look at H. A. Priestley's 'Introduction to Complex Analysis', Oxford University Press.

5.6 GCDs of polynomials

Theorem 33.

- Any two polynomials f and g have a greatest common divisor in $F[X]$.
- The gcd of two polynomials in $F[X]$ can be found by Euclid's algorithm.
- If $\gcd(f, g) = \gamma$ (a polynomial in $F[X]$), then there exist p, q in $F[X]$ such that

  $$fp + gq = \gamma;$$

  these polynomials p and q can also be found from the extended Euclid's algorithm.

Proof. Non-examinable. Similar to the proof in the setting of $\mathbb{Z}$ though. □

Examples.
- Let $f = X^4 + 1$ and $g = X^2 + X$ in $\mathbb{Q}[X]$. What is $\gcd(f, g)$? Since

$$\begin{array}{rcl} X^4+1 & = & (X^2 - X + 1)(X^2 + X) + (-X + 1) \\ X^2 + X & = & (-X - 2)(-X + 1) + 2 \\ -X + 1 & = & \frac{1}{2}(-X + 1) \cdot 2 + 0, \end{array}$$

the gcd is 1 (not 2!) since gcd is defined to be monic. Note that if 2 is a common divisor, any $F^\times$-multiple of 2 is also a common divisor. Because gcd is defined to be monic, we are forced to choose 1, instead of 2.

To find p, q such that $fp + gq = \gcd(f, g) = 1$, we do something analogous to what we saw in Euclid's algorithm for $\mathbb{Z}$. Indeed, since

$$\begin{array}{rcl} 2 & = & (X^2 + X) - (-X - 2)(-X + 1) \\ & = & (X^2 + X) + (X + 2)((X^4 + 1) - (X^2 - X + 1)(X^2 + X)) \\ & = & (X + 2)(X^4 + 1) + (-X^3 - X^2 + X - 1)(X^2 + X) \end{array}$$

we have

$$\gcd(f, g) = 1 = \frac{1}{2}(X + 2)f + \frac{1}{2}(-X^3 - X^2 + X - 1)g.$$

- Let $f = X^4 + 2X^3 + X^2 - 4$ and $g = X^3 - 1$ in $\mathbb{Q}[X]$. What is gcd?

$$\begin{array}{rcl} X^4+2X^3+X^2-4 &=& (X+2)(X^3-1)+(X^2+X-2) \\ X^3-1 &=& (X-1)(X^2+X-2)+(3X-3) \\ X^2+X-2 &=& \frac{1}{3}(X+2)(3X-3)+0 \end{array}$$

and therefore $\gcd(f,g) = X-3$. As before, as soon as $3X-3$ is a common divisor of f and g in $\mathbb{Q}[X]$, we know that any $F^{\times}$-multiple of $3X-3$ is also a common divisor. Amongst those, the only one is monic and that is $X-1$ which is the gcd.

To find p and q such that $fp+gq = \gcd(f,g)$, we see that

$$\begin{array}{rcl} 3X-3 &=& (X^3-1)-(X-1)(X^2+X-2) \\ &=& g-(X-1)(f-(X+2)g) \\ &=& (-X+1)f+(X^2-X-1)g. \end{array}$$

- Let $f = X^4+[1]$ and $g = X^2+X$ in $\mathbb{F}_2[X]$. What is gcd in $\mathbb{F}_2[X]$?

Since $X^4+[1] = (X+[1])^4$ in $\mathbb{F}_2[X]$, we work with $(X+[1])^4$ instead. Since $g(X) = X(X+[1])$, both $f = (X+[1])^4$ and $g = X(X+[1])$ are divisible by $X+[1]$ exactly once. Since

$$\gcd(\frac{f}{X+[1]}, \frac{g}{X+[1]}) = \gcd((X+[1])^3, X) = 1,$$

the gcd is $X+[1]$. Alternatively, we may follow 'Euclid's algorithm':

$$\begin{array}{rcl} (X+[1])^4 &=& ((X+[1])^2+(X+[1])+[1])(X^2+X)+(X+[1]) \\ X^2+X &=& X(X+[1])+0. \end{array}$$

and conclude that $\gcd(f,g) = X+[1]$ in $\mathbb{F}_2[X]$. To find p,q, we simply see that

$$\gcd(f,g) = X+[1] = 1\cdot(X+[1])^4-((X+[1])^2+(X+[1])+[1])(X^2+X) = 1\cdot f+(X^2+X+1)g.$$

5.7 Power series rings (non-examinable)

Definition. Let R be a ring. A power series f in one variable X with coefficients in R is:

$$f = c+c_1X+\cdots+c_nX^N+\cdots = \sum_n c_nX^n$$

where c_n, for every n, is an element of R.

