MATH 602 (HOMEWORK 5)

HIDENORI SHINOHARA

Exercise. (1) This can be proved using induction. The base case $m = 1$ is trivial. Suppose that the proposition has been shown for some $m \in \mathbb{N}$. We will show the $(m+1)$ case. By the definition of a determinant,

$$\Delta = \sum_{k=1}^{m+1} (-1)^{k+1} \det(M_{k,1})$$

where $M_{k,1}$ is the matrix obtained by deleting the kth row and 1st column. We can apply the inductive hypothesis to each $M_{k,1}$ because, for instance, when $k = 1$,

$$\begin{aligned}
\det(M_{1,1}) &= \det \begin{bmatrix} \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^m \\ & \ddots & & \\ \alpha_{m+1} & \alpha_{m+1}^2 & \cdots & \alpha_{m+1}^m \end{bmatrix} \\
&= \alpha_2 \cdots \alpha_{m+1} \det \begin{bmatrix} 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{m-1} \\ & \ddots & & & \\ 1 & \alpha_{m+1} & \alpha_{m+1}^2 & \cdots & \alpha_{m+1}^{m-1} \end{bmatrix} \\
&= \alpha_2 \cdots \alpha_{m+1} \prod_{2 \le i < j \le m} (\alpha_j - \alpha_i).
\end{aligned}$$

A similar argument can be applied to other cases and we obtain

$$\Delta = \sum_{k=1}^{m+1} (-1)^{k+1} (\alpha_1 \cdots \hat{\alpha_k} \cdots \alpha_m) \prod_{i<j, i \neq k, j \neq k} (\alpha_j - \alpha_i).$$

It can be observed that, for each $k = 1, \cdots, m+1$, the kth term $(\alpha_1 \cdots \hat{\alpha_k} \cdots \alpha_m) \prod_{i<j,i\neq k,j\neq k}(\alpha_j - \alpha_i)$ does not contain any α_k. On the other hand, for any $l \neq k$, every term that we obtain when expanding the lth term contains α_k. Therefore, it suffices to show that, for each k, the sum of all the terms in $\prod_{1 \le i<j \le m+1}(\alpha_j - \alpha_i)$ that do not contain α_k is equal to the kth term in the above expression.

$$\begin{aligned}
\prod_{1 \le i<j \le m+1} (\alpha_j - \alpha_i) &= \prod_{k+1 \le j} (\alpha_j - \alpha_k) \prod_{j \le k-1} (\alpha_k - \alpha_j) \prod_{1 \le i<j \le m+1, i \neq k, j \neq k} (\alpha_j - \alpha_i) \\
&= (-1)^{k-1} \prod_{j \neq k} (\alpha_j - \alpha_k) \prod_{1 \le i<j \le m+1, i \neq k, j \neq k} (\alpha_j - \alpha_i) \\
&= (-1)^{k-1} (\alpha_1 \cdots \hat{\alpha_k} \cdots \alpha_{m+1}) \prod_{1 \le i<j \le m+1, i \neq k, j \neq k} (\alpha_j - \alpha_i) + \alpha_k F(\alpha_1, \cdots, \alpha_{m+1}) \\
&= (-1)^{k+1} (\alpha_1 \cdots \hat{\alpha_k} \cdots \alpha_{m+1}) \prod_{1 \le i<j \le m+1, i \neq k, j \neq k} (\alpha_j - \alpha_i) + \alpha_k F(\alpha_1, \cdots, \alpha_{m+1})
\end{aligned}$$

for some polynomial F.

$\Delta^2 \neq \prod_{i\neq j}(\alpha_j - \alpha_i)$ in general. Let $\alpha_1 = 0, \alpha_2 = 1$. Then $\det(A)^2 = \det \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}^2 = 1$. On the other hand, $\prod_{i\neq j}(\alpha_j - \alpha_i) = (0-1)(1-0) = -1$.

Exercise. (2(a)) By the primitive element theorem, $L = K[\alpha]$. Let E be the splitting field of α. Then E is a Galois extension of K. Let C denote the integral closure of A in E. Since E/K is Galois, C must be a finitely generated A-module. Then we have $A \subset B \subset C$, so B must be a finitely generated module since A is Noetherian.

Therefore, it suffices to consider the cases when the extension is Galois.

Exercise. (2(b)) Since $L = K[\alpha]$, $1/\alpha = a_n\alpha^{n-1} + \cdots + a_1\alpha^0$ with $a_n \neq 0$. Thus $0 = a_n\alpha^n + \cdots + a_1\alpha^1 - 1$. This implies $0 = a_n^n\alpha^n + \cdots + a_n^{n-1}a_1\alpha^1 - a_n^{n-1}$, so $0 = (a_n\alpha)^n + a_{n-1}(a_n\alpha)^{n-1} + \cdots + a_n^{n-2}\alpha_1(a_n\alpha)^1 - a_n^{n-1}$. Therefore, $a_n\alpha$ satisfies a monic polynomial with coefficients in A, so $a_n\alpha$ is integral over A. Moreover, $\alpha \in K[a_n\alpha]$, so $L = K[a_n\alpha]$.

Exercise. (2(c)) Any $b \in B$ satisfies a monic polynomial with coefficients in A. $\sigma(b)$ satisfies the same monic polynomial since σ fixes all the coefficients, so $\sigma(b) \in B$.

Exercise. (2(d)) Let A denote the Vandermonde matrix, k denote the column vector with k_i's and σ denote the column vector with $\sigma_i(b)$. Then $\det(A)k = \mathrm{adj}(A)Ak = \mathrm{adj}(A)\sigma$. By part (b) and (c), $\det(A), \mathrm{adj}(A), \sigma$ all live in B. Thus $\det(A)k_i$ lives in B. Therefore, $\det(A)^2 k_i \in B$.

