Name: Tuan Pham
ID: 4652218

Math 8202: General Algebra
Homework #5 9 0/10

(1) Problem 3, Lang, p. 353

Let A be an entire Noetherian ring and K be the field of fractions of A. Suppose that A is integrally closed in K. Let $K \subset L$ be a finite separable extension field. Let B be the integral closure of A in L. We'll show that B is a finitely generated A-module.

Put $n = [L:K]$. Then L is an n-dimensional vector space over K. Let $\{w_1, w_2, \dots, w_n\}$ be a basis of L. Because each w_i is algebraic over K, it is a root of a polynomial $f_i(X) = X^{n_i} + \sum_{j=0}^{n_i-1} \frac{a_{ij}}{s_{ij}} X^j \in K[X]$, where $n_i \in \mathbb{N}$, $a_{ij} \in A$, $s_{ij} \in A \setminus \{0\}$. Put $t_i = \prod_{j=0}^{n_i-1} s_{ij} \in A \setminus \{0\}$. We have

$$\begin{aligned} 0 = t_i^{n_i} f_i(w_i) &= t_i^{n_i}\left(w_i^{n_i} + \sum_{j=0}^{n_i-1} \frac{a_{ij}}{s_{ij}} w_i^j \right) \\ &= (t_i w_i)^{n_i} + \sum_{j=0}^{n_i-1} \frac{a_{ij}}{s_{ij}} t_i^{n_i} w_i^j \\ &= (t_i w_i)^{n_i} + \sum_{j=0}^{n_i-1} \underbrace{\frac{a_{ij} t_i^{n_i-j}}{s_{ij}}}_{\in A \text{ because } s_{ij} \mid t_i \text{ and } t_i \mid t_i^{n_i-j}} (t_i w_i)^j \end{aligned}$$

Thus $t_i w_i$ is a root of a ~~poly~~ monic polynomial with coefficients in A. Thus $t_i w_i$ is integral over A. Thus $t_i w_i \in B$. If we put $w_i = t_i w_i$ then

$\{\tilde{\omega}_1, \tilde{\omega}_2, \dots, \tilde{\omega}_n\}$ is also a basis of L over K and $\tilde{\omega}_i \in B$. Thus, we can assume from the beginning when we introduced $\omega_1, \dots, \omega_n$ that these are in B.

Because $K \subset L$ is separable, $[L:K]_s = [L:K] = n$. Thus, there are exactly n distinct embeddings $\sigma_1, \dots, \sigma_n : L \to K$ whose ~~restricting~~ restriction on K is identity. We know that the trace map $Tr: L \to K$, $Tr(\alpha) = \sigma_1(\alpha) + \dots + \sigma_n(\alpha)$ is K-linear. We will show that there is a basis $\{\omega_1', \omega_2', \dots, \omega_n'\}$ of L over K such that $Tr(\omega_i \omega_j') = \delta_{ij} = \begin{cases} 1 & \text{if } i=j, \\ 0 & \text{if } i \neq j. \end{cases}$

Proof of the claim

For each $x \in L$, we have a map $Tr_x : L \to K$, $Tr_x(y) = Tr(xy)$.

For $y_1, y_2 \in L$, we have $Tr_x(y_1+y_2) = Tr(x(y_1+y_2)) = Tr(xy_1 + xy_2)$
$= Tr(xy_1) + Tr(xy_2) = Tr_x(y_1) + Tr_x(y_2)$.

For $c \in K$, $y \in L$, we have $Tr_x(cy) = Tr(xcy) = Tr(cxy) = c\,Tr(xy) = c\,Tr_x(y)$.

Therefore, Tr_x is a K-linear map, i.e. $Tr_x \in L^\vee$ - the dual vector space of L over K. Then we get a map $\phi : L \to L^\vee$, $\phi(x) = Tr_x$.

We'll show that ϕ is a linear morphism. For $x_1, x_2, y \in L$, we have

$\phi(x_1+x_2)(y) = Tr_{x_1+x_2}(y) = Tr((x_1+x_2)y) = Tr(x_1y + x_2y) = Tr(x_1y) + Tr(x_2y)$
$= Tr_{x_1}(y) + Tr_{x_2}(y) = \phi(x_1)(y) + \phi(x_2)(y)$.

Thus $\phi(x_1+x_2) = \phi(x_1) + \phi(x_2)$.

