Solutions to Homework 3.

(1) For a polynomial $P(t) \in \mathbb{Q}$ show that the following conditions are equivalent:

(a) $P(n) \in \mathbb{Z}$ for all integers $n \in \mathbb{Z}$.

(b) $P(n) \in \mathbb{Z}$ for all but finitely many integers $n \in \mathbb{Z}$.

(c) $P(t) = \sum_{i=0}^{n} a_i \binom{t}{i}$ with $a_i \in \mathbb{Z}$ and $n \in \mathbb{N}$ suitable.

Proof. (a) $\Leftarrow$ (b) trivial

(b) $\Leftarrow$ (c) Note that the set $\{\binom{t}{i}\}_{i\in\mathbb{N}_0}$ is a basis of the $\mathbb{Q}$-vector space $\mathbb{Q}[t]$, where $\binom{t}{0} = 1$ and $\binom{t}{i} = (1/i!)t(t-1)\dots(t-i+1)$ for $i > 0$. Write $P(t) = \sum_{i=0}^{n} a_i \binom{t}{i}$ where $a_i \in \mathbb{Q}$ and $a_n \neq 0$. We proceed by induction on $n = \deg(P(t))$. For the induction step consider the polynomial $Q(t) = P(t+1) - P(t)$. Then

$$Q(t) = \sum_{i=0}^{n} a_i[\binom{t+1}{i} - \binom{t}{i}] = \sum_{i=1}^{n} a_i \binom{t}{i-1}.$$

Thus $\deg(Q(t)) = n - 1$ and by induction hypothesis $a_1, \dots, a_n \in \mathbb{Z}$. This implies that $a_0 \in \mathbb{Z}$.

(c) $\Leftarrow$ (a) trivial

(2) Show that $S = \{P(t) \in \mathbb{Q}[t] \,|\, P(n) \in \mathbb{Z} \text{ for all } n \in \mathbb{Z}\}$ is a non-Noetherian subring of $\mathbb{Q}[t]$.

Proof. Note that S is a subring of $\mathbb{Q}[t]$ with $\mathbb{Z}[t] \subseteq S \subseteq \mathbb{Q}[t]$. Since $\dim(\mathbb{Z}[t]) = 2$, the Krull-Akizuki theorem does not apply.

We want to show that the ideal

$$P = (\binom{t}{i})_{i\geq 1}$$

is not finitely generated. Suppose that P is finitely generated. Then there is an $n \in \mathbb{N}$ so that

$$P = (\binom{t}{1}, \dots, \binom{t}{n}).$$

Hence for all $i > n$

$$\binom{t}{i} = \sum_{j=1}^{n} h_{ij} \binom{t}{j}$$

where $h_{ij} \in S$. Write

$$h_{ij} = \sum_{k=0}^{m} a_{ijk} \binom{t}{k}$$

where $a_{ijk} \in \mathbb{Z}$. Thus

$$\binom{t}{i} = \sum_{j=1}^{n}\sum_{k=0}^{n} a_{ijk} \binom{t}{k}\binom{t}{j} + \sum_{j=1}^{n}\sum_{k>n} a_{ijk} \binom{t}{k}\binom{t}{j}.$$

For all $k > n$ write

$$\binom{t}{k} = \sum_{j=1}^{n} h_{kj} \binom{t}{j}$$

and substitute

$$\begin{aligned}\binom{t}{i} &= \sum_{j=1}^{n}\sum_{k=0}^{n} a_{ijk}\binom{t}{k}\binom{t}{j} + \sum_{j,\ell=1}^{n}\sum_{k>n} a_{ijk}h_{k\ell}\binom{t}{\ell}\binom{t}{j} \\ &= \sum_{j=1}^{n}\sum_{k=0}^{n} a_{ijk}\binom{t}{k}\binom{t}{j} + \sum_{j,\ell=1}^{n} \tilde{h}_{k\ell}\binom{t}{\ell}\binom{t}{j}.\end{aligned}$$

