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 $K \subseteq L$ 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 $\{w_1, w_2, ..., w_n\}$ 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 $n_i \in \mathbb{N}$, $a_{ij} \in A$, $s_{ij} \in A \setminus \{0\}$. Let $t_i = \frac{n_i-1}{\prod_{j=0}^{n_i-1} s_{ij}} \in A \setminus \{0\}$. We have

$$0 = t_{i}^{n_i} f_i(w_i) = t_i^{n_i} \left( w_i^{n_i} + \sum_{j=0}^{n_i-1} \frac{a_{ij}}{s_{ij}} w_i^j \right)$$

$$= (t_i w_i)^{n_i} + \sum_{j=0}^{n_i-1} \frac{a_{ij}}{s_{ij}} (t_i w_i)^j$$

$$= (t_i w_i)^{n_i} + \sum_{j=0}^{n_i-1} \frac{a_{ij} t_i^{n_i-j}}{s_{ij}} (t_i w_i)^j$$

$EA$ because $s_{ij} \mid t_i$ and $t_i \mid t_i^{n_i-j}$

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

Because } K \subseteq L \text{ is separable, } [L:K]_s = [L:K] = n. \text{ Thus, there are exactly } n \text{ distinct embeddings } \sigma_1, \ldots, \sigma_n: L \to K \text{ whose restricting restriction on } K \text{ is identity. We know that the trace map } \Tr: L \to K, \\Tr(\alpha) = \sigma_1(\alpha) + \ldots + \sigma_n(\alpha) \text{ is } K\text{-linear. We will show that there is a basis } \{\omega'_1, \omega'_2, \ldots, \omega'_3\} \text{ of } L \text{ over } K \text{ such that } \Tr(\omega_i \omega_j') = \delta_{ij} = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases}

}\underline{Proof \text{ of the claim}}.

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

For } y_1, y_2 \in L, \text{ 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, \text{ we have } \Tr_x(cy) = \Tr(xy_c) = \Tr(cy) = c \Tr(xy) = c \Tr_x(y).

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

We'll show that } \phi \text{ is a linear morphism. For } x_1, x_2, y \in L, \text{ we have } \phi(x_1 + x_2)(y) = \Tr_{x_1 + x_2}(y) = \Tr((x_1 + x_2)y) = \Tr(x_1 y + x_2 y) = \Tr(x_1 y) + \Tr(x_2 y) = \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 $c \in K$, $x, y \in L$, we have
\[
\phi(cx)(y) = Tr_c(y) = Tr(xy) = c Tr(x)(y) = c \phi(x)(y).
\]
Thus $\phi(cx) = c \phi(x)$. Therefore $\phi$ is a $K$-linear map. Next, we show that $\phi$ is injective. Take $x \in \ker \phi$. Then $Tr(x) = 0$, i.e., $Tr(xy) = 0$ for all $y \in L$.

If $x \neq 0$ then $x E = E$; then $Tr(E) = 0$; then $Tr = 0$ which is impossible because $\delta_1, \delta_2, \ldots, \delta_n$ are linearly independent characters. Thus $x = 0$. Thus $\phi$ is injective. Because $\phi : L \rightarrow L^\vee$ is an injective linear morphism with $\dim_K L = \dim_K L^\vee = n$, it is in fact an isomorphism.

For each $i = 1, 2, \ldots, n$, we denote by $\delta_i \in L^\vee$ the function such that
\[
\delta_i(w) = \delta_i = \begin{cases} 0 & \text{if } i \neq j, \\ 1 & \text{if } i = j. \end{cases}
\]
Then $\{\delta_1, \delta_2, \ldots, \delta_n\}$ is a basis of $L^\vee$. Put $w_i = \phi^{-1}(\delta_i)$. Since $\phi$ is a linear isomorphism, $\{w_1, w_2, \ldots, w_n\}$ is a basis of $L$. We have $\phi(w_i) = \delta_i$.

Thus $\delta_i = \phi(w_i)(w_j) = Tr(w_i, w_j)$.

