

# Algebraic Number Theory

## Problem sheet 1

1. (2 points) Let  $p$  be an odd prime number, show that  $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ . (Hint: consider  $\zeta_8 + \zeta_8^{-1}$  and mimic the proof of quadratic reciprocity)
2. (2+1 points) Prove that  $\mathbb{Z}[\sqrt{5}]$  is not integrally closed. Deduce that it is not UFD.
3. (3 points) Let  $K = \mathbb{Q}[\sqrt[3]{2}]$ . Show that  $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{2}]$ .
4. (3 points) Let  $A \subseteq B$  integral domains and let  $\beta \in B$  be an invertible element. Show that each element in  $A[\beta] \cap A[\beta^{-1}]$  is integral over  $A$ . (Hint: For  $\alpha \in A[\beta] \cap A[\beta^{-1}]$  find a finitely generated  $A$ -submodule  $M \subseteq B$  such that  $\alpha M \subseteq M$ .)
5. (1+2+2 points) The goal here is to show that whenever  $R$  is an integrally closed domain then so is  $R[x]$ .
  - (a) Reduce the statement to showing that  $R[x]$  is integrally closed in  $K[x]$  where  $K$  is the field of fractions of  $R$ . (Hint:  $K[x]$  is contained in the field of fractions of  $R[x]$  and it is integrally closed.)
  - (b) Let  $f, g \in K[x]$  be *monic* polynomials such that  $fg$  lies in  $R[x]$ . Show that both  $f$  and  $g$  are in  $R[x]$ . (Hint: write both polynomials as a product of linear factors over a bigger field.)
  - (c) If  $f \in K[x]$  is the root of a monic polynomial of degree  $k$  with coefficients in  $R[x]$  then  $f + x^N$  is also the root of another monic polynomial  $g_N \in R[x][y]$  of degree  $k$  (in the variable  $y$ ). Increase  $N$  so that the constant term of  $g_N$  can be written as a product of two monic polynomials (in  $R[x]$ ) one of which is  $f + x^N$ .
6. (1 point) What is the trace and the norm of  $1 + \sqrt{2}$  in the extension  $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ ?
7. (2 points) Consider the extension  $\mathbb{Q}(i)/\mathbb{Q}$ . This has a Galois group isomorphic to  $\mathbb{Z}/2\mathbb{Z}$ , in particular it is cyclic. What is the norm of an element of the form  $a + bi$ ? What does Hilbert 90 tell us in this special case on Pythagorean triples?
8. (3 points) Let  $K$  be a field containing a primitive  $n$ th root of unity and  $L/K$  be a Galois extension with Galois group  $\text{Gal}(L/K) \cong \mathbb{Z}_n$ . Show that  $L = K(\sqrt[n]{\alpha})$  for some  $\alpha$  in  $K$ . (Hint: Use Hilbert's Theorem 90.)
9. (3 points) Let  $f(x) \in \mathbb{Z}[x]$  be an irreducible monic polynomial. Assume that the Galois group of the splitting field of  $f$  over  $\mathbb{Q}$  is abelian and there is an  $\alpha$  in  $\mathbb{C}$  such that  $f(\alpha) = 0$  and  $|\alpha| = 1$ . Show that all the other roots of  $f$  (in  $\mathbb{C}$ ) have absolute value 1.

10. (4 points) Let  $\alpha$  be an algebraic integer whose all Galois conjugates have absolute value 1. Prove that  $\alpha$  is a root of unity.
11. (3+3 points) Let  $K \leq L \leq M$  be finite extensions. Show that  $N_{M/K} = N_{L/K} \circ N_{M/L}$  and  $Tr_{M/K} = Tr_{L/K} \circ Tr_{M/L}$ .
12. (3 points) Let  $L/K$  be a non-separable extension. Show that  $Tr_{L/K}$  is identically 0. (Hint: using the transitivity of the trace reduce the problem to the case when you are adjoining the  $p$ th root of an element to a field  $K$  of characteristic  $p$ .)
13. (2+2+2+2+2 points) Let  $L/K$  be a Galois extension. The goal of this problem is to prove the normal basis theorem: There exists an  $\gamma \in L$  such that the elements  $\{\sigma(\gamma) \mid \sigma \in \text{Gal}(L/K)\}$  are linearly independent over  $K$  ie. they form a basis of  $L$  as a  $K$ -vector space (bases of this form are called *normal bases*).
  - (a) Let  $f(x) \in K[x]$  be a separable monic polynomial that splits over  $L$  as a product  $f(x) = \prod_{i=1}^n (x - \alpha_i)$ . Put  $g_i(x) := \frac{f(x)}{f'(\alpha_i)(x - \alpha_i)} \in L[x]$ . Verify (i)  $\sum_{i=1}^n g_i(x) = 1$  (partial fraction decomposition of  $1/f(x)$ ) and
 
$$(ii) \ g_i(x)g_j(x) \equiv \begin{cases} 0 \pmod{f(x)} & \text{if } i \neq j \\ g_i(x) \pmod{f(x)} & \text{if } i = j \end{cases}.$$
  - (b) Let  $L/K$  be a Galois extension as above and pick  $\alpha$  such that  $L = K(\alpha)$  and denote by  $f \in K[x]$  the minimal polynomial of  $\alpha$ . Put  $\text{Gal}(L/K) = \{\text{id} = \sigma_1, \dots, \sigma_n\}$  and  $\alpha_i = \sigma_i(\alpha) \in L$ . Let  $A \in L[x]^{n \times n}$  be the matrix with  $j$ th entry in the  $i$ th row being  $\sigma_i(\sigma_j(g_1(x))) \in L[x]$ . Using part (a) show that  $A^T A \equiv I \pmod{f(x)}$  (where  $I$  is the identity matrix).
  - (c) Assume  $K$  is infinite. Using part (b) show that there is a  $\beta \in K$  with  $\det(A(\beta)) = \det(\sigma_i \sigma_j(g_1(\beta)))_{i,j} \neq 0$ . In particular,  $\{\sigma_1(\gamma), \dots, \sigma_n(\gamma)\}$  is a normal basis for  $\gamma = g_1(\beta)$ .
  - (d) Assume  $K \cong \mathbb{F}_q$  is finite and let  $n = |L/K|$  be the degree. Use Dedekind's Lemma and the fact that  $\text{Gal}(L/K)$  is cyclic of order  $n$  generated by the Frobenius  $\text{Frob}_q$  to determine the minimal polynomial of  $\text{Frob}_q: L \rightarrow L$  as a  $K$ -linear map.
  - (e) Using the theorem of elementary divisors (or otherwise) show that  $L \cong K[x]/(x^n - 1)$  as modules over  $K[x]$  where  $x$  acts on  $L$  via  $\text{Frob}_q$ . Let  $\gamma \in L$  be the element corresponding to  $1 + (x^n - 1)$  under this isomorphism.