EXAM ADVANCED ALGEBRAIC STRUCTURES,
April 13th, 2022, 8:30–10:30 (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 Legendre symbols $\left(\frac{a}{p}\right)$ for an odd prime p. Specifically, we take $a \in \mathbb{Z}$ such that $a^2 \equiv -1 \bmod p$; such an a exists whenever the prime p is congruent to 1 modulo 4.

  (a) [1 point] Find one such a for $p = 13$ and compute $\left(\frac{a}{p}\right)$.

  (b) [2 points] Given a prime $p \equiv 1 \bmod 4$, show that *every* $a \in \mathbb{Z}$ with the property $a^2 \equiv -1 \bmod p$ yields the same value $\left(\frac{a}{p}\right)$.

  (c) [3 points] For arbitrary a and p as above, use $(1+a)^2 \bmod p$ to show that $\left(\frac{a}{p}\right) = \left(\frac{2}{p}\right)$.

  (d) [3 points] Use (c) to show that $\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \bmod 8; \\ -1 & \text{if } p \equiv 5 \bmod 8. \end{cases}$

(2) We consider the splitting field K of $x^{20} - 1$ over $\mathbb{Q}$.

  (a) [1 + 1 + 1 points] Show that each of the polynomials $x^2 + 1$, $x^2 - 5$, and $x^2 + 5$ is reducible in $K[x]$.

  (b) [3 points] Show that if an integer n has the property that $x^2 + n$ is reducible in $K[x]$, then either $|n|$ or $|5n|$ is a square (in $\mathbb{Z}$).

  (c) [3 points] Prove that $K(\sqrt{2})$ is a splitting field of $x^{40} - 1$ over $\mathbb{Q}$. (Hint: compare degrees and show an inclusion.)

(3) This problem concerns tensor products. If R, S are commutative rings and $f\colon R \to S$ a ring homomorphism, then one obtains the structure of an R-module on $(S, +, 0)$ by using the scalar multiplication $R \times S \to S$ given by $(r, s) \mapsto f(r) \cdot s$. If M is any R-module, then $S \otimes_R M$ is an S-module with scalar multiplication defined by $s \cdot (\sum s_j \otimes m_j) = \sum (ss_j) \otimes m_j$ (you don't need to prove these assertions).

  (a) [3 points] Given $f\colon \mathbb{Z} \to \mathbb{Q}$ the inclusion, and the $\mathbb{Z}$-module $M = \mathbb{Q}/\mathbb{Z}$, determine $\mathbb{Q} \otimes_{\mathbb{Z}} M$.

  (b) [3 points] For $A = \mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$, determine the dimension of the vector space $\mathbb{Q} \otimes_{\mathbb{Z}} A$ over $\mathbb{Q}$.

  (c) [3 points] Now take a prime number p and let $f\colon \mathbb{Z} \to \mathbb{F}_p$ be the canonical ring homomorphism. With B any $\mathbb{Z}$-module, show that $\mathbb{F}_p \otimes_{\mathbb{Z}} B \cong B/pB$.