Errata and comments on the version of 22 March 2005 of "Catalan's Conjecture"
by René Schoof,
Gabor Wiese, 26. Juli 2006

1 Introduction

- 3rd line of the proof of the main theorem. Add "by Exercise 1.1" after "prime numbers".
- 10th line of the proof of the main theorem. Add "by Exercise 1.2" after "$p \equiv 1(\mod q^2)$".

2 The case "$q = 2$"

- Exercise 2.1 is even true for a factorial ring, not only a principal ideal domain. The most natural proof seems to be to use unique factorisation anyway.

3 The case "$p = 2$"

- In the statement of Lemma 3.3 x and y have to be assumed non-zero.
- 7th line of the proof of Lemma 3.3. Add "by Exercise 3.2" after "is positive".
- In line 8 of the proof of Lemma 3.3, I do not see why we may assume $b > 0$, since b seems to be fixed by the equation $x + 1 = 2b^q$ and x may not be replaced by $-x$, as such a choice had already been made in the first line of the proof. But we do not need that. It is elementary to see that a and b have the same sign, namely the sign of $x - 1 = 2^{q-1}a^q$. If that sign is positive, the trick in the text yields $a \geq b - 1/2$. If it is negative, one gets $-a \geq -b + 1/2$. A contradiction follows just as in the text.

4 The non-trivial solution

- p. 12, l.-6. Add "by Exercise 4.2" after "strictly smaller than $[k/3]$".
- 4th line of the proof of Proposition 4.2. "Exercise 3.4" must read "Exercise 6.4".
- The formula for the binomial coefficient of Exercise 4.1 is wrong: The last minus sign in the numerator has to be a plus.

- Exercise 4.3 is the same as Exercise 4.1.
- Exercise 4.2: Replace “strictly larger” by “strictly smaller”.
- In Exercise 4.5 replace “$1 + 2^{1/3}$” everywhere by “$1 - 2^{1/3}$”.
- It is possible to do without any 3-adic numbers throughout. In Proposition 4.1 one can distinguish two cases: $n \geq 0$ and $n < 0$. For $n \geq 0$ one can keep the present proof, but all series are only finite sums and the issues of convergence etc. vanish. The case $n < 0$ is even easier. By verification one checks that the inverse of η is given by $1 + 2^{1/3} + 4^{1/3}$. Induction directly gives that all coefficients in the representation as $a + b2^{1/3} + c4^{1/3}$ of all $(1 + 2^{1/3} + 4^{1/3})^n$ for $n \geq 1$ are positive (non-zero). That settles the negative powers of η.

5 Runge’s method

Not treated in the seminar.

6 Cassel’s Theorem

- Throughout “Exercise 3.4” must read “Exercise 6.4”.
- In Exercise 6.4 assume that $|x| < |y|$ (at least when n is even). Otherwise for even n one has the counter example $y = -x$ (noticed by Florian Klössinger).
- Exercise 6.3. Replace $a \equiv 1 \mod q$ by $a \equiv -1 \mod q$. Add that q must be an *odd* prime.
- Statement of Proposition 6.1. Maybe put an “and” after (i) to exclude the possibility of confusion.
- The discussion for $b < 0$ in the proof of Proposition 6.1 is wrong. In order to get a positive value, use $x = b^q$, while $x = b^q - 1$ must be used for a negative value. That is, one uses the same values as for $b > 0$.
- Last line on p. 21 “the expression”. Possibly repeat which expression.
- In the third line of the proof of Part (ii) of Proposition 6.1 replace “Exercise 6.2” by “Exercise 6.3”.

- In the last line but three of the proof of Part (ii) of Proposition 6.1, it seems that one cannot apply Exercise 3.4 (meaning 6.4) to conclude that $u \neq 1$. This, however, can be dealt with directly, using the standard telescoping sum trick.

- Statement of Lemma 6.2. The Taylor expansion is <u>around 0</u>.

- The comma after the first line of the first displayed equation in the proof of Lemma 6.2 must be deleted.

