exam Advanced Algebraic Structures,
January 24th, 2022, 16:00–18:00 (CEST).

- *Put your name on every sheet of paper you intend to hand in.*
- *Please provide complete arguments for all of your answers. The exam consists of* 3 *problems. You obtain* 3 *points for free, and up to* 27 *points for the problems you are supposed to hand in. In this way you will score in total between* 3 *and* 30 *points; your final grade is obtained by dividing this by* 3.

(1) This is an exercise concerning "squares modulo 221". Note that $221 = 13 \times 17$, and although during this course we discussed Legendre symbols $\left(\frac{a}{p}\right)$ for any odd prime $p$, we did not introduce something like $\left(\frac{a}{221}\right)$. Nevertheless:
  (a) [3 points] Show that $\varphi\colon \mathbb{Z}/221\mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z}$ given by $\varphi(a \bmod 221) = \left(\left(\frac{a}{13}\right), \left(\frac{a}{17}\right)\right)$ is well-defined.
  (b) [1+2 points] with $\varphi$ as above, show that

$$\varphi(a \bmod 221) = (1,1) \Longleftrightarrow a \bmod 221 \text{ is in } (\mathbb{Z}/221\mathbb{Z})^\times \text{ and is a square.}$$

  (c) [3 points] Show that 3 mod 221 and 5 mod 221 in $(\mathbb{Z}/221\mathbb{Z})^\times$ are non-squares and that their product 15 mod 221 is a non-square as well.

(2) We consider the splitting field $K$ of $x^9 - 1$ over $\mathbb{Q}$.
  (a) [1 point] Show that $\sqrt{-3} \in K$.
  (b) [3 points] Show that only one field $M$ exists such that both $\mathbb{Q} \subset M \subset K$ and $[M : \mathbb{Q}] = 2$.
  (c) [2 points] Compute $[K(\sqrt{5}) : \mathbb{Q}]$.
  (d) [3 points] Explain why $K(\sqrt{5})$ is a Galois extension of $\mathbb{Q}$ with an abelian Galois group $\mathrm{Gal}(K(\sqrt{5})/\mathbb{Q})$.

(3) We consider $\mathbb{Q}$, the set of rational numbers with the usual addition $+$, as a module over $\mathbb{Z}$ in the natural way. So scalar multiplication $\mathbb{Z} \times \mathbb{Q} \to \mathbb{Q}$ is the usual multiplication $(n, r) \mapsto nr$.
  (a) [3 points] Show that $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Z})$ consists of the zero-map only (hint: if $f$ is such a homomorphism and $f(1) = n$ and $m \in \mathbb{Z}$ is nonzero, observe that $m \cdot f(\frac{1}{m}) = n$).
  (b) [3 points] Show that $\mathbb{Q}$ is not a free $\mathbb{Z}$-module. (For this, it might help to observe that in $\mathbb{Q}$ every element can be divided by any nonzero integer.)
  (c) [3 points] Is $\mathbb{Q}$ a projective $\mathbb{Z}$-module?