Computational Algebra
Willem de Graaf
`https://degraaf.maths.unitn.it/algnotes/compalg.pdf`
version of 12 September 2022
Errata and addenda by Darij Grinberg

***

The following is a list of errors and comments to the notes "Computational Algebra" by Willem de Graaf in the version of 12 September 2022. The numbering of the pages corresponds to the page numbers on top of the pages (not the PDF page numbering, which differs by 4).

7. Errata

- **page 1:** "computatonal" $\to$ "computational".
- **page 1:** "Fanally" $\to$ "Finally".
- **page 10, Lemma 1.1.22:** Replace "e" by "and" on the first line of the lemma.
- **page 11, proof of Theorem 1.1.24:** In the last paragraph of the proof, after "hence $\mathrm{LM}(r)$ lies in J", add "(if $r \neq 0$)". A similar change is needed in the next sentence.
- **page 11, Lemma 1.1.29:** Replace "$g \in G$" by "$g \in G \setminus \{0\}$".

  Likewise, in the proof of the lemma, remove 0 whenever leading monomials are discussed.
- **page 13, Lemma 1.1.32:** The chain of inequalities

  $$\mathrm{LM}(f) = \mathrm{LM}(h_1 g_1) > \mathrm{LM}(h_2 g_2) > \cdots > \mathrm{LM}(h_s g_s)$$

  at the end should only be imposed if $s \neq 0$ (because in the case $f = 0$, there is no such thing as $\mathrm{LM}(f)$).
- **page 15, Lemma 1.1.37:** In "$\mathrm{LM}(u) < \mathrm{LM}(f)$ and $\mathrm{LM}(v) < \mathrm{LM}(g)$" it would be good (particularly with regard to how the lemma is being applied later on) to be explicit about the case when u or v is zero: Namely, we agree to consider the (normally undefined) "leading monomial" $\mathrm{LM}(0)$ to be smaller than any actual monomial. This is analogous to the convention that the "maximum" of an empty set of integers is $-\infty$.

- **page 15, Lemma 1.1.37:** The meaning of "reduces to 0" is a bit murky: It could mean either "reduces to 0 in one particular execution of the division-with-remainder algorithm" or "reduces to 0 in each execution of the algorithm". Fortunately, in this particular situation, both interpretations are valid (since the proof shows that the division algorithm can only proceed in one way – there is never a choice of f_i).

- **page 15, Lemma 1.1.38:** The meaning of "reduces to 0" is again a bit murky. Again, both possible interpretations ("reduces to 0 in one particular execution of the division-with-remainder algorithm" and "reduces to 0 in each execution of the algorithm") are valid.

- **page 16, proof of Lemma 1.1.38:** At the end of the first sentence, add "and $c_1 = \operatorname{LC}(f)$ and $c_2 = \operatorname{LC}(g)$, so that $\operatorname{LM}(r_1) < \operatorname{LM}(f)$ and $\operatorname{LM}(r_2) < \operatorname{LM}(g)$". (Here we again understand the "monomial" $\operatorname{LM}(0)$ to be smaller than any actual monomial.)

- **page 19, between Lemma 1.2.5 and Lemma 1.2.6:** In "$\operatorname{ev}_{a_1,\ldots,a_s}(f) = f(a_1,\ldots,a_s,x_{k+1},\ldots,x_n)$", replace "$x_{k+1}$" by "$x_{s+1}$".

- **page 27, proof of Theorem 1.2.23:** It's worth explaining why "the degree of $u_{i_k} f_{i_k}$ has to exceed $\sum_{i=1}^{n} (t_i - 1)$". Namely, the polynomial $u_{i_k} f_{i_k}$ is the nonzero term u_{i_k} multiplied by the polynomial $f_{i_k} = \prod_{s \in T_{i_k}} \left(x_{i_k} - s\right) \in \operatorname{span}\left(x_{i_k}^0, x_{i_k}^1, \ldots, x_{i_k}^{t_{i_k}}\right)$. Hence, if the monomial $x_1^{t_1-1} \cdots x_n^{t_n-1}$ occurs in this polynomial $u_{i_k} f_{i_k}$, then the monomial $x_1^{t_1-1} \cdots x_n^{t_n-1}$ must be u_{i_k} (more precisely, the monomial in u_{i_k}, without the coefficient, but let's ignore the coefficient for now) multiplied by some power $x_{i_k}^r$ of x_{i_k}. That is, up to scalar multiple, we have $x_1^{t_1-1} \cdots x_n^{t_n-1} = u_{i_k} x_{i_k}^r$ for some $r \in \mathbb{N}$. By comparing degrees in this equality, we conclude that $\sum_{i=1}^{n} (t_i - 1) = \deg u_{i_k} + r$. On the other hand, by comparing the exponent of x_{i_k} in $x_1^{t_1-1} \cdots x_n^{t_n-1} = u_{i_k} x_{i_k}^r$, we obtain $r \leq t_{i_k} - 1$, so that $t_{i_k} > t_{i_k} - 1 \geq r$.

  But the monomial $u_{i_k} x_{i_k}^{t_{i_k}}$ (again, ignoring the coefficient in u_{i_k}) must also occur in $u_{i_k} f_{i_k}$ (since $x_{i_k}^{t_{i_k}}$ occurs in f_{i_k} with coefficient 1), and has degree $\deg\left(u_{i_k} x_{i_k}^{t_{i_k}}\right) = \deg u_{i_k} + \underbrace{t_{i_k}}_{>r} > \deg u_{i_k} + r = \sum_{i=1}^{n} (t_i - 1)$. Thus, the degree of $u_{i_k} f_{i_k}$ has to exceed $\sum_{i=1}^{n} (t_i - 1)$.