Repeat by writing $\tilde{h}_{k\ell} = \sum_{u=0}^{s} a_{k\ell u}\binom{t}{u}$ where $a_{k\ell u} \in \mathbb{Z}$. After $i+1$ steps we obtain that

$$\begin{aligned}\binom{t}{i} = &\sum_{0\le \nu_j \le n} u_{\nu_1,\dots,\nu_{i+1}}\binom{t}{\nu_1}\cdots\binom{t}{\nu_{i+1}} \\ &+ \sum_{1\le \mu_j \le n} v_{\mu_1,\dots,\mu_{i+1}}\binom{t}{\mu_1}\cdots\binom{t}{\mu_{i+1}}\end{aligned}$$

where $u_{\nu_1,\dots,\nu_{i+1}} \in \mathbb{Z}$ and $v_{\mu_1,\dots,\mu_{i+1}} \in S$. Note that every term in the last sum has degree $> i$. Thus the leading term $(1/i!)t^i$ of $\binom{t}{i}$ corresponds to the i degree term of

$$(*) \qquad \sum_{0\le \nu_j \le n} u_{\nu_1,\dots,\nu_{i+1}}\binom{t}{\nu_1}\cdots\binom{t}{\nu_{i+1}}.$$

Let $i = q$ be a prime number with $q > n$ and set $m = n!$. Then every coefficient in $(*)$ is in $\mathbb{Z}_m$ while $1/q!$ is not an element of $\mathbb{Z}_m$, a contradiction. Thus P is not finitely generated and S is not Noetherian.

(3) Let A be a ring and $n \in \mathbb{N}$ an integer. Suppose that every ideal of A is generated by at most n elements. Show that $\dim(A) \le 1$.

Proof. First note that A is a Noetherian ring. We need to show that for every prime ideal $P \subseteq A$, $\mathrm{ht}P = \dim(A_P) \le 1$. Since every ideal of A_P is extended from an ideal of A, we may assume that A is a local Noetherian ring with maximal ideal $\mathfrak{m}$ and that every ideal of A is generated by at most n elements. Let $P(t) \in \mathbb{Q}[t]$ be the Hilbert-Samuel polynomial of A with respect to the maximal ideal $\mathfrak{m}$, that is, for $s \in \mathbb{N}$ with $s \ge n_0$:

$$P(s) = \ell_A(A/\mathfrak{m}^{s+1}) = \sum_{i=0}^{s} \ell_A(\mathfrak{m}^i/\mathfrak{m}^{i+1}).$$

Since $\ell_A(\mathfrak{m}^i/\mathfrak{m}^{i+1})$ is the minimal number of generators of the ideal $\mathfrak{m}^i$, it follows that

$$P(s) \le (s+1)n$$

where n is a fixed integer. This implies that $\deg(P(t)) \le 1$. Since $\deg(P(t)) = \dim(A)$ the assertion follows.

(4) Let $f \in \mathbb{C}[x_1,\dots,x_n]$ be an irreducible polynomial and let $Y = Z(f)$ be the algebraic variety defined by f. Y is called *non-singular* or *smooth* at a point $P \in Y$ if not all of the partial derivatives $\partial f/\partial x_i$ vanish at P. Let $A(Y)$ be the coordinate ring of Y and let $\mathfrak{m}_P \subseteq A(Y)$ be the maximal ideal of $A(Y)$ corresponding to P

(that is, if $P = (a_1, \dots, a_n)$, then $\mathfrak{m}_P = (x_1 - a_1, \dots, x_n - a_n)/(f)$). Show that Y is smooth at P if and only if the ring $A(Y)_{\mathfrak{m}_P}$ is regular.

Proof. In the following set $R = \mathbb{C}[x_1, \dots, x_n]$. First note that there are the following equivalences:

$$\begin{aligned} P = (a_1, \dots, a_n) \in Y = Z(f) &\Leftrightarrow f(a_1, \dots, a_n) = 0 \\ &\Leftrightarrow f(x_1, \dots, x_n) \in (x_1 - a_n, \dots, x_n - a_n) \\ &\Leftrightarrow f(x_1, \dots, x_n) = \sum_{i=1}^{n} h_i(x_i - a_i) \end{aligned}$$

where $h_i \in R$. (Note that the forward direction is an application of Taylor's formula.) Thus for all $1 \le i \le n$:

$$\partial f/\partial x_i = \sum_{j=1}^{n} \partial h_j/\partial x_i(x_j - a_j) + h_i.$$