- Last line on p. 22 and first line on p. 23. Replace "Lemma 4.1" by "Lemma 5.1", "Exercise 5.4" by "Exercise 5.6" and "Exercise 5.3" by "Exercise 5.4(i)".

- Lines 4 and 5 of the proof of Theorem 6.3. Replace "Exercise 2.2" by "Exercise 3.3", replace "therefore" by "Exercise 2.2".

- p. 24, l. 2. (Noticed by F. Klössinger) That the denomiantors of the coefficients are equal to $q^{k+ord(k!)}$ does not seem to follow from Exercise 5.4, but rather from

$$\mathrm{ord}_p(k!) \leq \mathrm{ord}_p(\frac{p}{q}(\frac{p}{q}-1)\cdots(\frac{p}{q}-(k-1)))$$

  for all $p \neq q$.

- p. 24, l. 7. Replace "Exercise 5.2" by "Exercise 5.3(ii)".

7 An obstruction group

- Second paragraph. "We let E denote the group of p-units. It is..." Question: Is that a definition of E or a lemma (presupposing that one knows what p-units are)? A reformulation solves the ambiguity.

- Second paragraph. Exercise 7.2 could be quoted as a reference that $\mathbb{Z}[\zeta_p]$ is the ring of integers in $\mathbb{Q}_p$.

- p. 27, first line. Replace "Therefore" by "By Exercise 7.1".

- On Lemma 7.1. It could be stated explicitly that all groups involved are $\mathbb{F}_q$-vector spaces (some students did not find that obvious).

- Statement of Proposition 7.2. This is a very general remark, applying to most statements in most sections. Some students found it annoying that all proofs use $p \neq q$, but never say so. Of course, it has been proved before that for $p = q$ no non-trivial solution to Catalan's equation exists, so that the statements are perfectly correct.

- Proof of Proposition 7.2. The notation μ_p is standard, but has not been introduced.
- Proof of Proposition 7.2, third line. $\alpha = x - \zeta_p$???
- Page 27, bottom. The notation $M[q]$ should be explained.
- p. 27, l. -5: Replace in the formula $\iota(\zeta)_p$ by $\iota(\zeta_p)$.
- p. 27, l. -2: Add "by Exercise 7.4" after "is injective".
- p. 28, l. 4f: Exercise 7.3 is on something else. It has already been said before that the map $CL^+ \to CL$ is injective, so the statement $h_p = h_p^+ h_p^-$ is obvious.

8 Small p or q

- In this section, one tends to forget what assumptions are used, namely, (i) that there is a non-trivial solution (x, y, p, q) to Catalan's equation, and (ii) that $(x - \zeta_p)^{1-\iota}$ <u>is trivial</u>. These assumptions are used in Proposition 8.1 and Lemma 8.2, but only (i) is stated. Also, (ii) is an assumption and not a notation (Proposition 8.1).
- p. 30, l. -4: The term "cyclotomic unit" has not been introduced. It is not needed here. Maybe: "which is a unit. In fact, it is an example of what is called a cyclotomic unit".
- p. 30, l. -3: Stupid remarks. Abuse of notation: unit of a number field instead of unit of its ring of integers. Maybe, explain the "of course"?
- Statement of Lemma 8.2. Might the denominator in Part (ii) be equal to $24q$ instead of $24q^2$?
- The logic of the first paragraph of the proof of Lemma 8.2 is quite difficult to follow, in particular the choice of w and w'. Hence, replace in l. 8 of the proof "assume that it is" by "assume that w is" (the students misunderstood that part). w' is still w/α. It might be recalled that α is the α from p. 30.
- When doing the congruences $\mod \pi$ for α in the first paragraph of the proof of Lemma 8.2, one would like to use that α is integral, in some sense. It does not seem so clear that α is in $\mathbb{Z}[\zeta_p]$. However, using valuations one can see that it is in $\mathbb{Z}_p[\zeta_p]$.
- Line 6 of the proof of Lemma 8.2. Maybe better "π-adically very small" instead of "p-adically"?

