**Mathematics via Problems, part 1: Algebra**
*Arkadiy Skopenkov*
MSRI/AMS 2021
**Errata and addenda by Darij Grinberg (version of March 16, 2024)**

# 1. Errata

Some of the items below are not corrections of literal mistakes but rather suggestions written according to my taste and ideology. I hope they are nevertheless helpful.

## 1.1. Introduction

- **page xx:** The definition of $A \sqcup B$ at the very bottom is not really understandable if one has not seen disjoint unions of non-disjoint sets before. I would suggest adding the formal definition, as I suspect that many olympiad-trained students do not know this concept.

## 1.2. Chapter 1

- **1.1.3:** "for any $a$ and $b$" → "for all $a$ and $b$". The word "any" is notoriously slippery in mathematics, as it can mean both $\forall$ and $\exists$ depending on its position in the sentence. In situations that are not completely clear-cut, I prefer not to use it at all.
- **1.1.3:** The solution to this uses problem 1.1.4. Why not switch the order of the two exercises then?
- **1.1.5:** The word "or" is unclear: Does it mean "$2 \nmid k$ or $3 \nmid k$ or $5 \nmid k$" or "$2 \nmid k$ and $3 \nmid k$ and $5 \nmid k$"? I suggest writing "If none of 2, 3 and 5 divides $k$".
- **1.2.1 (a):** "$a$¿1" should be "$a > 1$".
- **1.2.1 (b):** After "which are divisible by $p_i$", add "and larger than $p_i$".
- **1.2.5 (c):** This has nothing to do with primes. (The only thing necessary is that $p_1 = 2$ and $p_2 < p_3 < p_4 < \cdots$ and that $p_2, p_3, p_4, \ldots$ are odd.) Doesn't this inconsequential puzzle distract the reader here?
- **1.2.8 (d):** This uses a later result (1.5.7 (c)). Why not swap the order of the sections?
- **1.3.3 (a):** This requires $b > 0$; otherwise it should be $(a, b) = |b|$.
- **between 1.3.5 and 1.3.6:** "smallest number" → "smallest positive integer".

- **solution to 1.3.3 (c):** Here you use the Euclidean algorithm, which is only explained later (1.5.9 (b)). Maybe better restate this as an inductive proof? (This would probably be shorter anyway.)

- **hint to 1.4.1 (a):** Replace "$0 \leq a \leq |b|$" by "$0 \leq a < |b|$". Also, replace "about $a - b$" by "about $a - |b|$".

- **1.5.5 (a):** Why write $(|a|, |b|)$ instead of $(a, b)$ ?

- **1.5.9 (b):** "set $d := a_k$" → "set $d := |a_k|$".

- **1.5.10 (d):** I find it strange that such a crucial and nontrivial fact is stated without a hint or proof.

- **solution to 1.5.7 (c), "Another hint":** "so $p \mid ab$" should be "so $p \mid a$".

  Next, "let $p \leq ib$" should be "let $p < ib$".

  Finally, "Note that $0 \leq ib - p \leq b$" should be "Note that $0 < ib - p < b$".

- **solution to 1.5.8 (a):** The right hand side should be $\left|n^{(a,b)} - 1\right|$ (since $n^{(a,b)} - 1$ can be negative but a gcd cannot).

- **1.6.3:** When the number is called $n$, it is probably better to use a different letter for the number of its prime factors.

- **1.6.6 (a):** This must require $a, b > 0$; otherwise, $a = -4$ and $b = -9$ would be a counterexample.

- **1.6.6 (d):** Same as for part (a) (unless $n$ is odd).

## 1.3. Chapter 2

- **2.1.1 (d), Alternative formulation:** "$n^p - 1$" should be "$n^{p-1} - 1$".

- **2.1.5 (c):** "and $\varphi(m)$" → "and if $\varphi(m)$". (Otherwise, it sounds like $n$ should be relatively prime to both $m$ and $\varphi(m)$".

