ALGEBRA

SECOND EDITION (2011)

Artin

PARTIAL SCRUTINY,

SOLUTIONS OF SOME EXERCISES,

COMMENTS, SUGGESTIONS AND ERRATA

José Renato Ramos Barbosa

2017

Departamento de Matemática

Universidade Federal do Paraná

Curitiba - Paraná - Brasil

jrrb@ufpr.br

==

==

1

==

==

Comments

==

==

p. **27**, paragraph right before the last sentence of **1.5**, "Every permutation ..."

A permutation p can be written as a product of cycles. A cycle $(\imath_1\ \imath_2\ \imath_3\ \ldots\ \imath_m)$ can be written as a product

$$(\imath_1\ \imath_m)\ldots(\imath_1\ \imath_3)\,(\imath_1\ \imath_2)$$

of transpositions.[1] Now, once we write p as a product of cycles, let $\mathcal{N}(p)$ denote the number of distinct cycles of p, possibly including 1-cycles,[2] and consider a transposition $\tau = (\imath\ \jmath)$. Then

$$\mathcal{N}(\tau p) = \begin{cases} \mathcal{N}(p)+1 & \text{if } \imath \text{ and } \jmath \text{ belong to the same cycle of } p; \\ \mathcal{N}(p)-1 & \text{otherwise.} \end{cases}$$

(In fact, in the first case,

$$\tau\,(\imath\ \imath_1\ \ldots\ \imath_r\ \jmath\ \jmath_1\ \ldots\ \jmath_s) = (\imath\ \imath_1\ \ldots\ \imath_r)\,(\jmath\ \jmath_1\ \ldots\ \jmath_s)$$

increases the number of disjoint cycles by 1, whereas

$$\tau\,(\imath\ \imath_1\ \ldots\ \imath_r)\,(\jmath\ \jmath_1\ \ldots\ \jmath_s) = (\imath\ \imath_1\ \ldots\ \imath_r\ \jmath\ \jmath_1\ \ldots\ \jmath_s)$$

decreases the number of disjoint cycles by 1 in the second case.) So, if τ_i is a transposition, $i = 1, \ldots, k$,

$$\mathcal{N}\left(\tau_1 \cdots \tau_k p\right) \equiv \mathcal{N}(p) + k \mod 2$$

(by induction on k). Finally, in considering permutations of S_n, suppose that p can be written as a product of transpositions in two different ways, say

$$\begin{aligned} p &= \tau_1 \cdots \tau_k \\ &= \theta_1 \cdots \theta_\ell, \end{aligned}$$

and let

$$\begin{aligned} p_0 &= 1 \\ &= (\mathbf{1}) \cdots (\mathbf{n}). \end{aligned}$$

Then (it follows from the previous result that)

$$\begin{aligned} \mathcal{N}(p) = \mathcal{N}\left(p p_0\right) &\equiv n + k \mod 2 \\ &\equiv n + \ell \mod 2. \end{aligned}$$

Therefore

$$k \equiv \ell \mod 2,$$

which means that p is either a product of an even number of transpositions or a product of an odd number of transpositions, but never both.

==

[1] As a matter of fact, there are many ways to write a cycle as a product of transpositions. For example, the 4-cycle $(\mathbf{1\ 3\ 4\ 7})$ can be written as $(\mathbf{1\ 7})(\mathbf{1\ 4})(\mathbf{1\ 3})$ or as $(\mathbf{4\ 7})(\mathbf{3\ 4})(\mathbf{1\ 3})(\mathbf{3\ 7})(\mathbf{1\ 4})$.

[2] For example, concerning the identity permutation of S_n, $\mathcal{N}(1) = n$ when considering $1 = (\mathbf{1}) \cdots (\mathbf{n})$.

==
==
2
==
==
Comments/Errata
==
==
p. **40**, l. 12
'Exercise 1.3' should be 'Exercise 1.2'.
==
p. **47**, **P. 2.4.3**, last bullet
First, n/d is a positive integer and

$$\begin{aligned}\left(x^k\right)^{n/d} &= (x^n)^{k/d}\\ &= 1^{k/d}\\ &= 1.\end{aligned}$$