For $c \in L$, $x, y \in L$, we have

$$\phi(cx)(y) = Tr_{cx}(y) = Tr(cxy) = cTr(xy) = cTr_x(y) = c\phi(x)(y).$$

Thus $\phi(cx) = c\phi(x)$. Therefore, ϕ is a K-linear map. Next, we show that ϕ is injective. Take $x \in \ker\phi$. Then $Tr_x = 0$, i.e. $Tr(xy) = 0 \ \forall y \in E$. Since If $x \neq 0$ then $xE = E$; then $Tr(E) = 0$; then $Tr = 0$ which is impossible because $\sigma_1, \sigma_2, \dots, \sigma_n$ are linearly independent characters. Thus $x = 0$. Thus ϕ is injective. Because $\phi: L \longrightarrow L^\vee$ is an injective linear morphism with $\dim_K L = \dim_K L^\vee = n$, it is in fact an isomorphism.

For each $i = 1, 2, \dots, n$, we denote by $\delta_i \in L^\vee$ the function such that

$$\delta_i(w_j) = \delta_{ij} = \begin{cases} 0 & \text{if } i \neq j, \\ 1 & \text{if } i = j. \end{cases}$$

Then $\{\delta_1, \delta_2, \dots, \delta_n\}$ is a basis of $L^\vee$. Put $w_i' = \phi^{-1}(\delta_i)$. Since ϕ is a linear isomorphism, $\{w_1', w_2', \dots, w_n'\}$ is a basis of L. We have $\phi(w_i') = \delta_i$. Thus $\delta_{ij} = \phi(w_i')(w_j) = Tr(w_i' w_j)$. ∎

Return to the problem. Now we have a basis $\{w_1', \dots, w_n'\}$ of L over K such that $Tr(w_i w_j') = \delta_{ij}$. For each $\alpha \in L$, there exists $b_1, b_2, \dots b_n \in K$ such that $\alpha = b_1 w_1' + \dots + b_n w_n'$. We'll show that if $\alpha \in B$ then $b_1, b_2, \dots, b_n \in A$. Now suppose that $\alpha \in B$. For each $i = 1, 2, \dots, n$ we have

4

$$\alpha w_i = \sum_{j=1}^{n} b_j w_i w_j'$$

Thus, $Tr(\alpha w_i) = \sum_{j=1}^{n} b_j Tr(w_i w_j') = \sum_{j=1}^{n} b_j \delta_{ij} = b_i$.

Because $\alpha, w_i \in B$, $\alpha w_i \in B$. Thus $\sigma_1(\alpha w_i), \dots, \sigma_n(\alpha w_i)$ are also integral over A. Thus, $Tr(\alpha w_i)$ is integral over A. Thus $b_i \in K$ is integral over A. Since A is integrally closed in K, $b_i \in A$.

We have proved that $\alpha \in Aw_1' + \dots + Aw_n'$ for every $\alpha \in B$. Thus, $B \subset Aw_1' + \dots + Aw_n' = B'$. Since A is a Noetherian ring and B' is a finitely generated A-module, B' is a Noetherian A-module. Since B is submodule of B', every submodule of B is also a submodule of B', which is finitely generated. Thus B is a Noetherian A-module.

In addition, every ideal of B is a B-submodule of B and also is an A-submodule of B. Thus, every ideal of B is a finitely generated A-module. Thus every ideal of B is a finitely generated B-module.

Therefore, B is a Noetherian ring.

(2) Problem 7, Lang p. 353.

Let A be a ring such that
- entire (integral domain),
- Noetherian,
- integrally closed,
- every prime ideal that is nonzero is also a maximal ideal.

(a) Let $\underline{a}$ be a nontrivial ideal of A. We will show that there are nontrivial prime ideals $f_1, \dots, f_r$ of A such that $f_1 f_2 \cdots f_r \subset \underline{a}$.

Suppose by contradiction that this is not true. Put Σ to be the family of all nontrivial ideals of A that doesn't contain any finite product of nontrivial prime ideals of A. Then $\Sigma \neq \emptyset$ by our assumption. Σ together with the inclusion relation forms a poset, namely $(\Sigma, \subseteq)$. We'll show that Σ has a maximal element by using Zorn's lemma. Let $\mathcal{F}$ be a subcollection of Σ that is totally ordered. Put $J = \bigcup_{I \in \mathcal{F}} I \neq 0$. We want to show that $J \in \Sigma$.

First, we show that J is an ideal.