Return to the problem. Now we have a basis $\{w_1, w_2, \ldots, w_n\}$ of $L$ over $K$ such that $Tr(w_i, w_j) = \delta_{ij}$. For each $x \in L$, there exists $b_1, b_2, \ldots, b_n \in K$ such that $x = b_1 w_1 + \ldots + b_n w_n$. We'll show that if $x \in E$ then $b_1, b_2, \ldots, b_n \in E$. Now suppose that $x \in E$. For each $i = 1, 2, \ldots, n$ we have
\[ x^i_w = \sum_{j=1}^{n} b_j w_i^j \]

Thus, \( \text{Tr}(x^i_w) = \sum_{j=1}^{n} b_j \text{Tr}(w_i^j) = \sum_{j=1}^{n} b_j s_j = b_i \).

Because \( x, w_i \in B, \; \alpha w_i \in B \). Thus, \( \alpha w_i \in B \) are also integral over \( A \). Thus, \( \text{Tr}(x^i_w) \) is integral over \( A \). Thus \( b_i \in \mathbb{K} \) is integral over \( A \). Since \( A \) is integrally closed in \( \mathbb{K} \), \( b_i \in A \).

We have proved that \( x \in A w_1 + \ldots + A w_n \) for every \( x \in B \). Thus, \( B \subseteq A w_1 + \ldots + A w_n = \mathbb{A}' \). Since \( A \) is a Noetherian ring and \( \mathbb{A}' \) is a finitely generated \( A \)-module, \( \mathbb{A}' \) is a Noetherian \( A \)-module. Since \( B \) is submodule of \( \mathbb{A}' \), every submodule of \( B \) is also a submodule of \( \mathbb{A}' \), 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 $\mathfrak{a}$ be a nontrivial ideal of $A$. We will show that there are nontrivial prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ of $A$ such that $\mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_r \subseteq \mathfrak{a}$.

Suppose by contradiction that this is not true. Put $\Sigma$ 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. $\Sigma$ together with the inclusion relation forms a poset, namely $(\Sigma, \subseteq)$. We'll show that $\Sigma$ has a maximal element by using Zorn's lemma. Let $F$ be a subcollection of $\Sigma$ that is totally ordered. Put $J = \bigcup_{I \in F} I \neq 0$. We want to show that $J \in \Sigma$.

First, we show that $J$ is an ideal.

For $x, y \in J$, there are $I_1, I_2 \in F$ such that $x \in I_1$ and $y \in I_2$. Since $F$ is totally ordered, we can assume $I_1 \subseteq I_2$. Then $x - y \in I_2 \subseteq J$.

For $x \in J$ and $a \in A$, there exists $I \in F$ such that $x \in I$. Since $I$ is an ideal, $ax \in I \subseteq J$. Therefore, $J$ is an ideal of $A$.

Next, suppose by contradiction that $J \notin \Sigma$. Then $J$ contains a product $\mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_r$ of nontrivial prime ideals $\mathfrak{p}_i$. Since $A$ is Noetherian, $\mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_r$ is a finitely generated ideal of $A$. Thus there are $a_1, a_2, \ldots, a_n \in A$ such that $\mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_r = (a_1, a_2, \ldots, a_n)$. 


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

So far, we proved that $\Sigma$ 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 $J \not\subseteq J + aA$ and $J \not\subseteq J + bA$. Because $J$ is a maximal element of $\Sigma$, $J + aA$ and $J + bA$ are not in $\Sigma$. 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 $\mathfrak{p}_1 \cdots \mathfrak{p}_e$. Then $(J + aA)(J + bA)$ contains $\mathfrak{p}_1 \cdots \mathfrak{p}_s \mathfrak{p}_1 \cdots \mathfrak{p}_e$. We have

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

Let \( p \) be a prime (which is also maximal) ideal of \( A \). Define
\[
\begin{align*}
p^{-1} &= \{ x \in K : xp \subseteq A \}, \\
p^{-1}p &= \left\{ \sum_{\text{finite}} x_i a_i : x_i \in p^{-1}, a_i \in p \right\}.
\end{align*}
\]
We will show that \( p^{-1}p = A \). First we will show that \( p^{-1}p \) is an ideal of \( A \). For every \( x \in p^{-1} \) and \( a \in p \), we have \( xa \in xp \subseteq CA \). Thus \( p^{-1}p \subseteq CA \). The difference of two finite sums of the form \( \sum x_i a_i \) is also a finite sum of this form. Thus \( p^{-1}p \) is an additive subgroup of \( A \). For every \( x = \sum x_i a_i \in p^{-1}p \) and \( r \in A \), we have
\[
r x = \sum x_i (ra_i) \in p^{-1}p
\]
therefore \( p^{-1}p \) is an ideal of \( A \).

