MATH 250B: COMMUTATIVE ALGEBRA
HOMEWORK #8

JOHN VOIGHT

Problem 1. *Let K be a Galois extension of the $\mathbb{Q}$ with group G. Let B the integral closure of $\mathbb{Z}$ in K, and let $\alpha \in B$ be such that $K = \mathbb{Q}(\alpha)$. Let $f(X)$ be the irreducible polynomial for α over $\mathbb{Q}$. Let p be a prime number, and assume that f remains irreducible modulo p over $\mathbb{Z}/p\mathbb{Z}$. What can you say about the Galois group G?*

Solution. Let $\mathfrak{p}$ be a prime above p in B. Then the decomposition group $G_{\mathfrak{p}}$ is a subgroup of G; by Proposition 2.5, the extension $B/\mathfrak{p}$ over $\mathbb{Z}/p\mathbb{Z}$ is Galois with group cyclic of order $n = [K : \mathbb{Q}] = \deg f$. By proposition 2.8, $G_{\mathfrak{p}}$ is isomorphic to this Galois group, so $\mathbb{Z}/n\mathbb{Z} \subset G$. Since both groups are finite of order n, $G \cong \mathbb{Z}/n\mathbb{Z}$, i.e. G is cyclic.

Problem 2. *Let A be an entire ring and K its quotient field. Let t be transcendental over K. If A is integrally closed, show that $A[t]$ is integrally closed.*

Solution. Let $x \in K(t)$ be integral over $A[t]$. Since $K[t]$ is a UFD, it is integrally closed, so $x \in K[t]$ (Proposition 1.7). Let x satisfy the integral equation

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$$

with coefficients $a_i \in A[t]$. Write $x = x(t) = c_n t^n + \cdots + c_0$ with $c_i \in K$. Substituting these into f, looking at the coefficients of each t^i we see that the coefficients c_i are themselves integral over A, hence $c_i \in A$, and $x \in A[t]$.

Problem 4. *Let L be a finite extension of $\mathbb{Q}$ and let $\mathcal{O}_L$ be the ring of algebraic integers in L. Let $\sigma_1, \ldots, \sigma_n$ be the distinct embeddings of L into the complex numbers. Embed $\mathcal{O}_L$ into a Euclidean space by the map*

$$\alpha \mapsto (\sigma_1\alpha, \ldots, \sigma_n\alpha).$$

Show that in any bounded region of this Euclidean space, there is only a finite number of elements of $\mathcal{O}_L$. [Hint: The coefficients in an integral equation for α are elementary symmetric functions of the conjugates of α and thus are bounded integers.] Use Exercise 5 of Chapter III to conclude that $\mathcal{O}_L$ is a free $\mathbb{Z}$-module of dimension $\leq n$. In fact, show that the dimension is n, a basis of $\mathcal{O}_L$ over $\mathbb{Z}$ also being a basis of L over $\mathbb{Q}$.

Solution. Suppose α lies in the bounded region. Then the numbers $\sigma_i\alpha$ are all bounded; in particular, the coefficients of an integral equation for α (being elementary symmetric functions of the conjugates of α) are bounded integers. Since the

Date: April 10, 2003.
VII: 1, 2, 4, 6, 7, 9, 10.

degree of an integral equation for α is also bounded (by the degree $[L:\mathbb{Q}]$), there are only finitely many such integral equations, hence only finitely many α.

By Exercise III.5, $\mathcal{O}_L$ is a free $\mathbb{Z}$-module of rank $\leq n$. Let $\alpha_1, \dots, \alpha_n$ be a basis for L over $\mathbb{Q}$. For each α_i, there exists an integer $c_i \in \mathbb{Z}_{>0}$ such that $c_i\alpha_i \in \mathcal{O}_L$; therefore $c_i\alpha_i \in \mathcal{O}_L$ are $\mathbb{Z}$-linearly independent, so $\mathcal{O}_L$ contains a free $\mathbb{Z}$-submodule of rank n, hence $\mathcal{O}_L$ is itself free of rank n.

Problem 7. *Let $\mathcal{O}$ be an entire ring which is noetherian, integrally closed, and such that every nonzero prime ideal is maximal. Define a* fractional ideal $\mathfrak{a}$ *to be a nonzero $\mathcal{O}$-submodule of the quotient field K such that there exists $c \in \mathcal{O}$, $c \neq 0$ for which $c\mathfrak{a} \subset \mathcal{O}$. Prove that fractional ideals form a group under multiplication:*

(a) *Given an ideal $\mathfrak{a} \neq 0$ in $\mathcal{O}$, there exists a product of prime ideals $\mathfrak{p}_1 \dots \mathfrak{p}_r \subset \mathfrak{a}$.*
(b) *Every maximal ideal $\mathfrak{p}$ is invertible, i.e. if we let $\mathfrak{p}^{-1}$ be the set of elements $x \in K$ such that $x\mathfrak{p} \subset \mathcal{O}$, then $\mathfrak{p}^{-1}\mathfrak{p} = \mathcal{O}$.*
(c) *Every nonzero ideal is invertible, by a fractional ideal. [Use the noetherian property that if this is not true, there exists a maximal noninvertible ideal $\mathfrak{a}$ and get a contradiction.]*

Solution. For (a), consider the set of ideals which do not contain a product of primes. If the set is nonempty, since $\mathcal{O}$ is noetherian, there exists a maximal such ideal $\mathfrak{a}$. We cannot have $\mathfrak{a}$ prime, therefore there exists $x, y \in \mathcal{O}$ such that $xy \in \mathfrak{a}$ but $x, y \notin \mathfrak{a}$. Since $\mathfrak{a}$ is maximal, the ideals $\mathfrak{a} + (x)$ and $\mathfrak{a} + (y)$ contain a product of prime ideals: but

$$(\mathfrak{a} + (x))(\mathfrak{a} + (y)) \subset \mathfrak{a}$$

so $\mathfrak{a}$ contains a product of primes, a contradiction.

For (b), it is clear that $\mathfrak{p}^{-1}\mathfrak{p}$ is an ideal of $\mathcal{O}$, so since $\mathfrak{p}$ is maximal, we must have either $\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}$, or $\mathfrak{p}^{-1}\mathfrak{p} = \mathcal{O}$. Let $a \in \mathfrak{p}$ be nonzero: then by (a) there exists a product of primes $\mathfrak{p}_1 \dots \mathfrak{p}_r \subset (a) \subset \mathfrak{p}$. We may assume that $\mathfrak{p}_1 \dots \mathfrak{p}_r$ is a minimal such product (r taken as small as possible). Since every prime is maximal, we know $\mathfrak{p} = \mathfrak{p}_i$ for some i, so we may assume $\mathfrak{p} = \mathfrak{p}_1$. Then $\mathfrak{p}_2 \dots \mathfrak{p}_r \not\subset (a)$, so there exists $b \in \mathfrak{p}_2 \dots \mathfrak{p}_r$ such that $b \notin (a)$. But $b\mathfrak{p} \subset (a)$, so $ba^{-1}\mathfrak{p} \subset \mathcal{O}$, so $ba^{-1} \in \mathfrak{p}^{-1}$. Since $b \notin a\mathcal{O}$, $ba^{-1} \notin \mathcal{O}$, so $\mathfrak{p}^{-1} \neq \mathcal{O}$. This implies $\mathfrak{p}^{-1}\mathfrak{p} = \mathcal{O}$.

For (c), suppose that the set of nonzero noninvertible ideals is nonempty. Then since $\mathcal{O}$ is noetherian, there exists a maximal such noninvertible ideal $\mathfrak{a}$. If $\mathfrak{a}$ is maximal, then by (b) it is invertible; otherwise, it is contained (properly) in a maximal ideal $\mathfrak{p}$, and

$$\mathfrak{a} \subset \mathfrak{a}\mathfrak{p}^{-1} \subset \mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}.$$

We cannot have $\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}$, so $\mathfrak{a}\mathfrak{p}^{-1}$ is invertible. But then

$$\mathcal{O} = (\mathfrak{a}\mathfrak{p}^{-1})\mathfrak{a}\mathfrak{p}$$

implies that $\mathfrak{a}$ is invertible, a contradiction.

To conclude, note that every fractional ideal $\mathfrak{a}$ has $c\mathfrak{a} \subset \mathfrak{O}$ for some $c \neq 0$: then $(1/c)(c\mathfrak{a})^{-1}$ is an inverse for $\mathfrak{a}$.

Problem 9. *Let A be an entire ring, integrally closed. Let B be entire, integral over A. Let $\mathfrak{q}_1, \mathfrak{q}_2$ be prime ideals of B with $\mathfrak{q}_1 \supset \mathfrak{q}_2$ but $\mathfrak{q}_1 \neq \mathfrak{q}_2$. Let $\mathfrak{p}_i = \mathfrak{q}_i \cap A$. Show that $\mathfrak{p}_1 \neq \mathfrak{p}_2$.*

Solution. Suppose $\mathfrak{p}_1 = \mathfrak{p}_2 = \mathfrak{p}$. Then the ring $A_\mathfrak{p}$ is a local ring with maximal ideal $\mathfrak{p}A_\mathfrak{p}$, and $B_\mathfrak{p}$ is an integral extensions of $A_\mathfrak{p}$ with $\mathfrak{q}_i B_\mathfrak{p} \cap A_\mathfrak{p} = \mathfrak{p}A_\mathfrak{p}$, so since the latter is maximal, so too is each $\mathfrak{q}_i$. In particular, if $\mathfrak{q}_1 \subset \mathfrak{q}_2$, then $\mathfrak{q}_1 = \mathfrak{q}_2$, a contradiction.