For $x, y \in J$, there are $I_1, I_2 \in \mathcal{F}$ such that $x \in I_1$ and $y \in I_2$. Since $\mathcal{F}$ is totally ordered, we can assume $I_1 \subset I_2$. Then $x - y \in I_2 \subset J$. For $x \in J$ and $a \in A$, there exists $I \in \mathcal{F}$ such that $x \in I$. Since I is an ideal, $ax \in I \subset J$. Therefore, J is an ideal of A.

Next, suppose by contradiction that $J \notin \Sigma$. Then J contains a product $f_1 f_2 \cdots f_r$ of nontrivial prime ideals f_i. Since A is Noetherian, $f_1 \cdots f_r$ is a finitely generated ideal of A. Thus there are $a_1, a_2, \dots, a_n \in A$ such that $f_1 f_2 \cdots f_r = (a_1, a_2, \dots, a_n)$.

For each $i=1,2,\dots,n$, $a_i \in J$. Thus, there is $I_i \in F$ such that $a_i \in I_i$. Since F is totally ordered, there is $I_0 = \max\{I_1,\dots,I_n\} \in F$. Thus, $a_1, a_2, \dots, a_n \in I_0$. Thus $I_0 \supset (a_1, a_2, \dots, a_n) = \mathfrak{p}_1 \cdots \mathfrak{p}_r$. This means I_0 is an element of Σ that contains $\mathfrak{p}_1 \cdots \mathfrak{p}_r$. This is a contradiction.

Therefore, $J \in \Sigma$.

So far, we proved that Σ has a maximal element. We call it J. Then J is not a prime ideal because otherwise J contains a prime ideal, which is itself. Then there are $a, b \in A \setminus J$ such that $ab \in J$. We have $J \subsetneq J + aA$ and $J \subsetneq J + bA$. Because J is a maximal element of Σ, $J+aA$ and $J+bA$ are not in Σ. Thus, $J+aA$ contains a product of nontrivial prime ideals $\mathfrak{p}_1 \cdots \mathfrak{p}_s$, and $J+bA$ contains a product of nontrivial prime ideals $\mathfrak{q}_1, \dots, \mathfrak{q}_e$. Then $(J+aA)(J+bA)$ contains $\mathfrak{p}_1 \cdots \mathfrak{p}_s \mathfrak{q}_1 \cdots \mathfrak{q}_e$. We have

$$(J+aA)(J+bA) = JJ + aJ + bJ + abA \subseteq J + abA.$$

Since $ab \in J$, $abA \subseteq J$. Thus $(J+aA)(J+bA) \subset J$. Thus, J contains the product of prime ideals $\mathfrak{p}_1 \cdots \mathfrak{p}_s \mathfrak{q}_1 \cdots \mathfrak{q}_e$. This is a contradiction because $J \in \Sigma$.

Let $\mathfrak{p}$ be a prime (which is also maximal) ideal of A. Define

$$\mathfrak{p}^{-1} = \{x \in K : x\mathfrak{p} \subset A\},$$

$$\mathfrak{p}^{-1}\mathfrak{p} = \{\sum_{\text{finite}} x_i a_i : x_i \in \mathfrak{p}^{-1},\ a_i \in \mathfrak{p}\}.$$

We will show that $\mathfrak{p}^{-1}\mathfrak{p} = A$. First we will show that $\mathfrak{p}^{-1}\mathfrak{p}$ is an ideal of A. For every $x \in \mathfrak{p}^{-1}$ and $a \in \mathfrak{p}$, we have $xa \in x\mathfrak{p} \subset A$. Thus $\mathfrak{p}^{-1}\mathfrak{p} \subset A$. The difference of two finite sums of the form $\sum x_i a_i$ is also a finite sum of this form. Thus $\mathfrak{p}^{-1}\mathfrak{p}$ is an additive subgroup of A. For every $x = \sum x_i a_i \in \mathfrak{p}^{-1}\mathfrak{p}$ and $r \in A$, we have

$$rx = \sum \underbrace{x_i}_{\in \mathfrak{p}^{-1}} \underbrace{(ra_i)}_{\in \mathfrak{p}} \in \mathfrak{p}^{-1}\mathfrak{p}$$

Therefore $\mathfrak{p}^{-1}\mathfrak{p}$ is an ideal of A.