Now, suppose that ℓ is an integer such that $\left(x^k\right)^{\ell} = 1$. Since the second bullet also means that

$$x^k = 1 \Longleftrightarrow n|k,$$

it suffices to show that

$$n/d|\ell.$$

In fact, it follows from

$$\begin{aligned}x^{k\ell} = 1 &\Rightarrow n|k\ell\\ &\Rightarrow k\ell = mn \text{ for some integer } m\\ &\Rightarrow \frac{k}{d}\cdot\ell = m\cdot\frac{n}{d}\\ &\Rightarrow n/d|\frac{k}{d}\cdot\ell\end{aligned}$$

and

$$\gcd\left(\frac{n}{d},\frac{k}{d}\right) = 1.$$
==
p. **63**

- **E. 2.10.6**
  - Let $\mathcal{H}$ be a subgroup of S_3. First, $\mathcal{H} = S_3$ if $x, y \in \mathcal{H}$. Second, if $xy, x^2y \in \mathcal{H}$, then $x^2yxy = x \in \mathcal{H}$, which implies that $xx^2y = y \in \mathcal{H}$. Finally, if $xy \in \mathcal{H}$ or $x^2y \in \mathcal{H}$,

    $$x \in \mathcal{H}, \text{ that is, } x^2 \in \mathcal{H} \Longleftrightarrow y \in \mathcal{H}.$$

    Therefore, whichever $\mathcal{H}$ one considers,

    $$\mathcal{H} \in \left\{\{1\}, \langle x\rangle, \langle y\rangle, \langle xy\rangle, \langle x^2y\rangle, S_3\right\}.$$

  - Since $K \subset A_4$, A_4 corresponds to $\langle x\rangle$.

- last bullet[3]
  Consider $H = \varphi^{-1}(\mathcal{H})$ and the restriction $\varphi|_H$. Since $K \subset H$, $\ker(\varphi|_H) = K$ by (2.10.2). Therefore, since $\varphi(H) = \mathcal{H}$ is the image of $\varphi|_H$, the first bullet of **C. 2.8.13** implies that

  $$|H| = |\mathcal{H}||K|.$$

[3]On p. **64**, its proof is left as an exercise!

==
p. **67**, ll. 2-3 after □, “... $[C_1C_2]$, Where ...”
‘W’ should be ‘w’.
==
p. **69**, *Proof*

Some points on the bijectivity of $\overline{\varphi}$:

1st, the elements of the image of φ correspond bijectively to the nonempty fibres of φ as stated on p. **55**. 2nd, not only all such fibres are nonempty, by virtue of the surjectivity hypothesis, but also they are the equivalence classes for the relation defined by φ as stated on pp. **55-6**. Furthermore, such fibres are the cosets of N by **P. 2.7.15**.

Another way to prove that $\overline{\varphi}$ is bijective:

- $\overline{\varphi}$ is surjective.
  In fact, consider $y \in G'$. Since φ is surjective, there is an element $x \in G$ such that $y = \varphi(x)$. Therefore $\varphi^{-1}(y) = \overline{x}$ is an element of $\overline{G}$ such that $y = \overline{\varphi}\,(\overline{x})$.

- $\overline{\varphi}$ is injective.
  In fact,

$$\begin{aligned}\overline{\varphi}\,(\overline{x}) = \overline{\varphi}\,(\overline{y}) &\Rightarrow \varphi(x) = \varphi(y)\\ &\Rightarrow \overline{x} = \overline{y}\end{aligned}$$

  by **P. 2.5.8**.

==
==
3
==
==
Comments/Errata
==
==
p. **82**, l. 9
$\mathbb{F}_P^{\times}$ should be $\mathbb{F}_p^{\times}$.
==
p. **85**, l. -12
$\{cw\}$ should be cw.
==
p. **89**, **P. 3.4.15(a)**
Concerning the if part, consider $w \in \operatorname{Span} S$. Now apply **L. 3.4.5**.
==
p. **90**, **T. 3.4.18**, *Proof*, $(SA)X = S(AX)$
In fact,

$$\begin{aligned}(SA_1, \ldots, SA_2)\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} &= \sum_{j=1}^{n} \left(SA_j\right) x_j \\ &= \sum_{j=1}^{n} S\left(A_j x_j\right) \\ &= S\left(\sum_{j=1}^{n} A_j x_j\right)\end{aligned}$$

since, by abuse of notation, $S : F^m \to V$ is linear by (3.4.2).[4]
==
p. **98**, **C. 3.7.7**, 1st bullet
Suppose V has an infinite basis **B**. Therefore, on the one hand, **B** contains a finite subset S that spans V (**L. 3.7.6**), which is independent due to the independence of **B**. On the other hand, consider S, w and S' are as in **P. 3.4.15(b)** with $w \in$ **B**. Then, since $w \in \operatorname{Span} S$, S' is not independent, which is a contradiction since S' is a finite subset of **B**, which is independet.

[4]The notation for such a linear transformation appears in the sentence right after (3.5.3).

==
==

4

==
==

Comments/Errata

==
==

p. **104**, l. -1
(4.2.3) is consistent with possible repetitions of images.[5]

==

p. **106**, **P. 4.2.13**, *Proof*
Once bases are fixed for the domain and codomain of T, the conclusion of part **(a)** is a consequence of the uniqueness of A'. In fact, the coefficients of (4.2.7) are unique since **C** is independent.

