Introduction to Abstract Algebra
Samir Siksek
MA136; PDF version dated September 22, 2020
`https://samirsiksek.github.io/siksek.github.io/teaching/aa/aanotes.pdf`
Errata and comments by Darij Grinberg

The page numbers below refer to the printed page numbers in the PDF version dated September 22, 2020. This list is not claimed to be exhaustive.

All the errata below were found by GPT-5.6 Sol, then verified (and occasionally reworded) by myself.

A. Corrections and comments

1. **Page 2, last sentence of Section I.3:** Insert "be" in "where you may asked".
2. **Page 4, item (2):** Insert "a" in "It isn't possible to write $\mathbb{R}$ in straightforward way".
3. **Page 5, Section II.3:** Replace "If $\mathbf{x}, \mathbf{y} \in \mathbb{R}^3$ the $\mathbf{x} \times \mathbf{y}$ is again in $\mathbb{R}^3$" by "If $\mathbf{x}, \mathbf{y} \in \mathbb{R}^3$, then $\mathbf{x} \times \mathbf{y}$ is again in $\mathbb{R}^3$".
4. **Page 6, paragraph before Lemma II.2:** Insert "is" in "but it one of the most important results".
5. **Page 7, first paragraph of Section II.6:** Replace "If the S is finite" by "If S is finite".
6. **Page 7, Example II.3:** Delete the comma in "The result of the composition $a \circ b$, is found".
7. **Page 16, paragraph before (III.6):** Replace "This pair of equations can re-expressed" by "This pair of equations can be re-expressed".
8. **Page 17, first paragraph:** Replace "we expect that matrix equations (III.6) and (III.7) to be consistent" by either "we expect matrix equations (III.6) and (III.7) to be consistent" or "we expect that matrix equations (III.6) and (III.7) are consistent".
9. **Page 18, Example III.8:** Replace "C represent projection onto the y-axis" by "C represents projection onto the y-axis".
10. **Page 19, Subsection III.4.1:** Replace "slight-of-hand" by "sleight of hand".

11. **Page 19, proof of Theorem III.9:** Associativity of composition shows that the two sides induce the same function, but the proof has not explained why equality of the induced functions implies equality of the matrices. It also uses, without stating it, the compatibility between matrix multiplication and composition.

    A short completion is as follows. For compatible matrices X and Y, the definition of matrix multiplication gives

    $$T_{XY} = T_X \circ T_Y.$$

    Hence $T_{(AB)C} = T_{A(BC)}$. If two $m \times q$ matrices D and E induce the same function $\mathbb{R}^q \to \mathbb{R}^m$, then $D\mathbf{e}_j = E\mathbf{e}_j$ for every standard basis vector $\mathbf{e}_j$; but these vectors are the j-th columns of D and E. Thus $D = E$, and therefore $(AB)C = A(BC)$.

12. **Page 22, first sentence:** Replace the full stop in "Should there be such an inverse A^{-1} for every A." by a question mark.

13. **Page 23, end of Example III.10:** In

    $$C^{-1}C = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & b \\ 0 & d \end{pmatrix},$$

    it is the *top-left* entries that do not match those of I_2; the bottom-left entries are both 0.

14. **Page 24, Theorem III.11 and the surrounding discussion:** This is true over a field such as $\mathbb{R}$, $\mathbb{Q}$, or $\mathbb{C}$. It is false for invertibility inside $M_{2\times 2}(\mathbb{Z})$: there the determinant must be ± 1. This distinction becomes important in Exercise VI.2 and Example XIV.25.

15. **Page 25, proof of Theorem III.12 (c):** Replace "applying (ii)" by "applying (b)".

16. **Page 26, derivation of the rotation matrix:** After "and let the angle $\overrightarrow{OP}$ makes with the positive x-axis be ϕ", add "(or pick ϕ arbitrarily when $P = O$)".

17. **Page 30, first bullet point:** Replace "Like in $\mathbb{R}^2$ we have addition and scalar multiplication" by "Likewise, in $\mathbb{R}^2$ we have addition and scalar multiplication".

18. **Page 31, paragraph before the composition table:** Replace "This has the same effect at σ_1" by "This has the same effect as σ_1".