We see that $1 \cdot \mathfrak{p} = \mathfrak{p} \subset A$. Thus $1 \in \mathfrak{p}^{-1}$. Thus $\mathfrak{p} = 1 \cdot \mathfrak{p} \subset \mathfrak{p}^{-1}\mathfrak{p}$. Since $\mathfrak{p}$ is a maximal ideal of A, there are only two possibilities, namely $\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}$ and $\mathfrak{p}^{-1}\mathfrak{p} = A$. We will show that the first case cannot happen. Suppose by contradiction that $\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}$. Take an element $a \in \mathfrak{p} \setminus \{0\}$. Then $(a) = Aa \subset \mathfrak{p}$. In the previous part, we showed that (a) contains a product of prime ideals $\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r$. Assume that r was chosen to be the smallest possible number *

such that (a) contains a product of r prime ideals. We consider two cases, namely $r=1$ and $r \geq 2$.

• $\underline{r=1}$ Then $\mathfrak{p}_1 \subset (a) \subset \mathfrak{p}$.

Since $\mathfrak{p}_1$ is also a maximal ideal, $\mathfrak{p}_1 = \mathfrak{p}$. Thus $\mathfrak{p} = (a)$. We'll show that $\frac{1}{a} \in \mathfrak{p}^{-1}$. For every $x \in \mathfrak{p} = (a)$, there is $y \in A$ such that $x = ay$. Then $\frac{1}{a} x = \frac{1}{a} ay = y \in A$. Thus $\frac{1}{a} \mathfrak{p} \subset A$. Thus, $\frac{1}{a} \in \mathfrak{p}^{-1}$. Then $1 = \frac{1}{a} \cdot a \in \mathfrak{p}^{-1}\mathfrak{p}$. Since ~~$\mathfrak{p}^{-1}\mathfrak{p}$ is an~~ $\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}$, we have $1 \in \mathfrak{p}$, which is a contradiction.

• $\underline{r \geq 2}$ Then $\mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_r \subset (a) \subset \mathfrak{p}$.

Suppose by contradiction that none of $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_r$ is contained in $\mathfrak{p}$. Then for each $i = 1, 2, \cdots, r$, there exists $a_i \in \mathfrak{p}_i \setminus \mathfrak{p}$. We have, however,

$$a_1 a_2 \cdots a_r \in \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_r \subset \mathfrak{p}.$$

Thus at least one of $a_1, a_2, \cdots, a_r$ must be in $\mathfrak{p}$ since $\mathfrak{p}$ is a prime ideal. This is a contradiction. Therefore, at least one of $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_r$ is contained in $\mathfrak{p}$, say $\mathfrak{p}_1$ for instance. Since $\mathfrak{p}_1$ is maximal, $\mathfrak{p} = \mathfrak{p}_1$. Thus, $\mathfrak{p}\mathfrak{p}_2 \cdots \mathfrak{p}_r \subset (a)$. By the minimality of r, we have $\mathfrak{p}_2 \cdots \mathfrak{p}_r \not\subset (a)$. Thus there exists $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r \setminus (a)$. Then $b\mathfrak{p} \subset \mathfrak{p}\mathfrak{p}_2 \cdots \mathfrak{p}_r \subset (a)$. Put $c = \frac{b}{a}$.

We'll show that $c \in \mathfrak{f}^{-1}$. For every $x \in \mathfrak{f}$, $cx = \frac{bx}{a}$. Since $bx \in b\mathfrak{f} \subset (a)$, there is $y \in A$ such that $bx = ay$. Then $cx = \frac{ay}{a} = y \in A$. Thus $c\mathfrak{f} \subset A$, which means $c \in \mathfrak{f}^{-1}$. Then $c\mathfrak{f} \subset \mathfrak{f}^{-1}\mathfrak{f} = \mathfrak{f}$. We'll show by induction in n that $c^n\mathfrak{f} \subset \mathfrak{f}$. This is true for $n = 1$. Suppose that $c^n\mathfrak{f} \subset \mathfrak{f}$. Then $c^{n+1}\mathfrak{f} = c(c^n\mathfrak{f}) \subset c\mathfrak{f} \subset \mathfrak{f}$. Thus the claim has been proved.