We see that \( 1, p = p \subseteq A \). Thus \( 1 \in p^{-1} \). Thus \( p = 1, p \subseteq p^{-1}p \).

Since \( p \) is a maximal ideal of \( A \), there are only two possibilities, namely \( p^{-1}p = p \) and \( p^{-1}p = A \). We will show that the first case cannot happen. Suppose by contradiction that \( p^{-1}p = p \). Take an element \( a \in p \setminus \{0\} \). Then \( (a) = Aa \subseteq p \). In the previous part, we showed that \( (a) \) contains a product of prime ideals \( f_1 f_2 \cdots f_r \). 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 $r > 2$.

- **Case 1:** If $r = 1$, then $p_1 \subset (a) \subset p$.

  Since $p_1$ is also a maximal ideal, $p_1 = r$. Thus $p = (a)$. We shall show that $\frac{1}{a} \notin p^*$ for every $x \in f = (a)$, there is $y \in A$ such that $x = ay$. Then $\frac{1}{a} x = \frac{1}{a} ay = y \in A$. Thus $\frac{1}{a} r \subset A$. Thus, $\frac{1}{a} \notin p^*$.

  Then $1 = \frac{1}{a} \cdot a \in p^*$.

  Since $p^*$ is an ideal, $p^* \subset f$, we have $1 \in f$, which is a contradiction.

- **Case 2:** Then $p \subseteq f_1 f_2 \cdots f_r \subset (a) \subset f$.

  Suppose by contradiction that none of $f_1, f_2, \ldots, f_r$ is contained in $p$. Then for each $i = 1, 2 \ldots, r$, there exists $a_i \in f_i \setminus f$. We have, however,

  $a_1 a_2 \cdots a_r \in f_1 f_2 \cdots f_r \subset f$.

  Thus at least one of $a_1, a_2, \ldots, a_r$ must be in $p$ since $p$ is a prime ideal. This is a contradiction. Therefore, at least one of $f_1, f_2, \ldots, f_r$ is contained in $f$, say $f_1$, for instance. Since $p_1$ is a maximal ideal, $p = p_1$. Thus, $f_2 \cdots f_r \subset (a)$. By the minimality of $r$, we have $f_2 \cdots f_r \subset f(a)$. Thus, there exists $b \in f_2 \cdots f_r \setminus (a)$. Then $bf \subset f_2 \cdots f_r \subset (a)$. Put $c = \frac{b}{a}$. 


We'll show that \( c \in \phi \). For every \( x \in \phi \), \( cx = \frac{bx}{a} \). Since \( bx \in \phi \subset (a) \), there is \( y \in \alpha \) such that \( bx = ay \). Then \( cx = \frac{ay}{a} = y \in \alpha \).

Thus \( c \in \alpha \), which means \( c \in \phi \). Then \( cf \subset \phi \). We'll show by induction in \( n \) that \( c^n f \subset \phi \). This is true for \( n = 1 \). Suppose that \( c^n f \subset \phi \). Then \( c^{n+1} f = c(c^n f) \subset c f \subset \phi \). Thus the claim has been proved.

Pick any \( x \in \phi \setminus \{0\} \). We'll show that \( x\alpha[c] \subset \alpha \). Each \( x \in \alpha[c] \) is written in a form \( x = a_1 x^n + \cdots + a_q c + a_0 \) with \( a_i \in \alpha \) for all \( i \).