19. **Page 32, last paragraph:** Replace "$\circ$ simply becomes composition of functions from D_4 to itself" by "$\circ$ simply becomes composition of functions from $\{1, 2, 3, 4\}$ to itself".

20. **Page 33, Subsection IV.4.1:** Replace "seeing the $(R, \circ)$ is abelian" by "seeing that $(R, \circ)$ is abelian".

21. **Page 34, Exercise IV.14:** Replace "isoceles" by "isosceles".

22. **Page 39, Theorem VI.1:** Insert "a" in "$\mathrm{GL}_2(\mathbb{R})$ is group under multiplication of matrices".

23. **Page 40, Section VI.2:** Replace "In otherwords" by "In other words" (unless an otherworld is being referred to, which requires a different correction). Later in the same paragraph, "addition and multiplication is defined" should be "addition and multiplication are defined".

24. **Page 41, proof of Theorem VI.5:** Insert "is" in "To show that $\mathbb{Z}/m\mathbb{Z}$ a group".

25. **Page 43, Example VII.1:** Replace "The order of ρ_1 is D_4 is 4" by "The order of ρ_1 in D_4 is 4".

26. **Page 43, Example VII.2:** Replace the full stop after "What are the elements of finite order in $\mathbb{R}^*$" by a question mark.

27. **Page 45, paragraph before Example VII.9:** Replace "If there is no such positive integer that a has infinite order" by "If there is no such positive integer, then a has infinite order".

28. **Page 45, Example VII.9:** Replace the full stop in "How do we know this." by a question mark.

29. **Page 47, first paragraph after the heading:** Insert "be" in "we want H to be a group".

30. **Page 49, Example VIII.10:** Insert "a" in "Hence W is not subgroup of $\mathbb{R}^2$".

31. **Page 52, first sentence after Figure VIII.5:** Replace "Let's check that this is indeed a subgroup of V_Π" by "Let's check that V_Π is indeed a subgroup of $\mathbb{R}^3$".

32. **Page 53, end of Example VIII.17:** The question "Can you find a finite subgroup of $\mathbb{C}^*$ that isn't a subgroup of $\mathbb{S}$?" is never explicitly answered in the notes. Unless it is intended as a cliffhanger, it would be good to return to it (the answer is "no"; indeed, if α lies in a finite subgroup of $\mathbb{C}^*$, then $\alpha^n = 1$ for some $n > 0$, so $|\alpha|^n = 1$ and hence $|\alpha| = 1$).

33. **Page 54, proof of Theorem VIII.5:** Insert "is" in "It usual when proving an 'if and only if' statement ...".

34. **Page 56, opening paragraph:** Insert "a" in "This is group where the operation is multiplication of matrices".

35. **Page 56, paragraph before the definition of $\mathrm{SO}_2(\mathbb{R})$:** Insert "we" in "if compose two rotations". In footnote 1, replace "a subgroup of a something" by "a subgroup of something".

36. **Page 58, Example VIII.30:** Replace "Examples of a non-trivial subgroups" by "Examples of non-trivial subgroups".

37. **Page 59, Example VIII.34:** Insert "us" in "Lagrange's Theorem tells us that the order of U_2 must divide the order of U_4".

38. **Page 62, Example IX.3:** Replace "$\mathbb{Z}/m\mathbb{Z}$" by "$\mathbb{Z}/6\mathbb{Z}$" twice in this example, since the displayed table is specifically for the six residue classes modulo 6.

39. **Page 64, Theorem IX.12:** Insert "of" in "The order g divides the order of G".

40. **Page 68, Exercise X.3:** Replace "$\{1, Z, \ldots, Z^5\}$" by "$\{I_2, Z, \ldots, Z^5\}$". The identity in this matrix group is I_2, not the scalar 1.

41. **Page 68, Exercise X.4:** Replace "cylic" by "cyclic".

42. **Page 70, Exercise XI.4:** Replace "In otherwords" by "In other words".

43. **Page 71, Example XI.7:** Replace "One convenient way of a specifying a line" by "One convenient way of specifying a line".