Pick any $\alpha \in \mathfrak{f} \setminus \{0\}$. We'll show that $\alpha A[c] \subset A$. Each $x \in A[c]$ is written in a form $x = a_n c^n + \cdots + a_1 c + a_0$ with $a_i \in A$ for all i. Then $\alpha x = (\alpha a_n) c^n + \cdots + (\alpha a_1) c + (\alpha a_0)$ where each $\alpha a_i \in \mathfrak{f}$. Thus $\alpha x \in c^n\mathfrak{f} + \cdots + c\mathfrak{f} + \mathfrak{f}$. Since $\mathfrak{f}, c\mathfrak{f}, \cdots, c^n\mathfrak{f} \subset \mathfrak{f}$ as we proved in the previous paragraph, $\alpha x \in \mathfrak{f} \subset A$. Therefore, $\alpha A[c] \subset A$. This means $\alpha A[c]$ is an A-submodule of A. Because A is Noetherian, $\alpha A[c]$ is finitely generated. On the other hand, the map

$$\phi : A[c] \longrightarrow \alpha A[c], \quad \phi(x) = \alpha x$$

determines an A-module isomorphism. Thus $A[c]$ is also a finitely generated A-module. ~~Since~~ This means c is integral over A. Since A is integrally closed in K, $c \in A$. Thus $b = ca \in (a)$.

This contradicts the choice of b.

(c) For each nonzero ideal of A, we define $\underline{a}^{-1} = \{x \in K : x\underline{a} \subset A\}$. First we will show that $\underline{a}^{-1}$ is an A-module in K. Let $x, y \in \underline{a}^{-1}$. We have $x\underline{a}, y\underline{a} \subset A$. Moreover, $(x+y)\underline{a} = \{(x+y)z : z \in \underline{a}\}$

$= \{xz + yz : z \in \underline{a}\} \subset x\underline{a} + y\underline{a}$,

which is contained in A. Thus $x+y \in \underline{a}$. Let $r \in A$ arbitrarily. For every $x \in \underline{a}^{-1}$, we have $(rx)\underline{a} = x(r\underline{a}) \subset x\underline{a} \subset A$. Thus $rx \in \underline{a}^{-1}$. Thus $\underline{a}^{-1}$ is an A-module in K. In other words, $\underline{a}^{-1}$ is a fractional ideal of A. We will show that $\underline{a}^{-1}\underline{a} = A$.

Suppose that $\underline{a}^{-1}\underline{a} \neq A$ for some nonzero ideal $\underline{a}$ of A. ~~Then we can assume that~~ Put $S = \{\underline{b} \supset \underline{a}$ nonzero ideal of $A : \underline{b}^{-1}\underline{b} \neq A\}$. Then $\underline{a} \in S$. Since S is a subset of submodules of A and A is Noetherian, it has a maximal ~~ideal~~ element. Thus we could have chosen $\underline{a}$ to be this maximal element. This implies that every ideal of A that contains but not equals $\underline{a}$ is invertible.

~~By the first part of the problem, $\underline{a}$ contains a product of nonzero prime ideals $\mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_r$. Assume that r was chosen to be the smallest number that makes this possible.~~ Let $\mathfrak{p}$ be a maximal ideal of A

that contains $\underline{a}$. We know from part (b) that $\mathfrak{p}^{-1}\mathfrak{p} = A$. Because $1 \in \mathfrak{p}^{-1}$, $\underline{a} \subset \mathfrak{p}^{-1}\underline{a}$. Note that $\mathfrak{p}^{-1}\underline{a} \subset \mathfrak{p}^{-1}\mathfrak{p} = A$. So $\mathfrak{p}^{-1}\underline{a}$ is an ideal of A. There are two possibilities, namely $\underline{a} = \mathfrak{p}^{-1}\underline{a}$ and $\underline{a} \subsetneq \mathfrak{p}^{-1}\underline{a}$. Suppose by contradiction that $\underline{a} = \mathfrak{p}^{-1}\underline{a}$. Pick any $\alpha \in \underline{a} \setminus \{0\}$ and $c \in \mathfrak{p}^{-1}$. Then $c\underline{a} \subset \mathfrak{p}^{-1}\underline{a} = \underline{a}$. Then $c^2\underline{a} = c(c\underline{a}) \subseteq c\underline{a}$. Then by induction we can prove that $c^n\underline{a} \subset c\underline{a}$ for all $n \in \mathbb{N}$. Thus $\alpha c^n \in \underline{a}$ for all $n \in \mathbb{N}$. For each $x \in A[c]$, we have

$$\alpha x = \sum_{i=0}^{n} \underbrace{\alpha a_i}_{\in \underline{a}} c^i \in \underline{a} + c\underline{a} + \cdots + c^n\underline{a} \subset \underline{a}.$$

Therefore, $\alpha A[c] \subset \underline{a}$. Thus $\alpha A[c]$ is an A-submodule of A. Since A is Noetherian, $\alpha A[c]$ is finitely generated. Thus $A[c] \cong \alpha A[c]$ is also a finitely generated A-module. Thus c is integral over A. Since A is integrally closed in K, $c \in A$. We have proved that $\mathfrak{p}^{-1} \subset A$. Then $\mathfrak{p} \subset A\mathfrak{p} \subset \mathfrak{p}$. This is impossible because $\mathfrak{p}^{-1}\mathfrak{p} = A$.

Therefore we must have $\underline{a} \subsetneq \mathfrak{p}^{-1}\underline{a}$. By the maximality of $\underline{a}$, $\mathfrak{p}^{-1}\underline{a}$ is invertible. Let $I = \{x \in K : x\mathfrak{p}^{-1}\underline{a} \subset A\}$ be its inverse. Then $I(\mathfrak{p}^{-1}\underline{a}) = A$. For every $x \in I\mathfrak{p}^{-1}$, we have $x\underline{a} \subset (I\mathfrak{p}^{-1})\underline{a} = A$. Thus by definition, $x \in \underline{a}^{-1}$. This means $I\mathfrak{p}^{-1} \subset \underline{a}^{-1}$. Then

$$A = (\mathfrak{I}\mathfrak{p}^{-1})\mathfrak{a} \subseteq \mathfrak{a}^{-1}\mathfrak{a}.$$

Thus $\mathfrak{a}^{-1}\mathfrak{a} = A$, which is a contradiction.

(3) Problem 1, Lang, p. 374

Denote by $\mathrm{Aut}(\mathbb{C})$ the set of all field automorphisms of $\mathbb{C}$. We will show that $\mathrm{Aut}(\mathbb{C})$ is infinite. In the following, we will use without proof the fact that if E is an infinite field and $E \subset F$ is an algebraic extension then $|F| = |E|$.

Because $|\mathbb{Q}| < 2^{\aleph_0} = |\mathbb{C}|$, $\mathbb{C}$ is not algebraic over $\mathbb{Q}$. Let $\mathcal{B} = \{X_i : i \in I\} \neq \emptyset$ be a transcendental basis of $\mathbb{C}$ over $\mathbb{Q}$. Put $K = \mathbb{Q}(\mathcal{B})$. Then $K \subset \mathbb{C}$ is an algebraic extension. Thus, $|K| = |\mathbb{C}|$. We'll show that $\mathcal{B}$ is an uncountable set. Suppose by contradiction that $\mathcal{B}$ is at most countable. Then we can write $\mathcal{B} = \{X_1, X_2, X_3, \dots\}$. Then

$$K = \mathbb{Q}(X_1, X_2, \dots) = \bigcup_{k=1}^{\infty} \mathbb{Q}(X_1, \dots, X_k). \qquad (*)$$

Let X be any variable over $\mathbb{Q}$. ~~Then $\mathbb{Q}[X]$ can be viewed as the set of all sequences with entries in $\mathbb{Q}$ that are all but finitely many equal to zero. The map is simply $\sum a_i X^i \mapsto (a_0, a_1, \dots)$. Thus $\mathbb{Q}[X]$ is~~ Then $\mathbb{Q}[X]$ is the union of the sets of polynomials

of degree n, as n goes from 0 to infinity. There are only countably many polynomials of degree n and with coefficients in $\mathbb{Q}$. Thus $\mathbb{Q}[X]$ is countable. Then $\mathbb{Q}[X] \times \mathbb{Q}[X]$ is also countable. We have a surjective map $\mathbb{Q}[X] \times (\mathbb{Q}[X] \setminus \{0\}) \longrightarrow \mathbb{Q}(X)$ defined by $(f, g) \mapsto \frac{f}{g}$. Thus $\mathbb{Q}(X)$ is also countable. Then by induction in k we have $\mathbb{Q}(X_1, \dots, X_{k-1}, X_k) = \mathbb{Q}(X_1, \dots, X_{k-1})(X_k)$ is also countable. Then by (*), K is countable. This is a contradiction because $|K| = |\mathbb{C}|$. Therefore B is uncountable. Thus $|B| \geq |\mathbb{C}|$.