Then \( xx = (a_1 x^n + \cdots + a_q c + a_0) \alpha[c] \), where each \( a_i \in \phi \). Thus \( xx \in c^n f + \cdots + cf + f \). Since \( f, cf, \ldots, c^n f \subset \phi \) as we proved in the previous paragraph, \( xx \in \phi \subset \alpha \). Therefore, \( x\alpha[c] \subset \alpha \). This means \( \alpha[c] \) is an \( \alpha \)-submodule of \( \alpha \). Because \( \alpha \) is Noetherian, \( \alpha[c] \) is finitely generated. On the other hand, the map

\[
\phi : \alpha[c] \to x\alpha[c], \quad \phi(x) = xx
\]

determines an \( \alpha \)-module isomorphism. Thus \( \alpha[c] \) is also a finitely generated \( \alpha \)-module. Since this means \( c \) is integral over \( \alpha \). Since \( \alpha \) is integrally closed in \( K \), \( c \in \alpha \). Thus \( b = ca \in (a) \).
This contradicts the choice of \( b \).

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

\[
= \{ xz+yz : z \in \mathfrak{a} \} \subseteq x \mathfrak{a} + y \mathfrak{a},
\]

which is contained in \( A \). Thus \( x+y \in \mathfrak{a}^{-1} \). Let \( r \in \mathfrak{a} \) arbitrarily. For every \( x \in \mathfrak{a}^{-1} \), we have \( (rx) \mathfrak{a} = x(r \mathfrak{a}) \subseteq x \mathfrak{a} \subseteq CA \). Thus \( rx \in \mathfrak{a}^{-1} \).

Thus \( \mathfrak{a}^{-1} \) is an \( A \)-module in \( K \). In other words, \( \mathfrak{a}^{-1} \) is a fractional ideal of \( A \). We will show that \( \mathfrak{a}^{-1} \mathfrak{a} = \mathfrak{a} \).

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

By the first part of the problem, \( \mathfrak{a} \) contains a product of nonzero prime ideals \( p_1, p_2, \ldots, p_r \). Assume that \( r \) was chosen to be the smallest number that makes this possible. Let \( f \) be a maximal ideal of \( A \)
that contains \( a \). We know from part (b) that \( p^{-1}p = A \).

Because \( t \in p^{-1} \), \( a \subseteq p^{-1}a \). Note that \( p^{-1}a \subseteq p^{-1}p = A \). So \( p^{-1}a \)

is an ideal of \( A \). There are two possibilities, namely \( a = p^{-1}a \)

and \( a \neq p^{-1}a \). Suppose by contradiction that \( a = p^{-1}a \). Pick any

\( x \in \mathbb{A} \setminus \{0\} \) and \( c \in p^{-1} \). Then \( cx \subseteq p^{-1}a = a \). Thus \( c^na = c(cx) =

\leq ca \). Then by induction we can prove that \( c^n a \subseteq ca \) for

all \( n \in \mathbb{N} \). Thus \( xc^n a \subseteq \text{ for all } n \in \mathbb{N} \). For each \( x \in \mathbb{A}[c] \),

we have \( \lambda x = \sum_{i=0}^{n} \alpha c^i \subseteq a + ca + \ldots + c^n a \subseteq ca \).

Therefore, \( xA[c] \subseteq ca \). Thus \( xA[c] \) is an A-submodule of \( A \).

Since \( A \) is Noetherian, \( xA[c] \) is finitely generated. Thus \( A[c] - xA[c] \)

is also a finitely generated A-module. Thus \( c \) is integral over \( A \).

Since \( A \) is integrally closed in \( K \), \( c \subseteq A \). We have proved that \( p^{-1}A \)

Then \( \frac{1}{p} \subseteq A \). This is impossible because \( p^{-1}p = A \).

Therefore we must have \( a \neq p^{-1}a \). By the maximality of \( a \),

\( p^{-1}a \) is invertible. Let \( I = \{ x \in K : xp^{-1}a \subseteq A \} \) be its inverse. Then

\( I(p^{-1}a) = A \). For every \( x \in I \), \( xA \subseteq A \). Therefore, \( x \subseteq A \).

