EXERCISES SET 3

1. Discriminant

1.– Supply the proof not given in class for the proposition: the discriminant
\( D \) of the module \( A \oplus A x \oplus \cdots \oplus A x^{n-1} \) (where \( x \) is an integral element over \( A \) whose minimal polynomial is a monic polynomial \( P(X) \in A[X] \) of degree \( n \)) is \( \prod_{i \neq j} (x_i - x_j) \) where \( x_1, \ldots, x_n \) are the roots of \( P \) in some algebraic closure of \( K \). (You can proceed as follows: By mimicking the argument seen in class to prove that \( D \) is not 0, show that \( D \) is the square of the determinant of the matrix \((x_j^i)_{i,j}\). Then compute a Vandermond determinant).

2.– The quantity \( \prod_{i \neq j} (x_i - x_j) \) when the \( x_i \)'s are the roots of a polynomial \( P \) is called the discriminant of the polynomial \( P \). Show that the discriminant is invariant by changing the polynomial by the change of variable \( X \mapsto X + a \). Compute the discriminant of the polynomial \( X ^ n + a X + b \).

3.– Prove that if \( L = K[x] \) is a separable extension, and \( P(X) \) is the minimal polynomial of \( x \), then the discriminant of \( P \) is \( N_{L/K}(P'(x)) \).

4.– With the notations of the above exercise, let \( A \) be a subring of \( K \) which is a Dedekind domain and assume that \( x \) is integral over \( A \). Show that if \( Q(X) \) is any polynomial in \( A[X] \) such that \( Q(x) = 0 \), then the discriminant of \( A[x] \) over \( A \) divides \( N_{K/Q}(Q'(x)) \). (hint: reduce to the case where \( A \) is principal and use that \( A[x] \) is an UFD).

5.– Let \( x \) be a root in \( \mathbb{C} \) of \( X ^ 3 + X + 1 = 0 \), and let \( K = \mathbb{Q}(x) \). Prove that \( \mathcal{O}_K = \mathbb{Z}[x] \).

6.– Let \( A \) a Dedekind domain, \( K \) its fraction field, \( L \) a finite separable extension of \( K \) of degree \( n \), \( B \) the ring of elements in \( L \) that are integral over \( A \), and \( M \) a free \( A \)-module of rank \( n \) of \( B \). Let’s call \( e_1, \ldots, e_n \) a basis of \( M \) and \( D \) the discriminant of \( M \) over \( A \) (considered as an element of \( K \) modulo a (squared) unit of \( A \)). Let \( x \in L \). Show that if \( \text{tr}(xe_i) \in A \) for \( i = 1, \ldots, n \), then \( Dx \in M \).

In particular, then \( DB \subset M \).

2. An example of a ring of algebraic integers without a primitive element

This is an adaption of an exercise of Pierre Samuel’s book “Théorie algébrique des nombres”.

Let \( p, q \) be two prime numbers greater than 3, \( p \neq q \), such that \( p^2 q \neq \pm 1 \) (mod 9). Let \( u = (p^2 q)^{1/3} \) and \( v = (pq^2)^{1/3} \).

1.– Show that \( K := \mathbb{Q}(u) = \mathbb{Q}(v) \) is a cubic field of degree 3. Show that \( u \in \mathcal{O}_K \) and \( v \in \mathcal{O}_K \). Let \( A \) be be the sub-\( \mathbb{Z} \)-module of \( \mathcal{O}_K \) generated by 1,
u, and v. Show that A has rank 3 (in others words, 1, u, and v is a Z-basis of A) and that A is a subring of $O_K$.

In the following questions 2 to 6 we aim to prove that $A = O_K$.

2.– Show that there is a prime ideal $q$ of $O_K$ such that $qO_K = q^3$ (in other words, $q$ is totally ramified in $K$ – use $u^3 = p^3q$), and similarly a prime ideal $p$ of $O_K$ such that $p^3 = pO_K$.

3.– Show that $A \cap q$ is the ideal of $A$ generated by $u$, $v$ and $q$. Show that the inclusion $A/(A \cap q) \subset O_K/q$ is an equality, and that $O_K = A + q$. Deduce that $O_K = A + qO_K$. Similarly, we have $O_K = A + pO_K$.