For each subset A of I, the set $\{Y_j : j \in I\}$ where

$$Y_j = \begin{cases} X_j & \text{if } j \in A, \\ -X_j & \text{if } j \notin A, \end{cases}$$

is also algebraically independent over $\mathbb{Q}$. Then we can define a field isomorphism $f_A : K \to K$ which induces identity on $\mathbb{Q}$ and $f(X_j) = Y_j \ \forall j \in I$. In other words, f_A fixes X_j if $j \in A$, and switches the sign of X_j if $j \notin A$. Thus, different choices of subset $A \subset I$ result in different f_A. We can view f_A as an embedding from K to $\mathbb{C}$. Since $K \subset \mathbb{C}$ is algebraic and $\mathbb{C}$ is

algebraically closed, f_A can extend to an embedding $g_A : \mathbb{C} \to \mathbb{C}$.

Then $g_A \in \mathrm{Aut}(\mathbb{C})$. Thus we get an injective map $\phi : \mathcal{P}(I) \to \mathrm{Aut}(\mathbb{C})$,

$$\phi(A) = g_A.$$

Thus, $|\mathrm{Aut}(\mathbb{C})| \geq |\mathcal{P}(I)| = 2^{|I|} = 2^{|\mathbb{R}|} \geq 2^{|\mathbb{C}|}$.

On the other hand, each automorphism of $\mathbb{C}$ is a set-theoretic map from $\mathbb{C}$ to $\mathbb{C}$. Thus,

$$|\mathrm{Aut}(\mathbb{C})| \leq |\mathbb{C}|^{|\mathbb{C}|} = \left(2^{|\mathbb{N}|}\right)^{|\mathbb{C}|} = 2^{|\mathbb{N}||\mathbb{C}|} = 2^{|\mathbb{C}|}.$$

Therefore, $|\mathrm{Aut}(\mathbb{C})| = 2^{|\mathbb{C}|} = 2^{2^{|\mathbb{N}|}}$.

(4) (i) Let $A \subset B \subset C$ be commutative rings. Suppose that A is Noetherian, and C is a finitely generated A-algebra, and that C is integral over B. We will show that B is a finitely generated A-algebra.

First we write $C = A[x_1, x_2, \cdots, x_n]$. Because $B \subset C$ is integral, each x_i is a root of a monic polynomial over B, namely $f_i(X)$. Let $\{y_1, y_2, \cdots, y_m\}$ be the set of all coefficients of $f_1(X), f_2(X), \cdots, f_n(X)$. Then $A[y_1, y_2, \cdots, y_m] \subset B$. Put $D = A[y_1, y_2, \cdots, y_m]$. Then $f_i(X) \in D[X]$. Thus each x_i is integral over D. Let E be the set of all elements

of C that are integral over D. Then E is a subring of C (in fact E is the integral closure of D in C). Since $A \subset E$ and $x_1, x_2, \dots, x_n \in E$, $C = A[x_1, x_2, \dots, x_n] \subset E$. Thus $E = C$. This means C is integral over D. Since C is a finitely generated A-algebra, it is also a finitely generated D-algebra. Now that C is integral over D and finitely generated as a D-algebra, C is finitely generated as a D-module.

Since A is a Noetherian ring and D is finitely generated as an A-algebra, by a consequence of Hilbert's Basis theorem, D is also a Noetherian ring. On the other hand, C is finitely generated as a D-module, so C is a Noetherian D-module. Since $D \subset B \subset C$, B is a D-submodule of C. Thus B is a finitely generated D-module. Then there exists $z_1, z_2, \dots, z_r \in B$ such that $B = D[z_1, z_2, \dots, z_r]$. Then

$$B = A[y_1, \dots, y_m][z_1, z_2, \dots, z_r] = A[y_1, \dots, y_m, z_1, \dots, z_r].$$

Thus B is a finitely generated A-algebra.

(ii) Let A be a Noetherian ring and B be a finitely generated A-algebra. Suppose that G is a finite group of automorphisms of B over A. Put $B_G = \{ b \in B : \sigma(b) = b \ \forall \sigma \in G \}$. We will show that

B_G is a finitely generated A-algebra.

First we will show that B_G is a subring of B. Obviously, B_G contains 0 and 1. For $x, y \in B_G$, we have $\sigma(x) = x$, $\sigma(y) = y$ $\forall \sigma \in G$. Thus $\sigma(xy) = \sigma(x)\sigma(y) = xy$ and $\sigma(x \pm y) = \sigma(x) \pm \sigma(y) = x \pm y$ $\forall \sigma \in G$. Therefore $xy, x-y \in B_G$, and so B_G is a subring of B.