Thus by definition, \( x \in A \). This means \( IA^{-1} \subseteq A^{-1} \). Then

\( IA^{-1} \subseteq A^{-1} \). Thus \( IA^{-1} \subseteq A^{-1} \). Consequently,

\( IA^{-1} \subseteq A^{-1} \). Therefore, \( IA^{-1} \subseteq A^{-1} \). Consequently,

\( IA^{-1} \subseteq A^{-1} \). Therefore, \( IA^{-1} \subseteq A^{-1} \). Consequently,

\( IA^{-1} \subseteq A^{-1} \). Therefore, \( IA^{-1} \subseteq A^{-1} \). Consequently,

\( IA^{-1} \subseteq A^{-1} \). Therefore, \( IA^{-1} \subseteq A^{-1} \). Consequently,

\( IA^{-1} \subseteq A^{-1} \). Therefore, \( IA^{-1} \subseteq A^{-1} \). Consequently,

\( IA^{-1} \subseteq A^{-1} \). Therefore, \( IA^{-1} \subseteq A^{-1} \). Consequently,

\( IA^{-1} \subseteq A^{-1} \). Therefore, \( IA^{-1} \subseteq A^{-1} \). Consequently,

\( IA^{-1} \subseteq A^{-1} \). Therefore, \( IA^{-1} \subseteq A^{-1} \). Consequently,

\( IA^{-1} \subseteq A^{-1} \). Therefore, \( IA^{-1} \subseteq A^{-1} \). Consequently,

\( IA^{-1} \subseteq A^{-1} \). Therefore, \( IA^{-1} \subseteq A^{-1} \). Consequently,

\( IA^{-1} \subseteq A^{-1} \). Therefore, \( IA^{-1} \subseteq A^{-1} \). Consequently,

\( IA^{-1} \subseteq A^{-1} \). Therefore, \( IA^{-1} \subseteq A^{-1} \). Consequently,

\( IA^{-1} \subseteq A^{-1} \). Therefore, \( IA^{-1} \subseteq A^{-1} \). Consequently,

\( IA^{-1} \subseteq A^{-1} \). Therefore, \( IA^{-1} \subseteq A^{-1} \). Consequently,

\( IA^{-1} \subseteq A^{-1} \). Therefore, \( IA^{-1} \subseteq A^{-1} \). Consequently,

\( IA^{-1} \subseteq A^{-1} \). Therefore, \( IA^{-1} \subseteq A^{-1} \). Consequently,

\( IA^{-1} \subseteq A^{-1} \). Therefore, \( IA^{-1} \subseteq A^{-1} \). Consequently,

\( IA^{-1} \subseteq A^{-1} \). Therefore, \( IA^{-1} \subseteq A^{-1} \). Consequently,

\( IA^{-1} \subseteq A^{-1} \). Therefore, \( IA^{-1} \subseteq A^{-1} \). Consequently,

\( IA^{-1} \subseteq A^{-1} \). Therefore, \( IA^{-1} \subseteq A^{-1} \). Consequently,

\( IA^{-1} \subseteq A^{-1} \). Therefore, \( IA^{-1} \subseteq A^{-1} \). Consequently,

\( IA^{-1} \subseteq A^{-1} \). Therefore, \( IA^{-1} \subseteq A^{-1} \). Consequently,

\( IA^{-1} \subseteq A^{-1} \). Therefore, \( IA^{-1} \subseteq A^{-1} \). Consequently,

\( IA^{-1} \subseteq A^{-1} \). Therefore, \( IA^{-1} \subseteq A^{-1} \). Consequently,

\( IA^{-1} \subseteq A^{-1} \). Therefore, \( IA^{-1} \subseteq A^{-1} \). Consequently,

\( IA^{-1} \subseteq A^{-1} \). Therefore, \( IA^{-1} \subseteq A^{-1} \). Consequently,
\[ A = (I_p)^{-1} \leq a^t a. \]

Thus \( a^t a = A \), which is a contradiction.

(3) Problem 1, Lang, p. 374

Denote by Aut(C) the set of all field automorphisms of C. We will show that Aut(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 \( |\mathbb{R}| < 2^{\aleph_0} = |\mathbb{C}| \), it is not algebraic over \( \mathbb{Q} \).

Let \( B = \{X_i : i \in I\} \neq \emptyset \) be a transcendental basis of \( C \) over \( \mathbb{Q} \). Put \( K = \mathbb{Q}(B) \). Then \( K \subset C \) is an algebraic extension.