Thus P is a non-singular point of Y if and only if $h_i(a_1, \dots, a_n) \neq 0$ for some $1 \le i \le n$, or equivalently, $h_i \notin (x_1 - a_1, \dots, x_n - a_n)$ for some $1 \le i \le n$. Set $\mathfrak{m} = (x_1 - a_1, \dots, x_n - a_n) \subseteq R$.
Claim: $h_i \notin \mathfrak{m} \Leftrightarrow$ the maximal ideal $\mathfrak{m}R_{\mathfrak{m}}$ of $R_{\mathfrak{m}}$ is generated by $x_1 - a_1, \dots, x_{i-1} - a_{i-1}, f, x_{i+1} - a_{i+1}, \dots, x_n - a_n$.
Proof of Claim: " $\Rightarrow$ " Since h_i is a unit in $R_{\mathfrak{m}}$:

$$\begin{aligned} &(x_1 - a_1, \dots, x_{i-1} - a_{i-1}, f, x_{i+1} - a_{i+1}, \dots, x_n - a_n)R_{\mathfrak{m}} = \\ &(x_1 - a_1, \dots, x_{i-1} - a_{i-1}, h_i(x_i - a_i), x_{i+1} - a_{i+1}, \dots, x_n - a_n) = \\ &(x_1 - a_1, \dots, x_{i-1} - a_{i-1}, x_i - a_i, x_{i+1} - a_{i+1}, \dots, x_n - a_n) = \\ &\mathfrak{m}R_{\mathfrak{m}} \end{aligned}$$

" $\Leftarrow$ " If $h_i \in \mathfrak{m}$ for all $1 \le i \le n$, then $f \in \mathfrak{m}^2$ and $\mathfrak{m}/\mathfrak{m}^2 = \mathfrak{m}/((f) + \mathfrak{m}^2)$. Thus the maximal ideal of $R_{\mathfrak{m}}/(f)R_{\mathfrak{m}}$ is minimally generated by n elements ($\dim(\mathfrak{m}/(f) + \mathfrak{m}^2) = n$) and f is not part of a minimal system of generators of $\mathfrak{m}$. This shows that claim.

Thus P is a smooth point of Y if and only if f is part of a minimal system of generators of $\mathfrak{m}R_{\mathfrak{m}}$ or, equivalently, if and only if $\operatorname{edim}((R/(f))_{\mathfrak{m}}) = n - 1 = \dim((R/(f))_{\mathfrak{m}})$. Since $R/(f) = A(Y)$ we have that P is smooth on Y if and only if $A(Y)$ is a regular local ring at P.

(5) Let K be a field, $R = K[x_1, \dots, x_n]$ the polynomial ring over K, and $I \subseteq R$ an ideal. Show that:

$$\operatorname{ht} I + \dim(R/I) = \dim(R).$$

Proof. (a) We first show that we may assume that I is a prime ideal of R. Suppose that for every prime ideal $P \subseteq R$:

$$\operatorname{ht} P + \dim(R/P) = \dim(R) = n.$$

Let $I \subseteq R$ be an ideal and let $P \subseteq R$ be a prime ideal with $I \subseteq P$ and $\operatorname{ht} I = \operatorname{ht} P$. Assume that $\operatorname{ht} I + \dim(R/I) \neq n$. Since $\operatorname{ht} P + \dim(R/P) = n$, this implies that

$\dim(R/I) > \dim(R/P)$. Let $Q \subseteq R$ be a prime ideal with $I \subseteq Q$ and $\dim(R/I) = \dim(R/Q)$. Since $\dim(R/Q) = n - \mathrm{ht}Q > \dim(R/P) = n - \mathrm{ht}P$ it follows that $\mathrm{ht}P > \mathrm{ht}Q$, a contradiction, since $\mathrm{ht}I = \inf\{\mathrm{ht}P \,|\, I \subseteq P \in \mathrm{Spec}(R)\}$.
(b) We claim that every maximal ideal of R has height n. The proof is by induction on n. The case $n = 1$ is trivial. Suppose that $n > 1$ and that $\mathfrak{m} \in R$ is a maximal ideal of R. Then $R/\mathfrak{m} = K[\alpha_1, \ldots, \alpha_n]$ is an algebraic field extension of K. By (3.15) $\mathfrak{m} = (f_1, \ldots, f_n)$ where $f_i \in K[x_1, \ldots, x_i]$ monic in x_i. Set $L = K[x_1]/(f_1)$, where f_1 is the minimal polynomial of α_1 over K. Then $\bar{\mathfrak{m}} = \mathfrak{m}/(f_1)$ is a maximal ideal of $L[x_2, \ldots, x_n]$ and by induction hypothesis $\mathrm{ht}\bar{\mathfrak{m}} = n-1$. Therefore $\mathrm{ht}\mathfrak{m} = n$.
(c) Let $P \subseteq R$ be a prime ideal. If P is maximal, then by (b):