Since G consists of automorphisms of B over A, we have $A \subseteq B_G$. Thus, $A \subseteq B_G \subseteq B$. We are given that A is Noetherian and that B is finitely generated as an A-algebra. By Part (i), to show that B_G is a finitely generated A-algebra, we only need to prove that B is integral over B_G.

Take any $b \in B$. We are looking for a monic polynomial with coefficients in B_G of which b is a root. Since G is a finite group, we can write $G = \{g_1, g_2, \ldots, g_n\}$. Then we put

$$f(X) = \prod_{k=1}^{n} (X - g_k(b)) = X^n + \sum_{k=0}^{n-1} (-1)^{n-k} a_{n-k} X^k,$$

where $a_k = e_k(g_1(b), \ldots, g_n(b))$, and e_k is the k'th symmetric polynomial of n variables. Since $\mathrm{Id}_B \in G$, there is some k such that $g_k(b) = b$. Thus b is a root of $f(X)$. Now we will show that each $a_i \in B_G$.

To do so, we will show that each a_i is fixed by G. Let $g \in G$ be any element. Since g is an automorphism of B, we have

$$g(a_i) = g\left(e_i(g_1(b), \dots, g_n(b))\right) = e_i\left(g\circ g_1(b), \dots, g\circ g_n(b)\right).$$

Since G is a group, $(g\circ g_1, \dots, g\circ g_n)$ is just a permutation of $(g_1, \dots, g_n)$. Since e_i is a symmetric polynomial of n variables, we have $e_i(g\circ g_1(b), \dots, g\circ g_n(b)) = e_i(g_1(b), \dots, g_n(b)) = a_i$. Thus $g(a_i) = a_i$. Therefore, a_i is fixed by all elements of G.

(5) Let A be a commutative ring, f be a monic polynomial over A with $\deg f = n \geq 1$. We'll show that there is a ring B containing A and is finitely generated as an A-module such that f has a root in B. Let $\hat{X}$ be a variable over A. Put $E = A[\hat{X}]/(f(\hat{X}))$. Then we have an inclusion map $A \longrightarrow E$ in which $\alpha \longmapsto [\alpha] = \alpha + (f(\hat{X}))$.

~~Now we view f as a polynomial $\tilde{f}$ over E, namely~~

We write $f(X) = X^n + a_{n-1}X^{n-1} + \dots + a_1 X + a_0$ where $a_i \in A$ and X is a variable over A and E. Then we will view A as a subring of E and f as a polynomial $\tilde{f}$ over E, namely

$$\tilde{f}(X) = X^n + [a_{n-1}]X^{n-1} + \dots + [a_1]X + [a_0].$$

We have $\hat{X} \in E$ and $\tilde{f}(\hat{X}) = \hat{X}^n + [a_{n-1}]\hat{X}^{n-1} + \cdots + [a_1]\hat{X} + [a_0]$

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

$$= f(\hat{X}) + (f(\hat{X}))$$

$$= [0].$$

Therefore $\tilde{f}$ has a root in E. Next, we will show that E is a finitely generated A-module. Let D be the A-submodule of E generated by $1, \hat{X}, \ldots, \hat{X}^{n-1}$. We will show that $D = E$. We have

$$\hat{X}^n = [a_{n-1}]\hat{X}^{n-1} + \cdots + [a_1]\hat{X} + [a_0]$$

We will show that $\hat{X}^m$ is a linear combination of $1, \hat{X}, \ldots, \hat{X}^{n-1}$ over A, for every $m \geq n$. For $m = n$, this is true. Suppose that

$$\hat{X}^m = [b_{n-1}]\hat{X}^{n-1} + \cdots + [b_1]\hat{X} + [b_0], \quad b_i \in A$$

Then $\hat{X}^{m+1} = \hat{X}\hat{X}^m = [b_{n-1}]\hat{X}^n + [b_{n-2}]\hat{X}^{n-1} + \cdots + [b_1]\hat{X}^2 + [b_0]\hat{X}$

$$= [b_{n-1}]\left([a_{n-1}]\hat{X}^{n-1} + \cdots + [a_0]\right) + [b_{n-2}]\hat{X}^{n-1} + \cdots + [b_0]\hat{X},$$

which is a linear combination of $1, \hat{X}, \ldots, \hat{X}^{n-1}$ over A. Therefore we have proved that all powers of $\hat{X}$ lie in D. Thus $E \subset D$, which implies $E = D$. Thus E is finitely generated as an A-module.

Additional #3