Thus, \( |K| = |C| \). We'll show that \( B \) is an uncountable set. Suppose by contradiction that \( B \) is at most countable. Then we can write \( B = \{X_1, X_2, X_3, \ldots\} \). Then

\[ K = \mathbb{Q}(X_1, X_2, \ldots) = \bigcup_{k=1}^{\infty} \mathbb{Q}(X_1, \ldots, X_k). \quad (\#) \]

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 \( \mathbb{Z} \times X^* \to (a_0, a_1, \ldots) \).

Thus \( \mathbb{Q}[X] \) 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 \( \mathbb{A} \). Thus \( \mathbb{A}[X] \) is countable. Then \( \mathbb{A}[X] \times \mathbb{A}[X] \) is also countable. We have a surjective map \( \mathbb{A}[X] \times (\mathbb{A}[X] \setminus \{0\}) \to \mathbb{A}(X) \) defined by \((f, g) \mapsto \frac{f}{g}\). Thus \( \mathbb{A}(X) \) is also countable. Then by induction in \( k \) we have \( \mathbb{A}(X_1, \ldots, X_{k-1}, X_k) = \mathbb{A}(X_1, \ldots, X_{k-1})(X_k) \) is also countable. Then by \((\star)\), \( K \) is countable. This is a contradiction because \(|K| = |I|!\). Therefore \( B \) is uncountable. Thus \(|B| > |I|!\).

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 \( \mathbb{A} \). Then we can define a field isomorphism \( f_A : K \to K \) which induces identity on \( \mathbb{A} \) and \( f(X_j) = Y_j \) for \( j \in I \). 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 \( C \). Since \( K \subset C \) is algebraic and \( C \) is
algebraically closed, \( \mathcal{A} \) can extend to an embedding \( \mathcal{A} \hookrightarrow \mathcal{C} \). Then \( \mathcal{A} \subset \text{Aut}(\mathcal{C}) \). Thus we get an injective map \( \phi: \mathcal{P}(\mathcal{A}) \rightarrow \text{Aut}(\mathcal{A}) \),

\[
\phi(A) = \mathcal{A}.
\]

Thus, \( |\text{Aut}(\mathcal{A})| \geq |\mathcal{P}(\mathcal{A})| = 2^{\aleph_0} = 2^{\aleph_1} \geq 2^{\aleph_1} \).

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

\[
|\text{Aut}(\mathcal{C})| \leq |\mathcal{C}|^{|\mathcal{C}|} = (2^{|\mathcal{N}|})^{|\mathcal{C}|} = 2^{\mathcal{N}|\mathcal{C}|} = 2^{\aleph_1}.
\]

Therefore, \( |\text{Aut}(\mathcal{A})| = 2^{\aleph_1} = 2^{\aleph_1} \).

(4)(i) Let \( A \subseteq B \subseteq C \) 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 \( C = A[\gamma_1, \gamma_2, \ldots, \gamma_n] \). Because \( B \subseteq C \) is integral, each \( \gamma_i \) is a root of a monic polynomial over \( B \), namely \( f_i(X) \). Let \( \{f_1, f_2, \ldots, f_m\} \) be the set of all coefficients of \( f_1(X), f_2(X), \ldots, f_n(X) \). Then \( A[\gamma_1, \gamma_2, \ldots, \gamma_m] \subseteq B \). Put \( D = A[\gamma_1, \gamma_2, \ldots, \gamma_m] \). Then \( f_i(X) \in \mathcal{D}[X] \).

Thus each \( \gamma_i \) 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 \( A \subseteq E \) and \( x_1, x_2, \ldots, x_n \in E \), \( C = A[y_1, x_1, \ldots, x_n] \subseteq E \). 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 \( D \subseteq B \subseteq C \), \( B \) is a \( D \)-submodule of \( C \). Thus \( B \) is a finitely generated \( D \)-module. Then there exists \( y_1, y_2, \ldots, y_r \in B \) such that \( B = D[t_1, t_2, \ldots, t_r] \). Then

\[
B = A[y_1, \ldots, y_m] \langle t_1, t_2, \ldots, t_r \rangle = A[y_1, \ldots, y_m, t_1, \ldots, t_r].
\]

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
$B_\mathcal{A}$ is a finitely generated $A$-algebra.