- p. 31, l. -5: Since one is using $O(\mu^2)$, the $\ldots$ in this line are superfluous. Also, the notation $O(\mu^2)$ could be explained. Why not write $\mod (\mu^2)$? This should make sense, since all denominators are away from π.
- Possibly add at the end of the proofs of Parts (i) and (ii) of Lemma 8.2, why the lemma follows.
- p. 34, l. 4: "Exercise 7.3" instead of "Exercise 7.5".
- Exercise 8.1, second line: Replace "non" by "no".

9 The Stickelberger ideal

- Second line of section. Replace σ by σ_a.
- Statement (iii) of Lemma 9.1 is wrong (noticed by Tobias Schaffer and Christian Fahnenschreiber). It must correctly read $\Theta_i + \Theta_{p-i} = \Theta_p - N$. The proof has to be corrected accordingly.
- Proposition 9.2. It is refered to as "Corollary 9.2" in line -5 of p. 35. At the end of the statement $\Theta_2, \ldots$ should be removed.
- Line 4 of the proof of Proposition 9.2. One must use $i = \frac{p+1}{2}$ instead of $i = 1$ (noticed by Tobias Schaffer and Christian Fahnenschreiber).
- Theorem 9.3 (ii). "from" $\mapsto$ "form".
- p. 36, second paragraph. It could be refered to Section 13, when discussing characters.
- Line -4 of the proof of Theorem 9.3. Replace $\frac{p+1}{2}$ by $\frac{p-1}{2}$ (noticed by Tobias Schaffer and Christian Fahnenschreiber).
- p. 37 Captions of the tables. The coefficients $m_{i,a}$ and $n_{i,a}$ are exchanged, relative to previous usage.
- p. 37, l. -7: twice "only".
- p. 37, l. -5: "arbitrary" instead of "arbitary".
- Exercise 9.1(iii). Replace x by Θ.
- p. 39, l. 5: In the product, σ_a should be replaced by σ_a^{-1} (noticed by Alexander Oster).

- p. 39, l. 11: Replace $\mathbb{Z}[\Delta]$ by $\mathbb{Z}[G]$. Also replace “Lemma 9.1(i)” by “Lemma 9.1(ii)”. Moreover, replace $\mathfrak{l}^{p\Theta_i} = (\tau(\chi)^{(\sigma_i - i)p})$ by $\mathfrak{l}^{p\Theta_i} = (\tau(\chi)^{-(\sigma_i - i)p})$. Hence, also two lines below the formula must read $\mathfrak{l}^{\Theta_i} = (\tau(\chi)^{-(\sigma_i - i)})$. (All noticed by Alexander Oster).

10 The double Wieferich criterion

- Possibly mention in the proof of Theorem 10.2 and Theorem II that p and q can be taken to be distinct.

- First line of the proof of Theorem II. The reference is to Corollary 6.4, rather than Corollary 6.3.

- Third line of the proof of Theorem II. Replace “Exercise 10.1” by “Exercise 8.1”.

- p. 41, l. 8. In the displayed equation replace $H = \ldots$ by $H' = \ldots$.

11 The minus argument

- Both references to Corollary 6.3 on p. 42 should be to Corollary 6.4(iii).

- Possibly it could be mentioned that all absolute norms of $\mathbb{Q}(\zeta_p)$ are positive, since that is used.

- Is the proof of Lemma 11.2 not already finished after line 5 of page 43? One also does not seem to need the first line of the proof.

  First one shows that $\phi(\alpha)$ lies on the unit circle, and concludes, precisely as it is done, that $|\mathrm{Arg}(\phi(\alpha)) - \frac{2\pi k}{q}| \leq C$ with C the number in line 5 of p. 43. Now we have two numbers on the unit circle, namely $\phi(\alpha)$ and $e^{2\pi ik/q}$ whose radial distance (i.e. the length of the shortest arc on the unit circle joining the two) is less than or equal to C. But, the length of the shortest line segment joining the two is always shorter than the length of the shortest arc on the unit circle, giving even a stronger inequality (gaining a factor 2).