- **between 2.1.6 and 2.1.7:** The relation to cryptography is unlikely to be understood by anyone who does not already know about RSA.

- **2.3.1 (d):** "numbers" → "positive integers".

- **last line of page 24:** Any references to these texts?

- **solution to 2.4.1 (a):** An "$\equiv$" sign is missing between "$\cdot (8k+3)$" and "$2^{4k+2}$" on the second line of the long computation.

- **solution to 2.4.2 (a):** An "$\equiv$" sign is missing between "$\cdot (8k-1)$" and "$(-1)\, 2^{4k}$" on the second line of the long computation.

- **solution to 2.4.5 (d):** Replace "$\left[\frac{py}{p}\right]$" by "$\left[\frac{qy}{p}\right]$" three times in this solution.
- **2.5.6 (b):** Are you sure you want to leave this crucial and difficult fact without proof or hint?
- **solution to 2.5.6 (a):** "may by" → "may be".
- **2.6.3 (b):** Add "for $p > 2$ prime".
- **page 29, footnote $^3$:** "where $k$ satisfies" → "where $u$ satisfies".
- **hint to 2.6.2 (a):** *"smallest nonzero degree"* → *"smallest nonzero-degree power"*.
- **hint to 2.6.2 (c):** *"smallest nonzero degree"* → *"smallest nonzero-degree power"*.

## 1.4. Chapter 3

- **solution to 3.2.4 (b):** Don't forget to define $\varepsilon_3$. (I understand you want $\varepsilon_3 := \frac{-1+i\sqrt{3}}{2}$.)
- **solution to 3.2.7 (a):** "Since $p = 2\alpha - A^2$ and $\alpha$ are roots" → "Since $p = 2\alpha - A^2$ and since $\alpha$ is a root". There is no reason why $p$ should be a root!
- **page 39, third paragraph:** "function $\overline{P} : R \to R$" should be "function $\overline{P} : \mathbb{R} \to \mathbb{R}$".
- **3.3.2:** This really needs a solution, to ensure the reader is not left with a wrong definition.
- **3.4.5:** It should be explained what the "unique" means here (unique up to scalar factors, not just up to sign as for integers).
- **3.5.11:** A whitespace is missing in "and$\{y_n\}$".
- **solution to 3.6.3:** This needs a definition of "lexicographic order". On a related note, I don't expect many readers not already familiar with the theory to come up with a useful notion of "multi-degree" on their own.
- **3.7.2 (a):** Again, it should be explained what "uniqueness" means (unique up to multiplication of any factor by ±1 or $\pm i$).
- **3.7.2 (d):** "there exists $k$" → "there exists a Gaussian integer $k$" (the letter $k$ otherwise suggests an integer).
- **3.7.3:** "$Z[\xi]$" → "$\mathbb{Z}[\xi]$".

- **3.7.4 (b), (c):** Add "up to permuting the two addends".
- **3.7.4:** What do you mean by "section 3"?
- **solution to 3.9.1:** I can't make anything out of this. I know that Igor Pak gives a fairly nontrivial proof in his *Lectures on Discrete and Polyhedral Geometry* ( `https://www.math.ucla.edu/~pak/geompol8.pdf` , Theorem 3.2).