First we will show that $B_\mathcal{A}$ is a subring of $B$. Obviously, $B_\mathcal{A}$ contains 0 and 1. For $x, y \in B_\mathcal{A}$, we have $\delta(x) = x$, $\delta(y) = y \forall \mathcal{A} \in \mathcal{A}$. Thus $\delta(xy) = \delta(x)\delta(y) = xy$ and $\delta(x+y) = \delta(x) + \delta(y) = x+y \forall \mathcal{A} \in \mathcal{A}$. Therefore $x+y \in B_\mathcal{A}$, and so $B_\mathcal{A}$ is a subring of $B$.

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

Take any $b \in B$. We are looking for a monic polynomial with coefficients in $B_\mathcal{A}$ of which $b$ is a root. Since $G$ is a finite group, we can write $G = \{\epsilon_1, \epsilon_2, \ldots, \epsilon_n\}$. Then we put

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

where $\epsilon_k = \epsilon_k (\epsilon_1(b), \ldots, \epsilon_n(b))$, and $\epsilon_k$ is the $k$'th symmetric polynomial of $n$ variables. Since $I(B) \subseteq B_\mathcal{A}$, there is some $k$ such that $\epsilon_k(b) = b$.

Thus $b$ is a root of $f(X)$. Now we will show that each $\epsilon_k \in B_\mathcal{A}$. 


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

\[
g(a_i) = g \left( e_i(g_1(b), \ldots, g_n(b)) \right) = e_i(g \circ g_1(b), \ldots, g \circ g_n(b)).
\]

Since \( G \) is a group, \( (g \circ g_1, \ldots, g \circ g_n) \) is just a permutation of \( (g_1, \ldots, g_n) \). Since \( e_i \) is a symmetric polynomial of \( n \) variables, we have

\[
e_i(g \circ g_1(b), \ldots, g \circ g_n(b)) = e_i(g_1(b), \ldots, g_n(b)) = a_i.
\]

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 \( \deg f = n > 1 \). We'll show that there is a ring \( B \) containing \( A \) and \( f \) such that \( f \) has a root in \( B \).

A and is finitely generated as an \( A \)-module. Let \( \bar{X} \) be a variable over \( A \). Put \( E = A[\bar{X}] / (f(\bar{X})) \). Then we have an inclusion map \( A \to E \) in which \( \alpha \mapsto [\alpha] = \alpha + (f(\bar{X})) \).

Now we view \( f \) as a polynomial \( \bar{f} \) over \( E \), namely

We write \( f(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0 \) 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 \( \bar{f} \) over \( E \), namely

\[
\bar{f}(X) = X^n + \bar{a}_{n-1}X^{n-1} + \ldots + \bar{a}_1X + \bar{a}_0.
\]
We have \( \hat{X} \in E \) and
\[
\hat{f}(\hat{X}) = \hat{X}^n + [a_{n-1}] \hat{X}^{n-1} + \ldots + [a_1] \hat{X} + [a_0]
\]
\[
= (\hat{X}^n + a_{n-1} \hat{X}^{n-1} + \ldots + a_0) + (\hat{f}(\hat{X}))
\]
\[
= \hat{f}(\hat{X}) + (\hat{f}(\hat{X}))
\]
\[
= [0].
\]

Therefore \( \hat{f} \) 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
\[
\hat{X}^n = [a_{n-1}] \hat{X}^{n-1} + \ldots + [a_1] \hat{X} + [a_0]
\]
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
\[
\hat{X}^m = [b_{n-1}] \hat{X}^{n-1} + \ldots + [b_1] \hat{X} + [b_0]
\]
then
\[
\hat{X}^{m+1} = \hat{X} \hat{X}^m = [b_{n-1}] \hat{X}^n + [b_{n-2}] \hat{X}^{n-1} + \ldots + [b_2] \hat{X}^2 + [b_1] \hat{X} + [b_0]
\]
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 note: