MATHEMATICAL TRIPOS PART III (2017–18)

Algebraic Number Theory - Example Sheet 2 of 4 **C. Johansson**

1. Give an example of a discrete valuation ring A and a finite separable extension L of $K = \mathrm{Frac}(A)$ such that the integral closure B of A in L is not a DVR.

2. Let K be a complete DVF and let $M/L/K$ be finite separable extensions. Show that $f_{M/K} = f_{M/L}f_{L/K}$ and $e_{M/K} = e_{M/L}e_{L/K}$.

3. Let K be a local field and let $q = \#k_K$ be a power of p.

   (i) If K has characteristic p, show that $\mathcal{O}_K \cong \mathbb{F}_q[[T]]$ and hence that $K \cong \mathbb{F}_q((T))$ *(Hint: Consider the Teichmüller lifts).*

   (ii) If K has characteristic 0, show that K is a finite extension of $\mathbb{Q}_p$ *(Hint: Consider $\mathbb{Q} \subseteq K$ and show that $\mathbb{Q}_p \subseteq K$. To prove finiteness, you may use the following fact: If $M \subseteq K$ contains $\mathbb{Z}_p$ and is a finitely generated $\mathbb{Z}_p$-module, then M is closed in K).*

4. (Stronger versions of Hensel's Lemma) Let A be a complete DVR with valuation v and let $f(T) \in A[T]$ be a monic poynomial.

   (i) Suppose that there exists $x \in A$ such that $v(f(x)) > 2v(f'(x))$. Then there exists a unique $\alpha \in A$ such that $f(\alpha) = 0$ and $v(\alpha - x) > v(f'(x))$ *(Hint: Use the Newton–Raphson algorithm as in the proof of Hensel's Lemma in lectures).*

   (ii) Let π be a uniformizer of A and let k be the residue field of A. Suppose that the reduction $\overline{f}(T) \in k[T]$ admits a factorization $\overline{f}(T) = \overline{g}(T)\overline{h}(T)$ in $k[T]$ into monic, coprime polynomials. Then there exists monic polynomials $g(T), h(T) \in A[T]$, lifting $\overline{g}(T), \overline{h}(T)$ respectively, such that $f(T) = g(T)h(T)$ *(Hint: construct g and h modulo successive powers of π and take a limit).*

5. Let K be a complete DVF with valuation v and let $f(T) = a_0 + a_1T + \cdots + a_{n-1}T^{n-1} + T^n \in K[T]$. Let $\alpha_1, \ldots, \alpha_n$ be the roots of f in a splitting field L of f over K, and assume that L/K is separable. Let w be the unique valuation on L extending v. Prove that

$$f_r(T) = \prod_{i\,:\,w(\alpha_i)=r} (T - \alpha_i) \in K[T]$$

   for any $r \in \mathbb{R}$. Deduce that f has at least as many factors in $K[T]$ as there are line segments (distinct slopes) on its Newton polygon.

6. Let A be a complete DVR with uniformizer π and fraction field K. Let $f(T) = T^n + a_{n-1}T^{n-1} + \cdots + T_0 \in A[T]$ be a polynomial. Assume that K has characteristic 0, or that f is separable.

(i) (Eisenstein's criterion) Assume that $\pi \mid a_i$, $i = 0, \ldots, n-1$ and $\pi^2 \nmid a_0$. Reformulate this condition in terms of the Newton polygon of f and show that f is irreducible in $K[T]$.

(ii) Let $\Phi_{p^n}(T) = T^{p^{n-1}(p-1)} + T^{p^{n-1}(p-2)} + \cdots + T^{p^{n-1}} + 1 \in \mathbb{Z}[T]$ be the p^n-th cyclotomic polynomial for $p > 2$. Prove that $\Phi_{p^n}(T)$ is irreducible over $\mathbb{Q}_p$ for all $n \geq 1$.

(iii) Can you find an optimal criterion for the shape of the Newton polygon of f alone to imply that f is irreducible? When this criterion is satisfied, what can you say about the extension of K given by adjoining a root of f?

7. Consider the polynomial $f(T) = 5!(1 + T + T^2/2 + T^3/3! + T^4/4! + T^5/5!) \in \mathbb{Z}[T]$.

(i) Draw the Newton polygon of $f(T)$ over $\mathbb{Q}_p$ for $p = 2, 3, 5$.

(ii) Deduce that $f(T)$ is irreducible over $\mathbb{Q}$ and the Galois group of its splitting field is S_5.

8. (Continuity of roots) Let K be a complete DVF and let K^{sep} be a separable closure of K equipped with the extended valuation w (there is a unique extension to every separable finite extension, hence to every separable algebraic extension, though it need not be discrete). Let $f(T) = a_0 + a_1T + \cdots + T^n$ and $g(T) = b_0 + b_1T + \cdots + T^n$ be monic polynomials in $K[T]$ with roots in K^{sep}, and let $\beta_1, ..., \beta_n \in K^{sep}$ be the roots of g. If $\alpha \in K^{sep}$ is a root of f, prove that there exists a j such that

$$w(\alpha - \beta_j) \geq \min_{i=0,\ldots,n-1} \left(\frac{w(a_i - b_i)}{n} + \frac{i.w(\alpha)}{n} \right).$$

(*Hint: Consider* $g(\alpha) - f(\alpha) = g(\alpha) = \prod_i (\alpha - \beta_i)$.) Reformulating it somewhat imprecisely, if the coefficients of g are close enough to those of f, then there is a root of g close to α.

