Algebraic Number Theory

Problem sheet 1

9th September 2015

1. (2 points) Let ε_p be a primitive pth root of unity. Verify the identity

$$(S :=) \sum_{j=0}^{p-1} \varepsilon_p^{j^2} = 1 + 2 \sum_{a \in \mathbb{F}_p, \left(\frac{a}{p}\right)=1} \varepsilon_p^a = \sum_{j=0}^{p-1} \left(\frac{j}{p}\right) \varepsilon_p^j .$$

   Show, moreover, that we have $S^2 = \left(\frac{-1}{p}\right) p$.

2. (2 points) Using the 8th roots of unity and the proof of quadratic reciprocity find a formula for the value of the Legendre symbol $\left(\frac{2}{p}\right)$.

---

3. (2+2 points) Prove that unique factorization domains (eg. $\mathbb{Z}$ and $K[x]$ where K is a field) are integrally closed, but $\mathbb{Z}[\sqrt{5}]$ is not. (Hint: Gauss' lemma.)

4. (3+3 points) Determine the integral closure of $\mathbb{Z}$ in $\mathbb{Q}[x]/(x^3-2)$ and in $\mathbb{Q}[x]/(x^3-x-4)$.

5. (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 $\alpha M \subseteq M$.)

6. (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 $f + x^N$.

---

7. (1 point) What is the trace and the norm of $1 + \sqrt{2}$ in the extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$?

8. (2 points) Consider the extension $\mathbb{Q}(i)/\mathbb{Q}$. This has a Galois group isomorphic to Z_2, 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 Pythgorian triples?

9. (3 points) Let K be a field containing a primitive nth root of unity and L/K be a Galois extension with Galois group $\mathrm{Gal}(L/K) \cong Z_n$. Show that $L = K(\sqrt[n]{\alpha})$ for some α in K. (Hint: Use Hilbert's Theorem 90.)

10. (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 α 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.

11. (4 points) Let α be an algebraic integer whose all Galois conjugates have absolute value 1. Prove that α is a root of unity.

12. (2+2 points) Let $K \leq L \leq M$ be finite separable extensions. Show that $N_{M/K} = N_{L/K} \circ N_{M/L}$. What if the extensions are not separable?

13. (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 pth root of an element to a field K of characteristic p.)

14. (1+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 $\{\sigma(\gamma) \mid \sigma \in \mathrm{Gal}(L/K)\}$ 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) $g_i(x)g_j(x) \equiv \begin{cases} 0 \mod (f(x)) & \text{if } i \neq j \\ g_i(x) \mod (f(x)) & \text{if } i = j \end{cases}$.

    (*b*) Let L/K be a Galois extension as above and pick α such that $L = K(\alpha)$ and denote by $f \in K[x]$ the minimal polynomial of α. Put $\mathrm{Gal}(L/K) = \{\mathrm{id} = \sigma_1, \dots, \sigma_n\}$ and $\alpha_i = \sigma_i(\alpha) \in L$. Let $A \in L[x]^{n\times n}$ be the matrix with jth entry in the ith row being $\sigma_i(\sigma_j(g_1(x))) \in L[x]$. Using part (a) show that $A^T A \equiv I \mod (f(x))$ (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 bases 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 $\mathrm{Gal}(L/K)$ is cyclic of order n generated by the Frobenius Frob_q to determine the minimal polynomial of $\mathrm{Frob}_q \colon L \to L$ 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 Frob_q. Let $\gamma \in L$ be the element corresponding to $1 + (x^n - 1)$ under this isomorphism.