4.– Compute $(u+1)^3$ and $(u-1)^3$. Deduce that $3O_K$ is the cube of a prime ideal, and as in the above question, that $O_K = A + 3O_K$.

5.– Compute the discriminant $D$ of $A$ over $Z$. You should find $D = -27p^2q^2$.

6.– Using 3., 4., and 5., show that $O_K = A$.

Now we are ready to prove that there is no $x$ in $O_K$ such that $O_K = \mathbb{Z}[x]$.

By contradiction, assume there is such an $x$, and write $x = a + bu + cv$ with $a, b, c \in \mathbb{Z}$.

7.– Show that the discriminant of $O_K$ is $-27p^2q^2(b^3p - c^3q)^2$ (this is question is very computational, you may skip it if you wish. If you want to do it, show first that you can assume $a = 0$.)

8.– Deduce that $b^3q - c^3p = \pm 1$. But show that this equation has no solution if $q$ is not a cube modulo $p$. Find an example of $p, q$ satisfying the hypotheses made on them, and such that $b^3q - c^3p = \pm 1$ has no solutions. Hence $K = \mathbb{Q}(p^2q^{1/3})$ is such that $O_K$ cannot be written as $\mathbb{Z}[x]$ for some $x \in O_K$.

3. EQUATION $p = x^2 + dy^2$ – FIRST STUDY

Let $p$ be an odd prime number, and $d$ a positive integer which is prime to $p$.

1.– Show that $\left(\frac{d}{p}\right) \equiv d^{(p-1)/2} \pmod{p}$. In particular, $-1$ is a square mod $p$ if and only if $p \equiv 1 \pmod{4}$.

2.– Show that there exists $x, y \in \mathbb{Z}$, not both divisible by $p$, such that $p$ divides $x^2 + dy^2$ if and only if $\left(\frac{-d}{p}\right) = 1$.

We now want to investigate the more subtle question :

(1) When can $p$ be written as $x^2 + dy^2$ for some integers $x$ and $y$?

Note that the question can easily be reduced to the case when $d$ is square free (why?). So we assume that $d$ is square free below. Set $K = \mathbb{Q}(\sqrt{-d})$.

3.– Show that a necessary condition for (1) is that $\left(\frac{-d}{p}\right) = 1$, which is equivalent to the assertion : $p$ splits in $K$.
4.– Assume \( d \equiv 1 \pmod{4} \). Show that (1) has a positive answer if and only if there is a \( z \) in \( K^* \) such that \( p = N_{K/Q}(z) \). Deduce that a necessary and sufficient condition for (1) is \( p \) splits in \( K \), and if \( p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2 \), the ideals \( \mathfrak{p}_1 \) and \( \mathfrak{p}_2 \) are principal.

5.– In particular, deduce that a prime is a sum of two squares if and only if it is congruent to 1 mod 4 (or equal to 2).

6.– Give an example of prime \( p \) which is not of the form \( x^2 + 5y^2 \) but yet satisfies \( \left( \frac{-5}{p} \right) = 1 \).

4. **Miscellaneous**

1.– Can you formulate and prove a reciprocity law for the polynomial \( X^2 - 1 \) ? \( X^a - 1 \) ?

2.– Let \( L = \mathbb{Q}(\sqrt{5}, \sqrt{-1}) \).

   a.– Show that \( L \) is Galois over \( \mathbb{Q} \). Compute its Galois group.

   b.– Show that \( \mathcal{O}_K = \mathbb{Z}[\sqrt{-1}, \frac{1 + \sqrt{5}}{2}] \). (Hint: compute the discriminant of that ring over \( \mathbb{Z}[i] \).)

   c.– Show that the only primes of \( \mathbb{Q} \) that ramify in \( L \) are 2 and 5.

   d.– For \( l \) a prime number different from 2 and 5, calculate its Frobenius in \( \text{Gal}(L/\mathbb{Q}) \).

3.– Compute \( \left( \frac{1123}{234} \right) \).