  (Also, the use of the letter k for an integer here is somewhat confusing, since k already stands for the base field.)

- **page 30, Exercise 2:** Replace "$f_2 = z^2 - 1$" by "$f_3 = z^2 - 1$".
- **page 32, Exercise 10 (b):** Replace "with respect to $<_l$" by "with respect to $<$".
- **page 37, start of §2.2.2:** "similars idea" should be "similar ideas" or "a similar idea".
- **page 40, proof of Lemma 2.2.7:** Remove the comma before "is equal to x" (in the last sentence).
- **page 41, Remark 2.2.10:** The inequalities "$c_i > c_{i-1} > \cdots \geq 1$" are not entirely correct; e.g., it can happen that $c_1 = c_0 = 1$. However, the recursion $c_i = a_i c_{i-1} + c_{i-2}$ with $a_i \geq 1$ and $c_0, c_1 \geq 1$ yields that $c_i \geq c_{i-1} + 1$ for each $i \geq 2$, and thus the sequence $(c_0, c_1, c_2, c_3, \ldots)$ is strictly increasing at least starting with the c_1 term; and this is enough for the argument you are making.
- **page 42, proof of Theorem 2.2.11:** "the claim halds" $\to$ "the claim holds".
- **page 44, Example 2.2.18:** Replace "$x_0 - a_1$", "$x_1 - a_2$" and "$x_2 - a_3$" by "$x_1 - a_1$", "$x_2 - a_2$" and "$x_3 - a_3$".
- **page 45, Divertimento:** Replace "$s > 1$" by "$s \geq 1$" (twice).
- **page 45, Divertimento:** Replace "$x_i = a_1 + \dfrac{1}{x_{i+1}}$" by "$x_i = a_i + \dfrac{1}{x_{i+1}}$".
- **page 45, Divertimento:** In the displayed equation "$x_{ks} = a_{ks} + \dfrac{1}{x_1} = a_1 + \dfrac{1}{x_1}$", the "$a_1$" should probably be "$a_s$".
- **page 47, Remark 2.2.21:** "But then $f'(\alpha) = (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)$" should be "But then $f'(\alpha) = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)$".
- **page 61, Lemma 3.1.2:** Actually, this holds even if we don't require I to be nonzero. But the case $I = 0$ requires a (trivial) extra argument in the proof.
- **page 62, Theorem 3.1.8:** Add a requirement that f is nonzero.
- **page 63, proof of Corollary 3.1.9:** "h_2 divides h_2" should be "h_2 divides r".
- **page 69, proof of Lemma 3.4.2:** "we write $\overline{f}$" should be "we write $\overline{h}$".
- **page 73, Lemma 3.4.9:** The equality claimed here should be replaced by

$$||(x - a)h|| = ||(\overline{a}x - 1)h||.$$

This way, the problem of $\overline{a}^{-1}$ being undefined when $a = 0$ is no longer present. And of course, the last two lines of the proof become unnecessary with this reformulation.

- **page 73, proof of Lemma 3.4.9:** Remove the period after "$= \sum |\overline{a} h_{i-1} - h_i|^2$" (since the "Because" that follows it is actually explaining this computation).

- **page 74, proof of Theorem 3.4.10:** As stated, this argument works only if $a_1, a_2, \ldots, a_t$ are nonzero (since otherwise, some a_j^{-1} don't exist). But this restriction can be lifted while simplifying the proof as follows:

  Follow your argument until $f = f_n \prod_{i=1}^{s} (x - b_i) \prod_{j=1}^{t} (x - a_j)$. Then conclude that

$$\begin{aligned} ||f|| &= \left|\left| f_n \prod_{i=1}^{s} (x - b_i) \prod_{j=1}^{t} (x - a_j) \right|\right| \\ &= \left|\left| f_n \prod_{i=1}^{s} (x - b_i) \prod_{j=1}^{t} (\overline{a_j} x - 1) \right|\right| \end{aligned}$$

  by t-fold application of Lemma 3.4.9. But each polynomial h satisfies $||h|| \geq |h(0)|$ (since $||h||$ is the Euclidean length of the vector whose coordinates are the coefficients of h, whereas $h(0)$ is the 0-th coordinate of this vector). Thus,

$$\begin{aligned} &\left|\left| f_n \prod_{i=1}^{s} (x - b_i) \prod_{j=1}^{t} (\overline{a_j} x - 1) \right|\right| \\ &\geq \left| f_n \prod_{i=1}^{s} (0 - b_i) \prod_{j=1}^{t} (\overline{a_j} 0 - 1) \right| = \left| f_n \prod_{i=1}^{s} b_i \right| = |f_n b_1 b_2 \cdots b_s| . \end{aligned}$$

  Thus,

$$||f|| = \left|\left| f_n \prod_{i=1}^{s} (x - b_i) \prod_{j=1}^{t} (\overline{a_j} x - 1) \right|\right| \geq |f_n b_1 b_2 \cdots b_s| .$$

  Now continue as you do.

- **page 75, Example 3.4.13:** In "let $f = x^4 + 2x^3 - 3x^2 - 4x + 1$", replace the "$+1$" by "$-1$".

- **page 76, The algorithm:** In "If for all S, $f_S \neq g_S h_S$ then f is irreducible", replace "f_S" by "f".

- **page 82, Lemma 4.2.5:** This needs a requirement that $y \neq 0$.

- **General:** Some of the material here is worth reordering. In Lemma 1.2.5 and in the proof of Lemma 1.2.26, you are using the existence of the gcd of two univariate polynomials, which is proved in Lemma 3.1.3. Maybe Section 3.1 should be put at the very beginning of the notes?