==

p. **107**, 1st three sentences after (4.2.15)
The restriction of Q to U', the column space of A', is an isomorphism from U' to U, the column space of A, since:

1. Q is linear;
2. Q is invertible;
3. $Q(A'X') = A(PX')$ for each $X' \in F^n$.

==

p. **108**, l. -7
$K = 0$ should be $K = \{0\}$.

==

pp. **112-13**, content of the '•'
For a complete and general proof, see the Perron-Frobenius Theorem.

==
==

Exercises, pp. **125-131**

==
==

2.4. (A proof without using row and column operations!)
Concerning (4.2.9), replace T with A and take **B** and **C** as in **T. 4.2.10(a)**. Furthermore, if

$$\mathbf{B} = \{P_1, \ldots, P_n\} \quad \text{and} \quad \mathbf{C} = \{Q_1, \ldots, Q_m\},$$

consider the matrices

$$P = \begin{bmatrix} P_1 & \ldots & P_n \end{bmatrix} \quad \text{and} \quad Q = \begin{bmatrix} Q_1 & \ldots & Q_m \end{bmatrix}.$$

Therefore the diagram

$$\begin{array}{ccc} F^n & \xrightarrow{A'} & F^m \\ {\scriptstyle P}\downarrow & & \downarrow{\scriptstyle Q} \\ F^n & \xrightarrow{A} & F^m \end{array}$$

commutes.

[5] See p. **86**, 2nd paragraph of **3.4**.

==
==
11
==
==
Comments
==
==
p. **331**, l. -3
Let I be an ideal and a a unit (of R). Then the 2nd bullet of **D. 11.3.13** implies that $1 = a^{-1}a \in I$ and, for each $r \in R$, $r = r1 \in I$. Therefore $R \subset I$.
==
p. **334**, last sentence before **L. 11.3.24**
(Here, $R[x]f$ denotes the multiples of f in $R[x]$ with $R = \mathbb{Z}, \mathbb{Q}$ (11.3.15).) On the one hand, since $\ker \Phi' \subset \ker \Phi = \mathbb{Q}[x]f$ (**E. 11.3.23**), if $g \in \operatorname{Ker} \Phi'$, then $g \in \mathbb{Z}[x]$ and f divides g in $\mathbb{Q}[x]$. Thus f divides g in $\mathbb{Z}[x]$ (**L. 11.3.24**). Hence $\ker \Phi' \subset \mathbb{Z}[x]f$. On the other hand, since $\mathbb{Z}[x]f \subset \mathbb{Q}[x]f = \ker \Phi$, if $g \in \mathbb{Z}[x]f$, then $g \in \mathbb{Z}[x]$ and $\Phi(g) = 0$. Hence $g \in \ker \Phi'$. Therefore $\ker \Phi' = \mathbb{Z}[x]f$.
==
p. **336**, last sentence
Since φ is surjective by hypothesis and $\tilde{\pi}$ is surjective by **T. 2.12.2**, p. **66**, it follows that $f = \tilde{\pi}\varphi$ is surjective. Hence $\overline{f}$ is an isomorphism.
==
p. **337**

E. 11.4.4(b)
Here, π is used in place of φ of the **Correspondence Theorem**. $\ker \pi = \left(t^2 - 1\right)$ follows from **T. 11.4.1**. $I = (f)$ follows from **P. 11.3.22**.

l. -9
Since π is surjective and $\ker \pi = I$, if $I = R$, then $\overline{R} = \left\{\overline{0}\right\}$.

==
p. **338**, **E. 11.4.5**

- $\mathbb{Z}[x] \to \mathbb{Z}[i]$ can be thought of as being the extension Φ of $\varphi : \mathbb{Z} \to \mathbb{Z}[i]$ as considered in the **Substitution Principle**. (As a matter of fact, here, φ is the inclusion map by **P. 11.3.10**.) Notice that $K = \ker \Phi$ is an ideal as can be seen on page **331**. Furthermore, $K = (f)$. In fact, on the one hand, $i^2 + 1 = 0$ shows that $f \in K$; hence $(f) \subset K$. On the other hand, if $h \in K$, then $h(i) = 0$, which implies that $h(-i) = 0$ by the Complex Conjugate Root Theorem. Thus $x \pm i$ divide h in $\mathbb{C}[x]$. Then

$$\begin{aligned}(x+i)(x-i) &= x^2 + 1 \\ &= f\end{aligned}$$

  divides h in $\mathbb{Z}[x]$. So $h \in (f)$. Therefore $K \subset (f)$.

