MATH 210B. HOMEWORK 5

1. Let R be a commutative ring with 1 and G a finite group acting by ring automorphisms on R. Prove that R is integral over R^G.

2. Let $K/\mathbf{Q}$ be an extension field of degree n, and let $\mathscr{O}_K$ be the set of elements of K integral over $\mathbf{Z}$. This is called the ring of algebraic integers in K.

(i) Prove that the trace (from K to $\mathbf{Q}$) maps $\mathscr{O}_K$ into $\mathbf{Z}$.

(ii) Prove that $\mathscr{O}_K$ is a finite free $\mathbf{Z}$-module of rank n.

3. Let $K/\mathbf{Q}$ be an extension field of degree n. A $\mathbf{Z}$-subalgebra $\mathscr{O} \subset \mathscr{O}_K$ is an *order* if it is finite free of rank n as a $\mathbf{Z}$-module.

(i) Prove that a subring $\mathscr{O}$ of $\mathscr{O}_K$ is an order if and only if it has finite index in $\mathscr{O}_K$, and that $\mathscr{O}$ always admits a $\mathbf{Z}$-basis containing 1.

(ii) For $\alpha \in \mathscr{O}_K$ prove that $\mathbf{Z}[\alpha]$ is an order if and only if $K = \mathbf{Q}(\alpha)$, in which case $\{1, \alpha, \dots, \alpha^{n-1}\}$ is a $\mathbf{Z}$-basis of this order.

(iii) Assume $n = 2$. For $f \geq 1$, prove that $\mathbf{Z} + f\mathscr{O}_K$ is the unique order of index f in $\mathscr{O}_K$. Give an explicit $\mathbf{Z}$-basis $\{1, \alpha_f\}$ of $\mathbf{Z} + f\mathscr{O}_K$ when $K = \mathbf{Q}(\sqrt{d})$ for a square-free $d \in \mathbf{Z}$.

4. We continue with the notation of the previous question. Let $\mathscr{O}$ be an order in K, and let $x_1, \dots, x_r$ be a basis for $\mathscr{O}$ as a $\mathbf{Z}$-module. Define the *discriminant* of $\mathscr{O}$ to be

$$\mathrm{disc}(\mathscr{O}) = \det(\mathrm{Tr}_{K/\mathbf{Q}}(x_i x_j)).$$

(i) Prove this is an integer, independent of choice of basis x_i.

(ii) For $K = \mathbf{Q}(\sqrt{d})$ with a square-free $d \in \mathbf{Z} - \{0, 1\}$, prove $D_K := \mathrm{disc}(\mathscr{O}_K/\mathbf{Z})$ is $4d$ when $d \equiv 2, 3 \bmod 4$ and is d when $d \equiv 1 \bmod 4$. Deduce that $\mathscr{O}_K = \mathbf{Z}[(D_K + \sqrt{D_K})/2]$.

(iii) For a finite extension K of $\mathbf{Q}$ and an order $\mathscr{O} \subset \mathscr{O}_K$ (see Exercise 2), prove $\mathrm{disc}(\mathscr{O}/\mathbf{Z}) = [\mathscr{O}_K : \mathbf{Q}]^2 \mathrm{disc}(\mathscr{O}_K/\mathbf{Z})$. Deduce that if $\mathrm{disc}(\mathscr{O}/\mathbf{Z})$ is squarefree then $\mathscr{O} = \mathscr{O}_K$! As an application, prove that for $K = \mathbf{Q}(\alpha)$ with $\alpha^3 - \alpha + 1 = 0$, $\mathscr{O}_K = \mathbf{Z}[\alpha]$ with $\mathrm{disc}(\mathscr{O}_K/\mathbf{Z}) = -23$.

5. Suppose $M_1, \dots, M_r$ are a family of commuting $n \times n$ integer matrices. Take $v \in \mathbf{F}_q^n$ to be a common eigenvector, so that

$$M_i v = \lambda_i v \quad (i = 1, \dots, r).$$

Prove that we can *lift* this common eigenvalue to characteristic zero, in the following sense: There exists a finite field extension K of $\mathbf{Q}$, a homomorphism $\varphi : \mathscr{O}_K \to \mathbb{F}_q$ and a common eigenvector $V \in K^n$:

$$M_i V = \eta_i V$$

such that $\varphi(\eta_i) = \lambda_i$.

6. Suppose that $P_1, \dots, P_n \in \mathbf{Q}[x_1, \dots, x_n]$ are such that $\underline{P} : (P_1, \dots, P_n)$ gives an injection $\mathbf{C}^n \to \mathbf{C}^n$. We previously showed that $\underline{P}$ defines a bijective map $k^n \to k^n$ whenever k is a finite field of sufficiently large characteristic.

(i) Prove that $\underline{P}$ defines a surjective map $\mathbf{C}^n \to \mathbf{C}^n$. [1]

(ii) Explain how to extend the conclusion to the case when $P_1, \dots, P_n \in \mathbf{C}[x_1, \dots, x_n]$. [2]

Remark: There are many other pretty results that can be proven by "reduction modulo p." For example, if $\mathbf{C}^n$ is given a group law where the group operations are polynomials, then this group law must be nilpotent; this follows, eventually, from the fact that groups of order p^n are nilpotent.

[1]Hint: Suppose not; explain why there exists a point $\mathbf{x} \in \overline{\mathbf{Q}}^n$ not in the image. The coordinates of $\mathbf{x}$ lie in some finite extension $K \supset \mathbf{Q}$, and we may suppose they lie in $\mathcal{O}_K[\frac{1}{M}]$ for suitable M. Now "reduce mod p" to contradict what has already been proven.

[2]Hint: Replace $\mathbf{Q}$ by the ring R generated by $\mathbf{Z}$ and the coefficients of the P_i, and use Noether normalization to construct homomorphisms from R to finite fields.