6370-001 - FALL 2021 - WEEK 2 (8/31, 9/2)

1. Integral elements

Exercise 1.
Suppose $L/\mathbb{Q}$ is an algebraic extension. Show that $a \in L$ is integral over $\mathbb{Z}$ if and only if its minimal polynomial over $\mathbb{Q}$ has coefficients in $\mathbb{Z}$.

Exercise 2.
Show that a UFD is integrally closed.

Exercise 3.
If $R \subset S \subset T$ are commutative rings with S integral over R, show that $t \in T$ is integral over R if and only if it is integral over S.

Exercise 4.
Suppose K is a field and $R \subset K$ is a subring. Suppose $a \in K$ and $R[a] \subset M \subset K$, where M is a finite R-module. Show a is integral by using a determinant to find a monic polynomial with coefficients in R such that $f(a) = 0$.

Exercise 5.
Recall from your study of field automorphisms that, for K a field and $G \leq \mathrm{Aut}(K)$ a finite subgroup, $[K : K^G] = |G|$, where K^G denotes the elements in K fixed by G (so, in particular, K/K^G is Galois with group G).

(1) Use this to show that $\mathbb{Q}(t_1, \ldots, t_n)^{S_n} = \mathbb{Q}(e_1, \ldots, e_n)$, where e_i is the ith elementary symmetric polynomial, i.e. the sum of the distinct monomials of degree i in the $t_j's$.
(2) Deduce that $e_1, \ldots, e_n$ is a transcendence base.
(3) Conclude that $\mathbb{Z}[t_1, \ldots, t_n]^{S_n} = \mathbb{Z}[e_1, \ldots, e_n]$ (hint: use the result of Exercise 2).
(4) Use this to give another proof that the integers $\mathcal{O}_K$ in a finite extension $K/\mathbb{Q}$ is a ring.

Exercise 6.
For R a ring and $\mathfrak{m}$ a maximal ideal, the tangent space of Spec$R$ at $\mathfrak{m}$. Is defined to be $(\mathfrak{m}/\mathfrak{m}^2)^*$, a vector space over $\kappa = R/\mathfrak{m}$.

(1) Explain why this is a good definition (hint: Taylor expansions).
(2) Suppose R is a Noetherian domain of Krull dimension 1 (i.e. the only non-maximal prime ideal is 0). Show that R is integrally closed if and only if the tangent space at any maximal ideal is 1-dimensional. What does this mean geometrically?

2. Discriminants

Exercise 7. *Trace and norm.*
If L/K is a finite extension and $\alpha \in L$, the trace of α, $\mathrm{Tr}_{L/K}(\alpha)$ is the trace of the K-linear transformation $L \to L$ given by multiplication by α. The norm, $\mathrm{N}_{L/K}(\alpha)$ is the determinant.

(1) If $M/L/K$ are finite extensions and $\alpha \in L$, show

$$\mathrm{Tr}_{M/K}(\alpha) = [M : L]\mathrm{Tr}_{L/K}(\alpha) \text{ and } \mathrm{N}_{M/K}(\alpha) = \mathrm{N}_{L/K}(\alpha)^{[L:M]}.$$

(2) Describe $\mathrm{Tr}_{L/K}(\alpha)$ and $\mathrm{N}_{L/K}(\alpha)$ in terms of the minimal polynomial of α (hint: use part (1) to reduced to $L = K(\alpha)$, then compute with the basis $1, \alpha, \alpha^2, \ldots$.
(3) For L/K separable, describe $\mathrm{Tr}_{L/K}(\alpha)$ and $\mathrm{N}_{L/K}(\alpha)$ in terms of the images of α under the embeddings of L into an algebraic closure of K.
(4) Show that if $K/\mathbb{Q}$ is a finite extension and $\alpha \in \mathcal{O}_K$, then $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$ and similarly for norm.

Exercise 8.

(1) Suppose $\alpha \in \mathbb{C}$, $K = \mathbb{Q}(\alpha)$ and $\alpha \in \mathcal{O}_K$. Show that the discriminant of $\mathbb{Z}[\alpha]/\mathbb{Z}$ is the discriminant of the minimal polynomial f_α: if we write the complex roots of f as $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$,
$$\mathrm{disc} f_\alpha = \prod_{i<j} (\alpha_i - \alpha_j)^2.$$
(2) Show this is equal to $\mathrm{Nm}_{K/\mathbb{Q}} f'_\alpha(\alpha)$.