## 1.5. Chapter 4

- **first paragraph:** "subsection3.I" needs a whitespace.
- **after 4.1.1:** The two definitions of a permutation (either as a list of the elements in some order, or as a one-to-one mapping) are not equivalent, unless the set is of the form $\{1, 2, \ldots, n\}$ for some $n \in \mathbb{N}$. You use the latter definition.
- **page 59:** This would be a good place to define a graph. In a book that defines divisibility, I wouldn't expect the reader to know what a graph is! It doesn't help that there are several inequivalent notions of graph (directed/undirected, simple/multi) around that don't always behave identically.
- **4.1.4:** After "For any permutation $f$", add "of a finite set".
- **4.1.6:** "order of the composition" → "order of a composition".
- **4.1.8 (b):** "cyclic decomposition" has not been defined.
- **4.2.1 (c):** The 15-puzzle was invented by Noyes Palmer Chapman in New York State; I think its only connection to Russia is its popularity in the Soviet Union.
- **4.2.1 (c):** "by sequentially moving the squares to an open square" is not really a clear description of the allowed moves.
- **4.2.4:** Don't talk about "a permutation" each time. Rather, say "Given a permutation $\sigma$ of a finite set" at the beginning, and then speak of $\sigma$. Otherwise, it sounds like you have an implicit $\forall\sigma$ quantifier in front of each statement, which is not what you intend (you want $\sigma$ to be fixed).
- **page 65:** "Distribute trains between stations so that at each station we place all the different trains that can be obtained from a single coloring of the carousel (by decoupling two cars in the carousel). Then the required number $Z$ of colorings is equal to the number of stations.": I would be completely lost trying to understand this if I did not already know what this is supposed to explain (the partition of the set of all painted trains

into rotation-equivalence classes). I think it would be much clearer to talk about equivalence classes instead of trying to invent nicknames for them. For the sake of clarity, an example would work wonders...

## 1.6. Chapter 5

- **page 69, definition of concavity:** This definition of "concave up" is nonstandard (the standard definition would require $f(sx+ty) \leq sf(x) + tf(y)$ for any $x, y \in I$ and $s, t \in [0, \infty)$ satisfying $s+t=1$), and allows for "Cauchy monsters" (nowhere continuous functions that satisfy $f(x+y) = f(x) + f(y)$ for all $x, y \in \mathbb{R}$). I'm not sure if problem 5.1.2 can even be solved with this definition (the minimum is clear, but the maximum?).

- **5.1.7 (c):** "A function with" → "A function $f$ with".

- **5.1.9 (a):** "$f : I \to R$" should be "$f : I \to \mathbb{R}$".

- **5.1.9 (a):** "convex down" → "concave up" (that's how you called it when you defined it). And again, this seems to require the standard definition.

- **page 72, line 2:** The word "Therefore" here is inappropriate: The fact that we get to $\frac{1}{n}, \frac{1}{n}, \ldots, \frac{1}{n}$ after no more than $n$ replacements (actually $n-1$ are enough) has nothing to do with the product increasing.

- **solution to 5.1.2:** Remove the "(a)"; this problem has no parts.

- **5.2.4:** It is important to notice that the variables in this problem are not assumed by default to be nonnegative, except for the $y_1, y_2, \ldots, y_n$ in part (d) (which are assumed to be positive). Otherwise, part (a) would be false (assuming $at^2 + 2bt + c \geq 0$ only for $t \geq 0$ does not guarantee $b^2 \leq ac$).

- **5.2.4 (a):** "for any" → "for all".

- **Hint to 5.2.3 (c):** A non-Russian reference would be helpful to the Anglophone reader. Melvyn Nathanson's arXiv:2201.01270 preprint is one possible reference.

- **solution to 5.3.2 (a):** "The case of integer values" is irrelevant, since all variables are positive by assumption.

- **solution to 5.3.7 (a):** On the first line of the computation, "$\frac{c^2}{(d+a)}$" should be "$\frac{c^2}{c(d+a)}$".

## 1.7. Chapter 6

- **between 6.1.3 and 6.1.4:** "$\Delta\left(\Delta\left(\cdots\right)\right)a_n$" should be "$\Delta\left(\Delta\left(\cdots\left(a_n\right)\right)\right)$".
- **solution to 6.1.2 (b):** The displayed equation

$$\Delta\frac{1}{n\left(n+1\right)\cdots\left(n+\left(k+1\right)\right)}=-\frac{k+2}{\left(n+1\right)\left(n+2\right)\cdots\left(n+k+1\right)}$$

  should be

$$\Delta\frac{1}{n\left(n+1\right)\cdots\left(n+\left(k+1\right)\right)}=-\frac{k+2}{n\left(n+1\right)\cdots\left(n+k+2\right)}.$$

