HW 4: Elliptische Kurven II

- Hand in by January 13th.

Exercise 1. Prove or disprove:

1. If F is a field, $n \geq 1$ is an integer, $\alpha_1, \dots, \alpha_n \in F^\times$ are pairwise distinct, and $(c_1, \dots, c_n) \in F^n$ such that, for all $k \geq 1$,
$$c_1 \alpha_1^k + \ldots + c_n \alpha_n^k = 0,$$
then $c_1 = \ldots = c_n = 0$. [Hint: you might find the proof of the "independence of characters" VL4 useful.]
2. If M is a torsion-free abelian group and G is a finite abelian group acting trivially on M, then $\mathrm{H}^1(G, M) = 0$.
3. If M is an abelian group and G is a finite abelian group, then $\mathrm{H}^1(G, M)$ is finite.
4. If M is a finitely generated abelian group and G is a finite abelian group acting on M, then $\mathrm{H}^1(G, M)$ is finite.
5. There is a $\mathbb{Z}/2\mathbb{Z}$-module M such that all elements of $\mathrm{H}^1(\mathbb{Z}/2\mathbb{Z}, M)$ have order (precisely) three.
6. If $K \subset L$ is a Galois extension of fields and $\Omega \subset \mathrm{Gal}(L/K)$ is an open subgroup, then Ω is closed and of finite index.
7. If p is a prime number, then $\mathbb{Q}_p$ has precisely one quadratic extension (up to isomorphism).
8. If K is a number field and $A = O_K[x_1, \dots, x_n]$, then $A^\times$ is a finitely generated abelian group.
9. If p is a prime number, then the abelian group $\mathbb{Z}_p^\times$ is finitely generated.
10. The integral closure of $\mathbb{Z}$ in $\overline{\mathbb{Q}}$ is a Dedekind domain.
11. If ζ is a primitive 5-th root of unity in $\mathbb{C}$ and $K = \mathbb{Q}[\zeta]$, then $1 + \zeta$ is an element of $O_K^\times$ and the group generated by $1 + \zeta$ in $O_K^\times$ is of finite index.
12. There exist an uncountable field k and an elliptic curve E over k such that, for all $n \geq 1$, the group $E(k)/nE(k)$ is finite.

Exercise 2. Prove or disprove:

1. There are only finitely many $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves E over $\overline{\mathbb{Q}}$ which can be defined by a Weierstrass polyomial with integer coefficients and good reduction at 5.

2. There is an elliptic curve over $\mathbb{Q}$ with good reduction at all primes $p > 3$.

3. The elliptic curve E defined by $y^2 = x^3 + x + 1$ has good reduction outside 2 and 31, the torsion in $E(\mathbb{Q})$ is trivial, and the rank of $E(\mathbb{Q})$ is at least one.

Exercise 3. Find the group of rational torsion points on the elliptic curve E given by $y^2 = x(x-1)(x+2)$.

Exercise 4. Show (explicitly) that there is an elliptic curve E over $\mathbb{Q}$ such that

$$\mathrm{H}^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), E(\overline{\mathbb{Q}})[2])$$

is infinite. [Hint: Exercise 3.]

Exercise 5. For $a \in \mathbb{Z} \setminus \{0\}$ consider the elliptic curve E_a given by $y^2 = x^3 + a$. Show that $\#E(\mathbb{Q})_{tor}$ divides 6. [Hint: First try the case where $\gcd(a, 5) = 1$. To deal with the general case, prove that, for all $p \equiv 2 \mod 3$ with $p \not| a$, we have $\#\widetilde{E}(\mathbb{F}_p) = p + 1$.)