MA3D5 Galois Theory
Samir Siksek
65-page PDF generated on 28 October 2019
`https://samirsiksek.github.io/siksek.github.io/teaching/gt/whole.pdf`
Errata and comments by Darij Grinberg

The page numbers below refer to the printed page numbers in the supplied PDF. (The cover is PDF page 1 and the first chapter begins on printed page 3.) This list is not claimed to be exhaustive. Items marked "substantive" correct a mathematical assertion or repair a proof gap. Items marked "pedagogical" are not necessarily errors, but seem likely to cause avoidable difficulty for a student meeting Galois theory for the first time. The remaining items are local corrections or clarifications.

Most of the errata below were found with assistance from GPT-5.6 Sol and have been verified (and occasionally reworded) by myself.

A. Corrections and comments

1. **Page 4, Section 2 and the final paragraph:** Replace "pleny" by "plenty". Replace "dip in to" by "dip into".

2. **Page 5, definition of an ideal:** Replace "alway commutative with 1" by "always commutative with 1".

3. **Page 6, definition of a quotient:** The display defining $r + I$ should end with a comma, not a full stop, since the sentence continues with "and the quotient $R/I \ldots$".

4. **Page 6, Example 8:** In the surjectivity argument, replace "$a, b \in \mathbb{Q}$" by "$a, b \in \mathbb{R}$". Not every complex number has rational real and imaginary parts.

5. **Page 6, Example 8:** Replace "In otherwords" by "In other words".

6. **Page 7, Example 10:** At the end of the computation in $\mathbb{C}[x]$, replace "$J \neq R[x]$" by "$J \neq \mathbb{C}[x]$".

7. **Page 7, paragraph after Example 12:** The subject of "Hence it is not maximal" is accidentally the polynomial $x^2 + 1$. Write instead: "Hence the ideal $(x^2 + 1)$ is not maximal".

8. **Page 10, proof of Theorem 18:** After "so $m_1 = 0$ in K or $m_2 = 0$ in K", I would add "(since a field has no zero divisors)".

9. **Page 10, definition of field generation:** Delete one copy of "the" from "We define the the **subfield**".

10. **Page 12, paragraph before Proposition 27:** "indeterminant" is a rather uncommon spelling of "indeterminate".

11. **Page 13, Example 30:** The roots of $(x^2+1)(x^2+2x+2)$ are

$$i, \quad -i, \quad -1+i, \quad -1-i,$$

not $i, -i, 1+i, 1-i$. The stated splitting field $\mathbb{Q}(i)$ is nevertheless correct.

12. **Page 13, Definition of a splitting field:** As stated, this makes no sense when f is the zero polynomial. A trivial case, but worth getting right...

13. **Page 13, Theorem 32:** Also replace "isomophism" by "isomorphism".

14. **Page 13, proof of Theorem 32:** The case $\deg f = 0$ is also worth briefly mentioning (it is trivial, of course).

15. **Page 15, proof of Lemma 37:** Replace "a basis for $K/\mathbb{F}_p$" by "a basis for K over $\mathbb{F}_p$". Here $K/\mathbb{F}_p$ denotes a field extension, not a quotient vector space.

16. **Page 17, Lemma 44(ii):** Replace "the minimal polynomial m over α" by "the minimal polynomial m of α over K".

17. **Page 17, proof of Lemma 44(ii):** After writing $m = f_1 f_2$, replace "$f_1(\alpha)f_2(\alpha) = f(\alpha) = 0$" by "$f_1(\alpha)f_2(\alpha) = m(\alpha) = 0$".

    In the next sentence, "the degree of f is minimal" should likewise be "the degree of m is minimal".

    Also replace "stricly" by "strictly".

18. **Page 19, proof of Theorem 50:** Replace "$0 \leq \deg(r) \leq d-1$" by "$\deg(r) \leq d-1$". The polynomial r can be 0, in which case its degree is $-\infty$.

19. **Page 20, first line:** A parenthesis is missing after "$\mathbb{Q}(\sqrt[3]{2}$".

20. **Page 22, calculation in the extended example:** In "Thus either $a = 0,\ b = \sqrt{\frac{6}{5}}$ or $b = 0,\ a = \sqrt{6}$", add a "$\pm$" sign in front of both square roots.

21. **Page 23, minimal polynomial of $\sqrt{5}+\sqrt{6}$:** The reference "from (iii)" has no appropriate antecedent. The relevant result is Theorem 50(ii): since $\mathbb{Q}(\alpha) = M$ and $[M:\mathbb{Q}] = 4$, the minimal polynomial of α has degree 4.

22. **Page 24, proof of Lemma 53:** Replace "$L(x)$" by "$L[x]$" (both times it appears).

23. **Page 27, Example 61:** Replace "Examples 48 and 77 before" by "Example 48 above and Example 77 below".