  The error, alas, worms its way through the entire solution. In particular, the answer, too, is false.
- **6.2.6 (c):** You are using the letter $k$ for two different things here (the degree of the polynomial and the number of **distinct** roots).
- **6.5.10 (b):** The sum should start at $n=0$, not at $n=1$.
- **6.6.5 (b):** In the definition of $d_n\left(q\right)$, replace "$w_1,\ldots,w_q>0$" by "$w_1,\ldots,w_q\geq 0$".
- **page 102, proof of Mahler's theorem 6.6.7:** "Assume the converse" → "Assume the contrary".
- **page 103, first displayed equation:** Again replace "$w_1,\ldots,w_q>0$" by "$w_1,\ldots,w_q\geq 0$".
- **page 103:** After "It is clear that $d_n\left(q\right)=0$ if and only if $n$ has more than $q$ ones in its binary expansion", add "or $n<q$".

## 1.8. Chapter 7

- **page 108, second paragraph:** "defined a similar way" → "defined in a similar way".
- **§7.2, first paragraph:** "called the *change of sign*" → "called a *change of sign*".
- **7.2.7 (a):** "the maximum and minimum" → "a maximum and a minimum" (these are neither unique nor identical).
- **7.2.7 (b):** "lies the root" → "lies a root".
- **Theorem 7.2.8 (b):** It is strange to speak of a $c\in[a,b]$ here, since $f^{(n)}$ is constant and thus $f^{(n)}\left(c\right)$ does not depend on $c$. Perhaps you don't want to require $f$ to have degree $n$ ?

- **7.3.1 (a):** The words "convex hull" appear here for the first time in the book; the reader might not be familiar with them.
- **page 116, first two paragraphs:** "A point $x \in R$" → "A point $x \in \mathbb{R}$" (twice).
- **page 116, fourth paragraph:** "of the function" → "of the function $f$".
- **7.3.5 (c):** "polynomial" → "nonzero polynomial".
- **7.3.10 (b):** "$p(a) \neq 0$" should probably be "$p(0) \neq 0$".
- **7.5.1:** The period in "0001." should be outside of the quotation marks.

## 1.9. Chapter 8

- **§1.C, first line:** *"expressible by radicals"* → *"expressible in real radicals"*.
- **page 127, bullet point at the top:** This equivalence is not obvious, because the polynomials $p_0, p_1, \ldots, p_s$ can emulate addition, subtraction and multiplication but not obviously division. I understand that division is unnecessary because all the constructed real numbers are algebraic over $\mathbb{Q}$, but this is not obvious to the reader at this point.
- **Remark 8.1.9:** "none of the roots" → "all of the roots".
- **between Remark 8.1.9 and Theorem 8.1.10:** "A polynomial" → "A nonconstant polynomial".
- **Conjecture 8.1.11 (a):** After "(defined after problem 3.2.6 (b)", add a closing parenthesis.

  Also, it is worth stating a precise definition of the resolvent cubic. It is only vaguely hinted at in problem 3.2.6 (b).
- **Conjecture 8.1.11 (b):** I. M. Isaacs, in his paper *Solution of Polynomials by Real Radicals* (American Mathematical Monthly **92** (1985), issue 8), shows the following fact: If an irreducible polynomial $f \in \mathbb{Q}[x]$ (irreducible over $\mathbb{Q}$) splits over $\mathbb{R}$ (that is, all its complex roots are real) and has a root that is expressible in real radicals (Isaacs calls this "real radical"), then $\deg f$ is a power of 2. Applying this to the minimal polynomial of $\cos \frac{2\pi}{n}$ (which has degree $\varphi(n)/2$ because all the $\varphi(n)/2$ numbers $\cos \frac{2\pi k}{n}$ where $k$ is coprime to $n$ are algebraic conjugates of $\cos \frac{2\pi}{n}$ [1]), we see that $\varphi(n)/2$ is

[1] Alternatively, we can argue that this polynomial is the $n$-th cyclotomic Chebyshev polynomial of the first kind (whose roots are the $\varphi(n)/2$ numbers $\cos \frac{2\pi k}{n}$ where $k$ is coprime to $n$).

a power of 2 if $\cos \frac{2\pi}{n}$ is expressible in real radicals. But this quickly yields that $\cos \frac{2\pi}{n}$ is real constructive by Theorem 8.1.5. This proves Conjecture 8.1.11 (b).