44. **Page 72, Example XI.7:** Insert "is" in "which in L". More importantly, replace "$-\mathbf{v}_1 = (-t_1)\mathbf{v}_1$" by "$-\mathbf{v}_1 = (-t_1)\mathbf{v}$", since $\mathbf{v}_1 = t_1\mathbf{v}$.

45. **Page 73, Example XI.9:** Insert "the" in "one of things you'll look at".

46. **Page 75, proof of Lemma XI.15:** Replace "In otherwords" by "In other words". Later, replace "By we *can* say multiply both sides" by "But we *can* multiply both sides".

47. **Page 76, Example XI.18:** Insert "at" in "There we looked the cosets of the circle subgroup".

48. **Page 77, last line:** Replace "ecstacy" by "ecstasy".

49. **Page 80, Example XII.2:** Insert "the" in "the small fractional part of number".

50. **Page 80, Example XII.4:** Insert "if" in "if and only their constant terms are equal". In footnote 1, replace "writing f and g" by "writing g and h", since these are the two polynomials in the displayed formula.

51. **Page 81, Exercise XII.5:** Insert "be" in "for a and b to congruent modulo $\{0\}$".

52. **Page 81, Lemma XII.7:** Insert "and" after "Let $a \in G$".

53. **Page 81, definition of the quotient group:** Replace "We define the quotient group $(G/H, +)$ to the set" by "We define the quotient group $(G/H, +)$ to be the set".

54. **Page 82, Section XII.3:** Delete one occurrence of "and" in "and and simplify by subtracting an integer".

55. **Page 85, Lemma XII.16:** Replace "Let a, a', b, b' satisfying" by "Let a, a', b, b' satisfy". In the following paragraph, replace "representatitives" by "representatives" and insert "is" in "even though it defined in terms of those representatives".

56. **Page 85, paragraph before Lemma XII.17:** Delete the first occurrence of "addition" in "Are we sure addition that addition is well-defined ...".

57. **Page 88, definition of injections and surjections:** It is safer not to say that B is "the *range* of f". Many texts reserve the word "*range*" for the image

$$f(A) = \{f(a) : a \in A\},$$

which may be a proper subset of the codomain B. This distinction is particularly useful when defining surjectivity.

58. **Pages 88–89, discussion of f_2:** Replace "$f(1) \neq b$ and $f(2) \neq b$" by "$f_2(1) \neq b$ and $f_2(2) \neq b$".

59. **Page 91, Example XIII.11:** Replace $f_2^n \neq \mathrm{id}_A$ by $f_2^n \neq \mathrm{id}_{\mathbb{Z}}$ (or define $A = \mathbb{Z}$).

60. **Page 94, Subsection XIII.4.1:** Replace "One way of seeing this is convince ourselves" by "One way of seeing this is to convince ourselves". Later, replace "the permutation $\{1, 2, 3\}$" by "the permutation of $\{1, 2, 3\}$".

61. **Page 94, first paragraph of Section XIII.5:** In "It is not all obvious from this formula", replace "all" by "at all".

62. **Page 96, paragraph before Theorem XIII.23:** Delete one occurrence of "and" in "more concise and and more transparent", and replace "surprize" by "surprise".

63. **Page 96, Example XIII.24:** Replace "are repeatedly apply" by "and repeatedly apply".

64. **Page 98, proof of Lemma XIII.29:** Replace "Let σ and τ be disjoint cycle" by "Let σ and τ be disjoint cycles".

65. **Pages 98–99, proof of Theorem XIII.23:** When arguing that "This contradicts our assumption that a does not appear in the list $1, \rho 1, \ldots, \rho^{u-1}1$", you are tacitly using the fact that $\rho^k 1$ does appear in this list (because $\rho^u 1 = 1$ ensures that all of $1, \rho 1, \rho^2 1, \ldots$ appear in this list). Perhaps it would be good to be less tacit about it.

66. **Pages 100 and 103, the five-transposition decomposition of $(1,2,3,4)$:** The displayed decomposition uses the symbol 5, so it is an identity in S_n only for $n \geq 5$. State explicitly that $(1,2,3,4)$ is being viewed as an element of S_5 (or replace the example by a five-transposition decomposition using only $1, 2, 3, 4$).