    More importantly for a first reader, explain the potentially surprising terminology: $x^p - t$ is squarefree as a polynomial in $K[x]$ (it has no repeated irreducible factor there), although over its splitting field it has one root with multiplicity p and is therefore inseparable.

24. **Page 27, Example 62:** Insert a full stop after "We continue Example 61".

25. **Page 28, discussion of formal derivatives and Lemma 68:** Replace "non-contant" by "non-constant" and "Let K has characteristic 0" by "Let K have characteristic 0".

26. **Page 32, proof of Lemma 73:** Replace "Now suppose let $f = m$" by "Now let $f = m$".

27. **Page 32, proof of Theorem 74:** Replace "the possibilities for each $\sigma(\alpha_i)$ is finite" by "the set of possibilities for each $\sigma(\alpha_i)$ is finite".

28. **Page 33, proof that Frobenius is an automorphism:** After "$\phi(\alpha^{-1}) = \phi(\alpha)^{-1}$", add "(for $\alpha \neq 0$)".

29. **Page 36, proof of Lemma 85:** In "$\psi(a) = \phi(a)$ for all $a \in K$", replace "K" by "K_1". Also replace "isomomorphism" by "isomorphism".

30. **Page 37, proof of Proposition 86:** In the second sentence, replace "$n = 1$" by "$n \leq 1$" (the trivial case $n = 0$ is also possible).

    When choosing the irreducible factor g, it is also cleanest to choose it monic before invoking Lemma 85.

31. **Page 37, §6, cyclotomic-field discussion:** Replace "These are the root of $x^p - 1$" by "These are the roots of $x^p - 1$".

32. **Page 39, proof of Lemma 88:** Replace "As any such σ is contained in $\mathrm{Aut}(L/K)$" by "As any such σ belongs to $\mathrm{Aut}(L/K)$". ("Contained in" can also mean "subset of", and in fact has been used in that exact meaning in the first paragraph of this proof.)

33. **Page 41, proof of Lemma 93:** Replace "$\sigma(A)$ has the same kernel at A" by "$\sigma(A)$ has the same kernel as A".

34. **Page 42, proof of Lemma 93:** Write "The rank of A" rather than "The $\mathrm{rank}(A)$".

35. **Page 43, Example 95:** Replace "This a continuation" by "This is a continuation".

36. **Page 46, proof of Theorem 101:** In the proof of (c) $\Longrightarrow$ (b), "Moreover f is separable" is not true in general: The product $f = m_1 \cdots m_n$ can have equal factors (since two of the α_i may have the same minimal polynomial) and thus have repeated roots. Take instead the product of the *distinct* polynomials among $m_1, \ldots, m_n$. It still has splitting field L and is separable.

37. **Page 47, proof of Theorem 102:** Replace "has distincts roots" by "has distinct roots".

    In the last paragraph, replace "So K' is contained in a splitting field K'' for f" by "So K' is a splitting field for f (since all p^n elements of K' are roots of the polynomial $x^{p^n} - x$, and the latter polynomial has degree p^n, so it cannot have any further roots). Thus, $K' \cong K$, since the splitting field is unique up to isomorphism". This renders the (rather murky) next two sentences unnecessary.

38. **Page 47, §4, paragraph defining the permutation representation:** "think of $\mathrm{Aut}(L/\mathbb{Q})$" should be "think of $\mathrm{Aut}\,(L/K)$".

39. **Page 48, Example 104:** Replace "Letting $\alpha_1 = \sqrt{p}, \ldots$" by "Let $\alpha_1 = \sqrt{p}, \ldots$".

40. **Page 49, Example 105:** The conventional abbreviation for "compare" is "cf.", not "c.f."; it would also help to identify the intended Section 2 more precisely.

41. **Page 51, proof of Theorem 106(iii):** Replace "$[L : K] = \#\,\mathrm{Aut}(L/K) = G$" by "$[L : K] = \#\,\mathrm{Aut}(L/K) = \#G$".

42. **Page 52, proof of Theorem 106(i):** In "L/L^H is Galois by part (i)", replace "(i)" by "(iii)".

43. **Page 52, proof of Lemma 108:** Replace "a basis for F/K" by "a basis for F over K". (Once again, the intended meaning is a field extension, not a quotient vector space.)

44. **Page 53, Completing the proof of the Fundamental Theorem:** The assertion that "$*\colon \mathcal{F} \to \mathcal{H}$ is a bijection" comes from part (i), not part (ii), of the Fundamental Theorem.

45. **Page 54, worked example:** Replace "ζ is the root of the irreducible $x^2 + x + 1$" by "ζ is a root of the irreducible polynomial $x^2 + x + 1$".

46. **Page 56, definition of a normal series:** Replace "we say call the chain" by "we call the chain".

47. **Page 56, Example 116:** Write, for example, "the two quotients $R/1 \cong C_4$ and $D_4/R \cong C_2$ are abelian"; the present sentence combines "with" and "are" ungrammatically.