- **Remark 8.2.1 (b):** What does this mean? Are you just saying that we can construct any polynomial of the form $P(\sigma_1, \sigma_2, \ldots, \sigma_n)$ ?
- **Remark 8.2.1 (d):** Replace "$sigma_n$" by "$\sigma_n$" (missing backslash).
- **8.2.4 (b):** "mulitiplication" → "multiplication".
- **page 138, solution to 8.2.7 (a):** On the very last line of the page, a closing parenthesis is missing after the product.
- **page 143, line 2:** "such that $mx + ny = 1$" → "such that $nx + my = 1$".
- **page 143, proof of constructibility:** It should be explained that $\varepsilon$ means $\varepsilon_n$ here.
- **page 143, proof of constructibility:** At the end of the last display, "for any $k$" should be "for any $k \not\equiv 0 \bmod n$".
- **page 143, proof of constructibility:** "Consider the polynomial $x + a_2x^2 + \cdots + a_{n-1}x^{n-1}$" → "Consider the polynomial $a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1}$".
- **page 143, end of §2.F:** The same argument that you use to prove 8.1.5 here also proves 8.1.15 (a). This is worth mentioning, since the other proof you give on page 146 is much more complicated and hard to follow.
- **page 144, sketch of the proof:** This is not a sketch of a proof, but rather an approach that you only finish later. Calling it a "sketch" is confusing.
- **8.2.18 (c):** "(in residues modulo $2^m$)" → "(in residues modulo $2^{m-1}$)".
- **8.2.20 (a):** "$4k + g^{4l+2}$" should be "$g^{4k} + g^{4l+2}$".
- **page 146:** There are several typos in this proof and I cannot completely follow it (although I understand the idea). I think a lot of it would be simplified if you gave names to the groups and cosets that you are summing over; with all the groups being cyclic, this hardly requires any serious abstraction. Anyway, here is a short (perhaps incomplete) list of typos:
  - There is a $j$ appearing sometimes. Is it a synonym for $k$ ?
  - Replace "$gb_0$" by "$g^{b_0}$".
  - Replace "$g^{2j}$" by "$g^{2^j}$".
  - Replace "$gb'_0$" by "$g^{b'_0}$".

- **page 152, hint to 8.3.4 (d):** "$\mathbb{Q}\left[\sqrt{2}\right]$" should be "$\mathbb{Q}\left[r\right]$".
- **page 153, solution to 8.3.2:** On the last line, remove the "$b$" in "$a_1 + b\sqrt{a_2^2 c}$".
- **page 157, solution to 8.3.12:** How exactly? (And I'm not sure how helpful this is, seeing that you give no hint to 8.4.1.)
- **solution to 8.3.15 (d):** "$x^2 - 2 - \sqrt{3}$" and "$x^2 - 2 + \sqrt{3}$" should be "$x^2 - 1 - \sqrt{3}$" and "$x^2 - 1 + \sqrt{3}$", respectively.
- **solution to 8.3.18 (c):** "Divide $x^3 - r^3$" → "Divide by $x^3 - r^3$".
- **8.3.32:** Please don't use the notation $f'$ for something that isn't the derivative of $f$ (or at least explain that it does not mean the derivative here).
- **8.3.32 (c):** There is an unnecessary linebreak before "$f_s$".
- **8.3.33:** What does "only one way" mean?
- **page 182, proof of Lemma 8.4.13:** In the long equality that defines $\rho$, should the "$\varepsilon_q^{(1-k)l}$" in the numerator perhaps be "$\varepsilon_q^{(1-q)l}$"?