ERRATA

On p. 18 l. 7, it should be '$\circ\psi$' instead of '$\psi\circ$'.

On p. 30, there is a mistake in the formula for the discriminant of a cubic. It should be

$$d(f) = a_1^2a_2^2 - 4a_1^3 - 4a_0a_2^3 - 27a_0^2 + 18a_0a_1a_2.$$

On p. 32, in Thm. 2.2.3, the last polynomial should be $X^2 + a_3X + (a_2 - r)$, as in the proof.

On p. 43, the expression for α^{-3} should be

$$\alpha^{-3} = x^8\kappa x^4\kappa^2x^2\kappa^3x,$$

with no $\sqrt[5]{\alpha}$'s.

In the second-to-last paragraph, it should read $M/\mathbb{Q} = M(\mu_5)^{C_4}/\mathbb{Q}$.

On p. 44, on line 9 from the bottom, the formula for s is wrong. s should be defined as the first-degree coefficient in the polynomial two lines above. The polynomial itself, as well as Thm. 2.3.5, is correct.

On p. 46, in Thm. 2.3.6 (LECACHEUX), there is an error in the polynomial: The degree-4 coefficient should be $t^2d - 2s - 17/4$.

On p. 47, in Thm. 2.3.7, there is an error in the definition of C: It should be $C = 5A^2 - B^2 + 36$, not $C = 5A^2 - B^2 + 3$.

On p. 56, the result about the non-existence of a generic C_8-polynomial over $\mathbb{Q}$ is mistakenly attributed to Lenstra. It is in fact due to Saltman, cf. [Sa1].

In the Remark on p. 189, it is stated that $\mathrm{PGL}_2(\mathbb{Q})$ contains no elements of order 4. This is not correct: The matrix

$$\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$$

is a counter-example. We are grateful to J.–P. Serre for pointing out this mistake.

The non-existence of one-parameter generic polynomials for D_4 and S_4 over $\mathbb{Q}$ can still be established easily a little later on, since both groups contain V_4, and therefore have essential dimension at least 2.

As for the cyclic group C_4 of order 4:

Lemma. *All elements in* $\mathrm{PGL}_2(\mathbb{Q})$ *of order* 4 *are conjugate.*

Proof. Let $\mathbf{A} \in \mathrm{GL}_2(\mathbb{Q})$, and assume that A has order 4 modulo $\mathbb{Q}^*$. Then $\mathbf{B} = \mathbf{A}^2$ has order 2: $\mathbf{B}^2 = a\mathbf{E}$ for some $a \in \mathbb{Q}^*$.

Any non-scalar 2×2 matrix is conjugate to a matrix of the form $\left(\begin{smallmatrix} 0 & * \\ 1 & * \end{smallmatrix}\right)$, and so we may assume

$$\mathbf{B} = \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix}.$$

With

$$\mathbf{A} = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$$

we then have

$$x^2 + yz = w^2 + yz = 0, \quad y(x+w) = a, \quad z(x+w) = 1,$$

from which we get $y = a/2x$, $z = 1/2x$ and $w = x$. Thus,

$$x^2 + yz = x^2 + \frac{a}{4x^2} = 0,$$

i.e.,

$$a = -4x^4.$$

Scaling $\mathbf{A}$ by $1/x$, we see that we may assume $a = -4$ and $x = 1$:

$$\mathbf{A} = \begin{pmatrix} 1 & -2 \\ \frac{1}{2} & 1 \end{pmatrix}.$$

□

Now assume the existence of a one-parameter generic polynomial $P(t, X)$ for C_4 over $\mathbb{Q}$. Then the C_4-extension $\mathbb{Q}(w)/\mathbb{Q}(w)^{C_4}$, where C_4 acts on w by $\sigma\colon w \mapsto (w-1)/(w+1)$, is obtained by specialising t, and since t is necessarily specialised in a transcendental element, we get from Roquette-Ohm that the splitting field for $P(t, X)$ over $\mathbb{Q}(t)$ is rational. And since, by the Lemma, there is essentially only one C_4-action on $\mathbb{Q}(w)$, we may assume the splitting field to be $\mathbb{Q}(w)$, with $\mathbb{Q}(w)^{C_4} = \mathbb{Q}(t)$.

Consider now the Linear Noether Extension $\mathbb{Q}(u, v)/\mathbb{Q}(u, v)^{C_4}$, where the action of C_4 is given by $\sigma\colon u \mapsto v \mapsto -u$. It is also obtained by specialising $P(t, X)$, and again t must specialise to a transcendental element, meaning that $\mathbb{Q}(w) \hookrightarrow \mathbb{Q}(u, v)$.

We have $\sigma^2\colon w \mapsto -1/w$, and this remains true in $\mathbb{Q}(u, v)$. Write

$$w = \frac{f(u, v)}{g(u, v)},$$

where $f, g \in \mathbb{Q}[u, v]$ have greatest common divisor 1. Then

$$f(u, v)f(-u, -v) = -g(u, v)g(-u, -v),$$

and therefore $f(-u, -v) \mid g(u, v)$ and $g(u, v) \mid f(-u, -v)$. Hence,

$$f(u, v) = cg(-u, -v)$$

for a $c \in \mathbb{Q}^*$, and

$$w = c\frac{g(-u, -v)}{g(u, v)}.$$

This gives us

$$\sigma^2 w = c\frac{g(u,v)}{g(-u,-v)} = \frac{c^2}{w},$$

and thus $c^2 = -1$. An obvious contradiction.

The conclusion is that there is no one-parameter generic polynomial for C_4 over $\mathbb{Q}$.

Remark. This argument works for any field K of characteristic $\neq 2$, provided $\sqrt{-1} \notin K$.