The set of all power series in one variable X with coefficients in R will be denoted by $R[[X]]$. This is a ring with addition and multiplication defined similarly to the one for $R[X]$.

What is the difference between $R[X]$ and $R[[X]]$? For example, $1-X$ is not a unit in $R[X]$ and it is a unit in $R[[X]]$ as

$$(1-X)(1+X+X^2+\cdots) = 1.$$

6 Matrices

Let $(R, +, \times)$ be a ring and let $\mathrm{M}_2(R)$ be the set of 'matrices'

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

where a, b, c, d are elements of R, together with addition

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a + a' & b + b' \\ c + c' & d + d' \end{pmatrix}$$

and multiplication

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + db' \end{pmatrix}.$$

Theorem 34. $\mathrm{M}_2(R)$ is a ring. If R is a ring with identity, then so is $\mathrm{M}_2(R)$.

Proof. Exercise. □

Remark. The additive identity, the identity element with respect to $+$ defined above, is $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, where each entry 0 is the additive identity in R as defined in (R+2). If R is a ring with identity 1, then $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the identity. Indeed,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a \times 1 + b \times 0 & a \times 0 + b \times 1 \\ c \times 1 + d \times 0 & c \times 0 + d \times 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

The $(1, 1)$-entry is a because $a \times 1 = a$ (since 1 *is* the element of R satisfying $a \times 1 = 1 \times a = a$) and $b \times 0$ (by Proposition 16), therefore $a \times 1 + b \times 0 = a + 0 = a$ by (R+2) for $(R, +, \times)$.

Remark. In contrast to Theorem 25, $\mathrm{M}_2(R)$ is never commutative, even if R is commutative. Let us see this in an example. Let $A = \begin{pmatrix} [1] & [1] \\ [0] & [1] \end{pmatrix}$ and $B = \begin{pmatrix} [1] & [1] \\ [1] & [1] \end{pmatrix}$ be matrices in $\mathrm{M}_2(\mathbb{F}_2)$, where $\mathbb{F}_2$ is the field with two elements $[0]$ and $[1]$. Following the formula above, together with $[1] + [1] = [2] = [0]$, we see that

$$AB = \begin{pmatrix} [0] & [0] \\ [1] & [1] \end{pmatrix}$$

while

$$BA = \begin{pmatrix} [1] & [0] \\ [1] & [0] \end{pmatrix}.$$

Proposition 35 If $(R, +, \times)$ is a ring with identity but is not a ring with the property that for every elements a, b in R, the product is always $ab = 0$, then $\mathrm{M}_2(R)$ is neither commutative nor a division ring.

Remarks. An example of those rings *excluded* is the ring $(G, *, \times)$ given by a group $(G, *)$ with multiplication $a \times b = e$ for all a, b in G. A field is an example of those rings considered in the proposition.

Proof. The assumption amounts to the existence of elements a, b in $\boldsymbol{R}$ such that ab is not 0 (the additive identity). By Proposition 16, neither a nor b is 0. We use these two elements to prove the assertions of the proposition.

Following the definition of multiplication in matrices, we see that

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & ab \\ 0 & 0 \end{pmatrix}$$

and

$$\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

and therefore the ring is not commutative.

To show that $M_2(\boldsymbol{R})$ is not a division ring, we show that $\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}$ does not have a multiplicative inverse, i.e. there is no matrix A in $M_2(\boldsymbol{R})$ that satisfies the relation $A \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Suppose, for contradiction, that such a matrix A exists. In which case, since $M_2(\boldsymbol{R})$ is a ring (Theorem 34), it follows from (R×1) that

$$A \left[\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \right] = \left[A \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \right] \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$$

holds. However, the LHS equals

$$A \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

while the RHS equals

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}.$$

Since a is not 0, this is a contradiction. Therefore $M_2(\boldsymbol{R})$ is not a division ring.□