$$\mathrm{ht}P + \dim(R/P) = n.$$

Suppose that $\dim(R/P) = r > 0$. The elements $x_1 + P, \ldots, x_n + P$ generate the quotient field $Q(R/P)$ over K. Moreover, $Q(R/P)$ has transcendence degree r over K and we may assume that $x_1 + P, \ldots, x_r + P$ is a transcendence basis of $Q(R/P)$ over K. This implies that $P \cap K[x_1, \ldots, x_r] = 0$. If Q is a prime ideal of R with $P \subseteq Q$ and $P \neq Q$, then

$$\dim(R/Q) < \dim(R/P).$$

Thus $Q(R/Q)$ has transcendence degree $< r$ over K. This implies that for all prime ideals Q with $P \subseteq Q$ and $P \neq Q$,

$$Q \cap K[x_1, \ldots, x_r] \neq 0$$

and with $S = K[x_1, \ldots, x_r] - (0)$ the ideal $PS^{-1}R$ is maximal in $S^{-1}R$. Note that

$$S^{-1}R = L[x_{r+1}, \ldots, x_n]$$

where $L = K(x_1, \ldots, x_r) = Q(K[x_1, \ldots, x_r])$. By (b),

$$\mathrm{ht}PS^{-1}R = \mathrm{ht}P = n - r.$$

This shows that $\mathrm{ht}P + \dim(R/P) = n$.

(6) Let $A \subseteq B$ be an extension of rings such that the set $B - A$ is closed under multiplication. Show that A is integrally closed in B.

Proof. Let $b \in B - (0)$ be integral over A. Then there is a minimal integer $n \in \mathbb{N}$ so that b satisfies an integral equation of degree n:

$$b^n + a_{n-1}b^{n-1} + \ldots + a_1 b + a_0 = 0 \quad \text{with} \quad a_i \in A.$$

Since n is minimal, $b \in A$ if and only if $n = 1$. If $b \notin A$ and $n > 1$, then

$$b^{n-1} + a_{n-1}b^{n-2} + \ldots + a_1 \notin A,$$

but

$$b(b^{n-1} + a_{n-1}b^{n-2} + \ldots + a_1) = -a_0 \in A,$$

a contradiction. Hence $n = 1$ and $b \in A$.

(7) Let A be a normal domain, $K = Q(A)$ its field of quotients, and $f(x) \in A[x]$ a monic polynomial. Show that $f(x)$ is irreducible in $K[x]$ if and only if $f(x)$ is irreducible in $A[x]$.

Proof. Let $\bar{K}$ denote the algebraic closure of K. Suppose that $f = gh$ with $g, h \in K[x]$ monic polynomials and g irreducible in $K[x]$. Let $\alpha \in \bar{K}$ be a root of g. Then $f(\alpha) = 0$ and α is integral over A, since $f \in A[x]$ is monic. Note that g is the minimal polynomial of α over K. By (5.18), $g \in A[x]$. This shows that every monic irreducible component of f in $K[x]$ is a polynomial in $A[x]$. Thus f is reducible in $A[x]$. The converse is trivial.

(8) Let $K \subseteq L$ be an extension of fields, $Q \subseteq L[x_1, \ldots, x_n]$ a prime ideal in the polynomial ring in n variables over L, and $P = Q \cap K[x_1, \ldots, x_n]$ its contraction to the polynomial ring over K. Show that $\mathrm{ht}Q \geq \mathrm{ht}P$ and that equality holds if L is algebraic over K. Use this to show that if two polynomials $f, g \in K[x_1, \ldots, x_n]$ have no common divisor in $K[x_1, \ldots, x_n]$, then f and g have no common divisor in $L[x_1, \ldots, x_n]$.