- $\mathbb{Z}[x] \to \mathbb{Z}$ can be thought of as being the extension Φ of $\varphi : \mathbb{Z} \to \mathbb{Z}$ as considered in the **Substitution Principle**. (As a matter of fact, here, φ is the identity map by **P. 11.3.10**.) Notice that $K = \ker \Phi$ is an ideal as can be seen on page **331**. Furthermore, $K = (g)$. In fact, on the one hand, $x - 2 \rightsquigarrow 0$ shows that $g \in K$; hence $(g) \subset K$. On the other hand, if $h \in K$, then $h(2) = 0$. Thus $x - 2$ divides h in $\mathbb{Z}[x]$. So $h \in (g)$. Therefore $K \subset (g)$.

==
p. **340**, *Proof of the proposition*, **(a)**, last sentence

$$\begin{aligned}\beta &= a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha_1 + a_0 \\ &= b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha_1 + b_0\end{aligned}$$

implies that $(a_{n-1} - b_{n-1})\, x^{n-1} + \cdots + (a_1 - b_1)\, x + a_0 - b_0$ belongs to (f)!
==

p. **341**, **P. 11.6.1(d)**
Note that $(1,1)$ is neither in $R \times \{0\}$ nor in $\{0\} \times R'$.
==
p. **342**, **E. 11.6.3(b)**
If $f(x,0) = 0$ and $f(0,y) = 0$, it follows from **C. 11.3.9** that both $y-0$ and $x-0$ divide $f(x,y)$ in $\mathbb{C}[x,y]$.
==
p. **343**, ll. 6,7
See **E. 7.2**.
==
p. **343**, *Mapping Property*
Note that, if ϕ denotes the embedding of R into F, then

$$\varphi = \Phi \circ \phi.$$

Now, Φ is a homomorphism since

$$\begin{aligned}
\Phi(0/1) &= \Phi(\phi(0)) \\
&= \varphi(0) \\
&= 0, \\
\Phi(1/1) &= \Phi(\phi(1)) \\
&= \varphi(1) \\
&= 1, \\
\Phi\left(\frac{a}{b} + \frac{c}{d}\right) &= \Phi\left(\frac{ad+bc}{bd}\right) \\
&= \varphi(ad+bc)\varphi(bd)^{-1} \\
&= (\varphi(a)\varphi(d) + \varphi(b)\varphi(c))\varphi(b)^{-1}\varphi(d)^{-1} \\
&= \varphi(a)\varphi(b)^{-1} + \varphi(c)\varphi(d)^{-1} \\
&= \Phi\left(\frac{a}{b}\right) + \Phi\left(\frac{c}{d}\right) \text{ and} \\
\Phi\left(\frac{a}{b}\frac{c}{d}\right) &= \Phi\left(\frac{ac}{bd}\right) \\
&= \varphi(ac)\varphi(bd)^{-1} \\
&= \varphi(a)\varphi(c)\varphi(b)^{-1}\varphi(d)^{-1} \\
&= \varphi(a)\varphi(b)^{-1}\varphi(c)\varphi(d)^{-1} \\
&= \Phi\left(\frac{a}{b}\right)\Phi\left(\frac{c}{d}\right).
\end{aligned}$$

==
p. **345**, l. 7
For the use of '$<$' in place of '$\subset$', see p. **527**.
===
=== ==========

Exercises, pp. **354-358**

==
==

7.2. Consider $p(x), q(x) \in R[x] - \{0\}$. Let $a_{\deg p}$ and $b_{\deg q}$ be the leading coefficients of $p(x)$ and $q(x)$, respectively. Since R is a domain, $a_{\deg p} b_{\deg q}$ is the leading coefficient of $p(x)q(x)$. In particular, $p(x)q(x) \neq 0$ and

$$\deg(pq) = \deg p + \deg q.$$

==
==
14
==
==
Errata

p. **421**, l. 6
r should be k.

==
==
Comments

p. **414**, *Proof*, **(a)**
If A is an $n \times n$ matrix and L is an $m \times n$ matrix with $LA = I_m$, then $m = n$.

p. **421**, ll. 10-12, "**(b)**,**(d)** ... □"
Note that, since $A' = Q^{-1}AP$, if $X' = P^{-1}X$ and $Y' = Q^{-1}Y$, then

$$\begin{aligned} AX = Y &\Leftrightarrow \left(Q^{-1}AP\right) P^{-1}X = Q^{-1}Y \\ &\Leftrightarrow A'X' = Y'. \end{aligned}$$

p. **421**, **C. 14.4.10**
See (14.2.9) (with $R = \mathbb{Z}$), (14.4.7) and the sentence right before **P. 14.2.6**.

p. **421**, 1st sentence of the *Proof* of **T. 14.4.11**
As far as the existence of **B** is concerned, consider the very end of the proof.

==
==