9. (Krasner's Lemma) Let K be a complete DVF and let K^{sep} be a separable closure of K equipped with the extended valuation w. Let $\alpha \in K^{sep}$ be separable and let $\alpha_2, \ldots, \alpha_n \in \overline{K}$ be the K-conjugates of α. If $\beta \in K^{sep}$ is such that

$$w(\alpha - \beta) > w(\alpha - \alpha_i)$$

for $i = 2, ..., n$, show that $K(\alpha) \subseteq K(\beta)$. (*Hint: Let* L *be the Galois closure of* $K(\alpha, \beta)$ *over* $K(\beta)$*, and show that* $w(\alpha - \sigma(\alpha)) > w(\alpha - \alpha_i)$ *for all* $i = 2, ..., n$ *and* $\sigma \in \mathrm{Gal}(L/K(\beta))$).

10. Let $L/\mathbb{Q}_p$ be a finite extension. Show, using the two previous exercises or otherwise, that we can find a finite extension $K/\mathbb{Q}$ and a maximal ideal $\mathfrak{p}$ of $\mathcal{O}_K$ containing p such that $L = K_{\mathfrak{p}}$.

11. Let $f(T) = 3T^3 + T + 3 \in \mathbb{Z}[T]$. Show that f is irreducible over $\mathbb{Q}$. Let $K = \mathbb{Q}(\alpha)$, where α is a root of $f(T)$. Decide how many primes in $\mathcal{O}_K$ there are lying above $p = 2, 3, 5$ in $\mathbb{Z}$, respectively.

12. Let $K = \mathbb{Q}(\alpha)$, where α is a root of equation $T^3+T^2-2T+8 = 0$. Show that there are three distinct primes of $\mathcal{O}_K$ lying above 2. Deduce that there is no element $\gamma \in \mathcal{O}_K$ such that $\mathcal{O}_K = \mathbb{Z}[\gamma]$.

13. This exercise is for enthusiasts, but I recommend reading through it even if you do not complete it (it is not as long as it looks!). It recalls the perspective on Galois groups as permutations on the roots and interprets decomposition groups in this language, and uses this to prove a result that sometimes allows you to compute Galois group by reduction mod p.

    Let K be a field and let $f(T) \in K[T]$ be a separable polynomial of degree n, with splitting field L/K. There is a surjective ring homomorphism $\phi : K[T_1, ..., T_n] \to L$ given by $T_i \mapsto \alpha_i$, where $\alpha_1, \ldots, \alpha_n$ are the roots of f. Let I denote the kernel of ϕ. If $\sigma \in S_n$, the symmetric group on $\{1, \ldots, n\}$, then σ defines an automorphism of $K[T_1, ..., T_n]$ given by

    $$(\sigma F)(T_1, ..., T_n) = F(T_{\sigma(1)}, ..., T_{\sigma(n)}).$$

    Show that the Galois group $\mathrm{Gal}(f/K) := \mathrm{Gal}(L/K)$ of f can be identified with the subgroup of those $\sigma \in S_n$ such that $\sigma(I) = I$. In somewhat imprecisely language, the Galois group of f is the group of permutations of the roots which preserve all polynomial relations between the roots over K. We will think of Galois group of polynomials as permutation groups on the roots in this exercise.

    Now consider an irreducible polynomial $f(T) \in \mathbb{Q}[T]$, with roots $\alpha_1, ..., \alpha_n$ inside some algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$. Show that $\mathrm{Gal}(f/\mathbb{Q}_p) \subseteq \mathrm{Gal}(f/\mathbb{Q})$ as permutation groups. If $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$, show that $\mathrm{Gal}(f/\mathbb{Q}_p) \subseteq \mathrm{Gal}(f/\mathbb{Q} = \mathrm{Gal}(K/\mathbb{Q})$ is the decomposition group $D_{\mathfrak{p}|p}$ for some prime $\mathfrak{p}$ of $\mathcal{O}_K$. How is this prime determined?

    Now assume that f is monic, and in $\mathbb{Z}[T]$. Let $\overline{f} \in \mathbb{F}_p[X]$ denote the reduction of f modulo p. If $\overline{f}$ is separable (i.e. p does not divide the discriminant of f), show that there is natural bijection between the roots of f in $\overline{\mathbb{Q}}_p$ and the roots of $\overline{f}$ in the residue field of $\overline{\mathbb{Q}}_p$ (which is an algebraic closure of $\mathbb{F}_p$). Then show that $\mathrm{Gal}(f/\mathbb{Q}_p) = \mathrm{Gal}(\overline{f}/\mathbb{F}_p)$ as permutation groups with respect to this bijection, and conclude that we have $\mathrm{Gal}(\overline{f}/\mathbb{F}_p) \subseteq \mathrm{Gal}(f/\mathbb{Q})$ as permutation groups in a natural way.

    If you're still curious at this point, here is a typical application of this result. Let $f(T) = T^7 - T - 1 \in \mathbb{Z}[T]$. By considering f modulo 2, show that f is irreducible. By considering f modulo 3, show that $\mathrm{Gal}(f/\mathbb{Q})$ contains a permutation of cycle type $(2, 5)$. Deduce that $\mathrm{Gal}(f/\mathbb{Q})$ contains a transposition and a 5-cycle, which implies that $\mathrm{Gal}(f/\mathbb{Q}) = S_7$ (the only transitive subgroup of S_7 containing a transposition and a 5-cycle is S_7; there are a number of such results).