- The factor 2 gained in Lemma 11.2 is needed in the proof of Theorem III. It seems that one needs the inequality $|\phi(\alpha) - 1| < 2/q$ (and not $4/q$) to be able to conclude that 1 is the root of unity nearest to $\phi(\alpha)$ so that one has a contradiction to Proposition 11.3.

- In the proof of Proposition 11.5 “It is a well known combinatorial fact...”. Could that become an exercise?

- Proof of Lemma 11.6. Replace "Exercise 11.2" by "Exercise 11.4".
- Page 46, line 3. Replace "Moreover, we have..." by "Moreover, by Exercise 11.2 we have...".
- Last line but 3 of the proof of Theorem III. Replace "Exercise 11.2" by "Exercise 11.3", replace "than" by "then" and replace "$\xi = 1$ is the nearest..." by "1 is the nearest..." (in order to avoid confusion with $\xi_1 = \xi_2$).
- In Exercise 11.1. The first item should be labelled "(i)" and not "(ii)".
- In Exercise 11.4. Does it refer to Lemma 11.6 (instead of Lemma 11.4)?

12 The plus argument I

- Since it is used a lot (not only in the present chapter), it might be an idea to state as an exercise the (formal) Taylor expansion
$$(1+x)^\alpha = \sum_{k\geq 0} \binom{\alpha}{k} x^k.$$
- In the statement of Proposition 12.1 (iii) the final formula could also be expressed as $\frac{1}{q}||\Theta||$.
- Proposition 12.2. In Part (ii) there is $\mathbb{Q}(\zeta_p)^+$, before the $+$ was always inside the brackets. Of course, it's the same. The proof could be put as an exercise, as it makes the proof of Part (i) of Proposition 12.2 obvious.
- p. 48, l. -2. On a formal level the formula $\phi((1-t\zeta_p)^\Theta)$ does not make sense, since $t \in \mathbb{R}$ is arbitrary, but the source of ϕ is $\mathbb{Q}(\zeta_p^+)$. Of course, ϕ is applied to the power series $(1-T\zeta_p)^\Theta$ which is then evaluated with $T = t$.
- p. 49, l. 7. It might be helpful to the student to point out $G = G^+ \times \{1, \iota\}$, in order to be able to make the lift more explicit.
- Lemma 12.3. The statement could be a bit clearer on $\pm(1+\iota)\psi$. The proof shows that one can lift either $(1+\iota)\psi$ or $-(1+\iota)\psi$ (not both), the statement could possibly be misread that one can lift both.
- Third line of the proof of Lemma 12.3. It must read "lifts $-(1+\iota)\psi$ (the $-$ was missing).
- p. 49, l. -2. It must read "we can lift $\pm(1+\iota)\psi$" (the $\pm$ was missing).

- p. 51, l. 2. The statement $-\log|x| \leq (p-1)\log(q)$ is totally trivial, since the left hand side is negative and the right hand side is positive. Does one really not need more?

- p. 51, l.-13. Proposition 1.2 does not exist.

13 Semi-simple group rings

- p. 53, l. 14. The product runs over the Galois conjugacy classes of characters, not all characters. Same remark for p. 53, l. -6.

- p. 54, l. 4. The K_χ are others than on the previous page.

- Lemma 13.6. In the definition of E^+ in the statement of that lemma, there's a $+$ missing in $\mathbb{Q}(\zeta_p^+)$.

14 The plus argument II

- In all the section "Theorem I" must read "Theorem II".

- p. 55, l. 8. Corollary 8.3 must be 10.3.

- p. 55, l. 14. "Section 14" must be "Section 13".

- p. 55, l. 18. "Lemma 7.1" must be "Lemma 7.3".

- p. 55, l. 20. C is a Galois module generated by $1-\zeta_p$ over which ring? Since the definition was not given before, the statement should be unambiguous here.

- p. 56, l. 9. "Proposition 13.1" with a capital "P".

- p. 57, l. 5. "Theorem 12.3" must read "Theorem 12.4".

15 Thaine's Theorem

- Third line of the section. "$E+$" must be E^+. Moreover, E^+ probably ought to be the ι-invariant p-units (not only units).