Exercise 9. Suppose $[K : \mathbb{Q}] = n$. If $\alpha_1, \ldots, \alpha_n$ is $\mathbb{Z}$- basis for $\mathcal{O}_K$ and $\sigma_1, \ldots, \sigma_n$ are the embbedings $K \hookrightarrow \mathbb{C}$, show that
$$\mathrm{disc}(\mathcal{O}_K/\mathbb{Z}) = \det((\sigma_i(\alpha_j)_{ij})^2$$

Exercise 10.

(1) Compute the discriminant of $\mathbb{Q}(\sqrt{n})$ for n squarefree.

Exercise 11. Let V be a finite dimensional $\mathbb{Q}$-vector space equipped with a non-degenerate bilinear pairing $(,)$. A $\mathbb{Z}$-lattice $M \subset V$ is a finitely generated $\mathbb{Z}$-submodule such that $\mathbb{Q} \cdot M = V$.

(1) Show a $\mathbb{Z}$-lattice is a free $\mathbb{Z}$-module of rank equal to $\dim_{\mathbb{Q}} V$.
(2) Show that if M is a lattice then so is M^*.
(3) For $M_2 \subset M_1$ two lattices, explain why the determinant of the change of basis matrix from any basis of M_1 to any basis of M_2 has absolute value $|M_2/M_1|$ and is well-defined up to its sign.
(4) For M a lattice, the discriminant of M, $\mathrm{disc}(M)$ is the determinant of the change of basis matrix from the dual basis $e_1^*, \ldots, e_n^*$ to $e_1, \ldots, e_n$ for any basis e_i. explain why $\mathrm{disc}(M)$ is well-defined (i.e. why does the sign not depend on the basis of M?)

Exercise 12.
This exercise shows the following useful result:
Theorem. If $K/\mathbb{Q}$ is a finite extension and $R \subset \mathcal{O}_K$ is such that $\mathrm{disc}(R)$ is square-free, then $R = \mathcal{O}_K$.

(1) Let V be a finite dimensional $\mathbb{Q}$-vector space equipped with a non-degenerate bilinear pairing $(,)$. Suppose M_1 is a lattice in V such that $M_1 \subset M_1^*$, and $M_2 \subset M_1$ is a sublattice.
   (a) Show $M_1^* \subset M_2^*$, and $|M_2^*/M_1^*| = |M_1/M_2|$.
   (b) Deduce $\mathrm{disc}(M_2)$ and $\mathrm{disc}(M_1)$ differ by a square.
(2) Conclude by applying the above to $R \subset \mathcal{O}_K$.

Exercise 13.

(1) For p an odd prime, compute the discriminant of $\mathbb{Z}[\zeta_p] \subset \mathbb{Q}(\zeta_p)$.
(2) Deduce that $\mathbb{Z}[\zeta_p]$ is the ring of integers in $\mathbb{Q}(\zeta_p)$.

Exercise 14. Let $K/\mathbb{Q}$ be a finite extension and let D be the discriminant of $K/\mathbb{Q}$.

(1) Let $2s$ be the number of embeddings $K \hookrightarrow \mathbb{C}$ that don't factor through $\mathbb{R}$ (why is this an even number?). Show
$$\mathrm{sign}(D) = (-1)^s.$$
(2) Show Stickelberger's theorem:
$$D \equiv 1 \text{ or } 0 \bmod 4.$$
(3) Compare both with your computation of the discriminants of quadratic fields.

Exercise 14.

(1) Show that if L/K is a a finite extension of fields, the trace pairing on L (with values in K) is non-degenerate if and only if L/K is separable.
(2) Show that if $L/\mathbb{F}_q(t)$ is a separable extension then the integral closure of $\mathbb{F}_q[t]$ in L is a finite free $\mathbb{F}_q[t]$-module of rank $[L : \mathbb{F}_q(t)]$.
(3) Show that if $L/\mathbb{F}_q(t)$ is any finite extension then the same still holds.