Problem Sheet 2

Problem 1

It was shown on the previous sheet that $\mathbb{Z}[i]$ is a PID. This was used in the first lecture to prove that $X^2 + Y^2 = p$, $p \geq 2$ prime, has an integral solution if and only if $p \equiv 1, 2\ (4)$.

(a) Consider $n \geq 1$ with prime factor decomposition $n = 2^m \cdot p_1^{e_1} \cdots p_r^{e_r}$, with all p_i odd and $p_i \neq p_j$ for $i \neq j$. Extend the lecture's arguments to show that

$$X^2 + Y^2 = n \text{ solvable} \Leftrightarrow \big(e_i \text{ odd only if } p_i \equiv 1\ (4)\ \forall i\big).$$

(b) Given such n, what is the number of solutions?

Problem 2

Let $K \subseteq L \subseteq M$ be finite field extensions. Prove the following facts on traces, norms and characteristic polynomials.

(a) Trace and norm are transitive in the sense $\mathrm{Tr}_{M/K} = \mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L}$ and $N_{M/K} = N_{L/K} \circ N_{M/L}$.

(b) If $x \in K$, then $\mathrm{Tr}_{L/K}(x) = [L : K]x$ and $N_{L/K}(x) = x^{[L:K]}$.

(c) Let $T^n + a_1 T^{n-1} + \ldots + a_n \in K[T]$ be the characteristic polynomial of $x \in L$. Then

$$\mathrm{Tr}_{L/K}(x) = -a_1, \quad N_{L/K}(x) = (-1)^n a_n.$$

More generally,

$$a_i = (-1)^i \mathrm{Tr}\big(\varphi_x \wedge \ldots \wedge \varphi_x \mid \textstyle\bigwedge^i L\big).$$

Problem 3

Let K be a field. Every finite-dimensional commutative K-algebra A/K is endowed with the K-bilinear trace pairing

$$A \times A \longrightarrow K,\ (x, y) \mapsto \mathrm{Tr}_{A/K}(xy).$$

(a) Assume $A = L$ is a field extension of K which is *not* separable. Show that the trace pairing is degenerate.

(b) Prove further that the trace pairing is non-degenerate if and only if A is a product of separable extensions of K.

Problem 4

We would like to show that the ring of integers of $\mathbb{Q}(\sqrt{7}, \sqrt{10})$ is not generated by a single element, meaning it is not equal to $\mathbb{Z}[\alpha]$ for any α.

(a) Let $K/\mathbb{Q}$ be an extension of degree 4 such that $\mathcal{O}_K = \mathbb{Z}[\alpha]$ is generated by a single element. Show that $\mathcal{O}_K$ has at most 3 prime ideals that contain 3.

(b) Now let $K = \mathbb{Q}(\sqrt{7}, \sqrt{10})$ and set $\mathcal{O} := \mathbb{Z}[\sqrt{7}, \sqrt{10}]$, which is a subring of $\mathcal{O}_K$. Show that

$$\mathcal{O}/3\mathcal{O} \cong \mathcal{O}_K/3\mathcal{O}_K.$$

Hint: Compute $\mathrm{Disc}(1, \sqrt{7}, \sqrt{10}, \sqrt{7}\sqrt{10})$.

(c) Determine the prime ideals of $\mathcal{O}_K/3\mathcal{O}_K$ through (b) and finish the argument.