

4 Exercises - lecture 1 and 2

Exercise 4.1 (Quadratic extension of $\mathbf{Q}_p$). Show that

$$\mathbf{Q}_p^\times \simeq p^{\mathbf{Z}} \times \mathbf{Z}_p^\times.$$

Use this to deduce that if p is odd then

$$\mathbf{Q}_p^\times / (\mathbf{Q}_p^\times)^2 \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}.$$

What about $p = 2$?

Exercise 4.2. Show that the polynomial $f(T) = T^3 - 3T + 4$ has a unique solution in $\mathbf{Z}_7$ and no solutions in $\mathbf{Z}_5$ and $\mathbf{Z}_3$. How many are there in $\mathbf{Z}_2$?

Exercise 4.3. Let $K = \mathbf{Q}(\alpha)$ be the extension of $\mathbf{Q}$ that is obtained by adjoining a root α of the irreducible polynomial $T^4 - 17$.

- For $p = 2$ show that 3 is a root modulo 64 that can be lift to a root α over $\mathbf{Z}_2$.
- Deduce that $f(T) = (T - \alpha) \cdot (T + \alpha) \cdot (T^2 + \alpha^2)$ over $\mathbf{Z}_2[T]$.
- Show that $\mathbf{Q}_2$ does not contain a primitive 4-th root of unity and deduce that $(T^2 + \alpha^2)$ is irreducible.

Exercise 4.4 (Elliptic curves). Let

$$E : y^2 = x^3 - Ax - B$$

with $A, B \in \mathbf{Z}$. Let p be a prime number and $(x_0, y_0) \in \mathbf{Z}$ such that

- $y_0^2 \equiv x_0^3 - Ax_0 - B \pmod{p}$;
- $2 \cdot y_0 \not\equiv 0 \pmod{p}$ or $3 \cdot x_0^2 - A \not\equiv 0 \pmod{p}$.

Show that there exists $(\tilde{x}, \tilde{y}) \in \mathbf{Z}_p$ such that $\tilde{y}^2 = \tilde{x}^3 - A\tilde{x} - B$, i.e. $(\tilde{x}, \tilde{y}) \in E(\mathbf{Z}_p)$.

Exercise 4.5. Let $f(x, y, z) \in \mathbf{Z}[x, y, z]$ be a homogeneous polynomial. Let $(a, b, c) \in \mathbf{Z}^3$ be such that $(\bar{a}, \bar{b}, \bar{c}) \in \mathbf{Z}/p\mathbf{Z} = \mathbf{F}_p$ is a non-singular point of the curve $\{\bar{f} = 0\}$ over $\mathbf{F}_p$. Then, $(\bar{a}, \bar{b}, \bar{c})$ lifts to a point on the curve $C = \{f(x, y, z) = 0\}$ with coordinates in $\mathbf{Z}_p$.

Exercise 4.6. Prove that

$$f(T) = 3T^3 - \frac{6}{7}T^2 + \frac{3}{2}T + 5$$

is the product of two irreducible factors in each of $\mathbf{Q}_2[T]$ and $\mathbf{Q}_7[T]$, that it is irreducible in $\mathbf{Q}_3[T]$, and that it is the product of three linear factors in $\mathbf{Q}_5[T]$. How does it factor in $\mathbf{Q}[T]$?