Proof. Consider the extension of rings:

$$A = K[x_1, \ldots, x_n]/P \subseteq B = L[x_1, \ldots, x_n]/Q.$$

Suppose (after renumbering if necessary) that $x_1 + P, \ldots, x_r + P$ is a transcendence basis of A over K. Thus for $r + 1 \leq i \leq n$ the element $x_i + P$ is algebraic over $K(x_1 + P, \ldots, x_r + P) \subseteq Q(A)$, where $Q(A)$ is the quotient field of A. This implies that $x_i + Q \in B$ is algebraic over $L(x_1 + Q, \ldots, x_r + Q)$ for all $r + 1 \leq i \leq n$. Therefore

$$\dim(B) = \mathrm{trdeg}_L(B) \leq \mathrm{trdeg}(A) = \dim(A).$$

By problem (5)

$$n - \mathrm{ht}Q = \dim(B) \leq n - \mathrm{ht}P = \dim(A)$$

and thus $\mathrm{ht}Q \geq \mathrm{ht}P$. If $K \subseteq L$ is algebraic, the extension $K[x_1, \ldots, x_n] \subseteq L[x_1, \ldots, x_n]$ is integral. By (5.25): $\mathrm{ht}P \geq \mathrm{ht}Q$ and hence $\mathrm{ht}Q = \mathrm{ht}P$.

Suppose that $K \subseteq L$ is algebraic and that $q \in L[x_1, \ldots, x_n]$ is a prime element with $q \,|\, f$ and $q \,|\, g$. The prime element q generates the height one prime ideal $Q = (q) \in L[x_1, \ldots, x_n]$. Thus $P = Q \cap K[x_1, \ldots, x_n]$ is a prime ideal of height one which is principal, $P = (p)$. Since $f, g \in P$, f and g have the common divisor p in $K[x_1, \ldots, x_n]$.

(9) Let $A \subseteq B$ be an integral extension of domains with A a normal domain, and $K = Q(A)$ the field of quotients of A. Let $I \subseteq A$ be an ideal, $b \in B$ an element, and $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$ the minimal polynomial of b over K. Show that $b \in \mathrm{rad}(IB)$ if and only if $a_i \in \mathrm{rad}(I)$ for all $0 \leq i \leq n-1$.

Proof. " $\Leftarrow$ " If $a_i \in \mathrm{rad}(I)$ for all $0 \leq i \leq n-1$, then $b^n = -(a_{n-1}b^{n-1} + \ldots + a_0) \in \mathrm{rad}(I)B \subseteq \mathrm{rad}(B)$.

" $\Rightarrow$ " First note that $f(x) \in A[x]$, since A is normal. We claim that

$$(*) \quad \mathrm{rad}(IB) \cap A = \mathrm{rad}(I).$$

The inclusion " $\supseteq$ " is trivial. For the other inclusion note that

$$\mathrm{rad}(IB) = \cap_{I \subseteq Q} Q$$

and

$$\mathrm{rad}(I) = \cap_{I \subseteq P} P$$

where Q and P are prime ideals in B and A, respectively. For every prime ideal $P \in \mathrm{Spec}(A)$ there is a prime ideal $Q \in \mathrm{Spec}(B)$ with $P = Q \cap A$. Thus $\mathrm{rad}(IB) \subseteq \mathrm{rad}(I)$. (Note that the claim is true for any integral extension $A \subseteq B$.)

Since $A \subseteq B$ is integral, the extension of the quotient fields $K = Q(A) \subseteq L = Q(B)$ is algebraic. Let $\bar{K} = \bar{L}$ be the algebraic closure of K and L, and let $\bar{B}$ be the integral closure of A (or B) in $\bar{L}$. Assume that $\beta_1, \ldots, \beta_n$ are the distinct roots of $f(x)$ in $\bar{L}$ with $b = \beta_1$. Then $\beta_1, \ldots, \beta_r \in \bar{B}$. Every automorphism $\tau \in \mathrm{Aut}_K(\bar{L})$ restricts to an automorphism $\tau|_{\bar{B}}$ of $\bar{B}$. For all $1 \leq i \leq r$ let $\sigma_i \in \mathrm{Aut}_K(\bar{L})$ be a K-automorphism with $\sigma_i(b) = \beta_i$. Since $b \in \mathrm{rad}(IB)$, also $\sigma_i(b) = \beta_i \in \mathrm{rad}(I\bar{B})$ for all $1 \leq i \leq r$. Since the coefficients a_j of $f(x)$ are elementary symmetric functions in the β_i, we have that $a_i \in \mathrm{rad}(I\bar{B})$ for all $0 \leq i \leq n-1$. Thus by $(*)$ $a_i \in \mathrm{rad}(I)$ for all $0 \leq i \leq n-1$.