67. **Page 106, Exercise XIII.51:** The puzzle promoter's name is **Sam Loyd**, not "Sam Lloyd".

68. **Page 107, property (iv) in the definition of a ring:** Insert "is" in "there an element, denoted by $-a$".

69. **Page 108, paragraph before Section XIV.2:** Replace "Observe, from properties (i)–(v), if ..." by "Observe from properties (i)–(v) that, if ...".

70. **Page 109, Example XIV.6:** The argument uses $a \cdot 0 = 0$ without having proved this ring identity. One can insert

$$a \cdot 0 = a(0+0) = a \cdot 0 + a \cdot 0;$$

cancelling $a \cdot 0$ in the additive group gives $a \cdot 0 = 0$. Similarly, $0 \cdot a = 0$. The printed conclusion $a = a \cdot 1 = a \cdot 0 = 0$ then follows.

It is probably best to state the identities $a \cdot 0 = 0$ and $0 \cdot a = 0$ as a lemma before or after this example, since their usefulness is not limited to trivial rings.

71. **Page 110, paragraph after the definition of a subring:** Insert "be" in "we want S to a ring", and replace "*the same two binary operations* that makes R a ring" by "the same two binary operations that make R a ring".

72. **Page 111, Example XIV.13:** With

$$\alpha = a_1 + a_2 i, \qquad \beta = b_1 + b_2 i,$$

the product should be

$$\alpha\beta = (a_1 b_1 - a_2 b_2) + (a_1 b_2 + a_2 b_1) i,$$

not

$$(a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1) i.$$

Consequently, the subsequent list of integers should be

$$a_1 + b_1, \quad a_2 + b_2, \quad -a_1, \quad -a_2, \quad a_1b_1 - a_2b_2, \quad a_1b_2 + a_2b_1.$$

The printed list has $-b_1$ in place of $-a_2$ and repeats the erroneous real part of the product.

73. **Page 112, continuation of Example XIV.15:** In the sentence beginning "Clearly $-\alpha, \alpha\beta$ are in S", replace

$$\text{"}-a, a+b, r, r+s \text{ are integers"} \quad \text{by} \quad \text{"}-a, ab, r, r+s \text{ are integers"}.$$

74. **Page 112, first paragraph of Section XIV.4:** Replace "we defined $\mathbb{R}^*, \mathbb{Q}^*, \mathbb{C}^*$ be removing" by "we defined $\mathbb{R}^*, \mathbb{Q}^*, \mathbb{C}^*$ by removing", and insert "a" in "We found that $\mathbb{R}^*$ is group".

75. **Page 112, definition of a unit:** Replace "An element u is called a unit" by "An element $u \in R$ is called a unit of R". This makes the ambient ring explicit before the inverse $v \in R$ is introduced.

76. **Page 114, Example XIV.25:** Replace "Taking determinants, are recalling" by "Taking determinants, and recalling".

77. **Page 115, Example XIV.26:** Insert "a" in "To be unit it is not enough for this matrix to be invertible". (Also perhaps add a comma after "unit".)

78. **Page 119, definition of a field:** This definition should also require that $1 \neq 0$ in F (so that the zero ring is not a field).

79. **Page 119, Example XV.4:** Replace "We want to show that existence of some $\beta \in \mathbb{Q}[i]$" by either "We want to show the existence of some $\beta \in \mathbb{Q}[i]$" or "We want to show that there exists some $\beta \in \mathbb{Q}[i]$".

80. **Page 121, Example XVI.1:** Insert "to" in "You don't have be very clever here!".

81. **Page 121, Example XVI.4:** Insert "time" (or remove "a") in "It would take us a very long to run through the elements ...".

82. **Page 123, definition of Euler's ϕ-function:** The notes previously introduced $\mathbb{Z}/m\mathbb{Z}$ only for $m \geq 2$, whereas this definition begins with $m \geq 1$. Either change the hypothesis here to $m \geq 2$, or extend the definition of $\mathbb{Z}/m\mathbb{Z}$ to $m = 1$ (this does not require any changes) and explain that its one-element unit group gives $\phi(1) = 1$.