48. **Page 57, proof of Proposition 120(i):** The two subnormal series "$1 \subseteq G_0 \subseteq \cdots \subseteq G_n = G$" and "$1 \subseteq H_0 \subseteq \cdots \subseteq H_n = H$" should have equality signs after "1", not subset signs. The further subnormal series "$1 \subseteq H_1 \cdots \subseteq H_n = H$" should be "$1 = H_0 \subseteq \cdots \subseteq H_n = H$".

49. **Page 57, proof of Proposition 122:** In the first paragraph of the proof, "f is separable" is false in general: Even in characteristic zero, the product $f = m_1 \cdots m_n$ need not be separable if some m_i coincide. Replace it by the product of the distinct minimal polynomials among the m_i. The splitting field is unchanged and the resulting polynomial is separable.

50. **Page 57, proof of Proposition 122:** Replace "Let M be the splitting field of f over K" by "Let M be a splitting field of f over K that contains $K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ as a subfield" (such a splitting field indeed exists, since $\alpha_1, \alpha_2, \ldots, \alpha_n$ are roots of f already). This is what allows you to conclude afterwards that "M contains the α_i and K".

51. **Page 58, proof of Proposition 122:** Replace "Fundamental Theorem of Galois Theorem" by "Fundamental Theorem of Galois Theory".

52. **Page 58, proof of Proposition 122:** Replace the displayed equation

$$\gamma_i^{r_n} = \sigma_i(\alpha_n^{r_n}) = \alpha_n^{r_n} \in F$$

by

$$\gamma_i^{r_n} = \sigma_i(\alpha_n^{r_n}) \in \sigma_i(F) = F.$$

(There is no reason why $\sigma_i(\alpha_n^{r_n})$ must equal $\alpha_n^{r_n}$.)

53. **Page 58, proof of Lemma 123:** Replace "ζ^{a+b}" by "ζ^{ab}". (On the other hand, the additive exponent in Lemma 124 is correct because there the automorphisms fix ζ and multiply $\sqrt[p]{\alpha}$ by a power of it.)

54. **Page 59, proof of Proposition 126:** The assertion that L/M is radical deserves one line of justification: If $K = L_0 \subseteq \cdots \subseteq L_n = L$ is a radical tower, then

$$M \subseteq ML_1 \subseteq \cdots \subseteq ML_n = L$$

is a radical tower after repetitions are removed.

55. **Page 59, proof of Corollary 127:** Replace "By definition of soluble polynomial" by "By the definition of soluble by radicals".

    Incidentally, "soluble by radicals" and "soluble in radicals" are used synonymously, but only the first has been defined.

56. **Page 60, proof of Lemma 130:** With the usual right-to-left composition convention,

$$(a, c, d, e)^2 (a, b) = (a, b, d)(c, e),$$

not $(a,d)(b,c,e)$. Both permutations have order 6, so the order argument survives.

57. **Page 60, same proof:** From $60 \mid \#G$ and $G \leq S_5$ one obtains $\#G \in \{60, 120\}$. To conclude that $G = A_5$ or S_5, add the standard fact that A_5 is the unique subgroup of index 2 in S_5 (or prove the needed special case).

58. **Page 60, proof of Theorem 131:** It is not immediately obvious that the polynomial $f = 2x^5 - 10x + 5$ is irreducible. One way to prove it is using Eisenstein's criterion at 5. Also, the existence of a 5-cycle in $\mathrm{Aut}(L/\mathbb{Q})$ follows from Cauchy's theorem, since $5 \mid \#\mathrm{Aut}(L/\mathbb{Q})$ and since the only permutations of order 5 in S_5 are 5-cycles.

59. **Page 62, Exercise 133:** Replace "non-colinear" by "non-collinear".

60. **Page 62, proof of Lemma 135:** Replace "rearragned" by "rearranged".

61. **Page 63, proof of Lemma 135:** Replace "the intersection of a non-parallel lines" by "the intersection of two non-parallel lines".

62. **Page 64, proof of Theorem 137:** There are two intersections of the line OD with the unit circle. Specify that P is the one on the ray $\overrightarrow{OD}$.

63. **Page 64, proof of Theorem 137:** Replace "$[K : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}]$" by "$[K : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$". This is the value used in the next equality.

64. **Page 64, proof of Theorem 137:** For a less-prepared reader, maybe also justify the final irreducibility assertion: by the rational-root test, $8x^3 - 6x - 1$ has no rational root, and a cubic over $\mathbb{Q}$ with no rational root is irreducible.

65. **Page 65, proof of Theorem 138:** Theorem 136 is stated for the field generated by one constructible point, whereas the proof applies it directly to $L = \mathbb{Q}(P, Q)$. Explain that the construction sequences for P and Q can be combined into one sequence; the proof of Theorem 136 then gives $[\mathbb{Q}(P, Q) : \mathbb{Q}] = 2^r$. Alternatively, state the corresponding finite-set version of Theorem 136.