Exercise. (2(e))

$$\begin{aligned}
\prod_{\tau\neq\sigma}(\sigma(\alpha) - \tau(\alpha)) &= \prod_{\tau\neq\sigma}(\sigma(\alpha) - \sigma(\sigma^{-1}(\tau(\alpha)))) \\
&= \prod_{\sigma}\sigma(\prod_{\tau\neq\sigma}(\alpha - \sigma^{-1}(\tau(\alpha)))) \\
&= \prod_{\sigma}\sigma(\prod_{\tau\neq\sigma}(\alpha - \tau(\alpha)))
\end{aligned}$$

Exercise. (3) Let $x_1, \cdots, x_m$ be generators of C as an A-algebra, and let $y_1, \cdots, y_n$ be generators of C as a B-module. Since $y_1, \cdots, y_n$ generate C as a B-module, every element in C can be expressed as a linear combination of y_i's over B. Specifically, $x_i = \sum b_{ij}y_j$ and $y_iy_j = \sum b_{ijk}y_k$ for some $b_{ij}, b_{ijk} \in B$. Let B_0 be the A-algebra generated by b_{ij} and b_{ijk}. Clearly, $A \subset B_0 \subset B$. Since A is Noetherian, B_0 is Noetherian.

Every element of C is a finite sum of monomials consisting of x_i's with coefficients in A. Since each x_i can be written as a linear combination of y_i's over B_0, every element in C can be written as a finite sum of monomials of y_i's with coefficients in B_0. Since every y_iy_j can be written as a linear combination of y_i's over B_0, every element in C can be written as a linear combination of y_i's over B_0. Therefore, C is finitely generated as a B_0-module. B_0 is Noetherian and B is a submodule of C, B is finitely generated as a B_0-module. Since B_0 is finitely generated as an A-algebra, it follows that B is finitely generated as an A-algebra.

Exercise. (4) Let K denote the field of fractions of A. Let $a/b \in K$ be an element integral over A. Since A is a UFD, we assume that there is no irreducible element q that divides both a and b. Since a/b is integral over A, $(a/b)^n + c_{n-1}(a/b)^{n-1} + \cdots + c_0 = 0$ for some $c_0, \cdots, c_{n-1} \in A$. This implies $a^n + b(c_{n-1}a^{n-1} + c_{n-1}ba^{n-2} + \cdots + c_0 b^{n-1}) = 0$. Then every irreducible element that divides b divides a^n, so every irreducible element that divides b divides a. Since there exists no irreducible element that divides both a and b, b must be a unit element. In other words, $a/b \in A$.

Exercise. (5) Since R is Noetherian, $\sqrt{I}$ is generated by finitely many elements. Let $g_1, \cdots, g_n$ denote a set of generators of $\sqrt{I}$.

For each i, there exists $m_i \geq 1$ such that $g_i^{m_i} \in I$. Let $N = \sum m_i$. Then $(\sqrt{I})^N = \sqrt{I} \cdots \sqrt{I}$ consists of elements of the form $(\sum_{i=1}^n x_{1,i} g_i) \cdots (\sum_{i=1}^n x_{N,i} g_i)$. Each term that we obtain by expanding it is of the from $x g_1^{k_1} \cdots g_n^{k_n}$ for some $k_1, \cdots, k_n$ with $k_1 + \cdots + k_n = N$. This implies that for at least one i, $m_i \geq k_i$, so each term in the expansion belongs to I. Therefore, every element in $(\sqrt{I})^N$ is in I.

Exercise. (6) Let $ab \in \sqrt{q}$. Then $a^n b^n \in q$ for some $n \in \mathbb{N}$. Then $a^n \in q$ or $(b^n)^m \in q$ for some $m \in \mathbb{N}$. If $a^n \in q$, then $a \in \sqrt{q}$. If $b^{nm} \in q$, then $b \in \sqrt{q}$. Therefore, $\sqrt{q}$ is prime.

Let $f : A \to B$ be given and q be a primary ideal of B. Let $ab \in f^{-1}(q)$. Then $f(a)f(b) \in q$, so $f(a) \in q$ or $(f(b))^m \in q$ for some $m \geq 1$. If $f(a) \in q$, then $a \in f^{-1}(q)$. If $f(b^m) \in q$, then $b^m \in f^{-1}(q)$. Therefore, $f^{-1}(q)$ is primary.

Exercise. (7) Since $\sqrt{I}$ is maximal, $I \neq R$.

Let $x + I, y + I \in A/I$ be two nonzero elements such that $(x + I)(y + I) = 0$. In other words, $xy \in I$. Since $I \subset \sqrt{I}$, $(x + \sqrt{I})(y + \sqrt{I}) = 0$. Since $\sqrt{I}$ is maximal, $A/\sqrt{I}$ is a field. Therefore, $x + \sqrt{I} = 0$ or $y + \sqrt{I} = 0$. In other words, $x \in \sqrt{I}$ or $y \in \sqrt{I}$. If $x \in \sqrt{I}$, then $x + I$ is nilpotent in $A + I$. Suppose $x \notin \sqrt{I}$. Since $\sqrt{I}$ is maximal, $(x) + \sqrt{I} = (1)$. Therefore, $ax + b = 1$ for some $a \in R$ and $b \in \sqrt{I}$. Since $b \in \sqrt{I}$, $b^n \in I$ for some $n \geq 1$. Therefore $1 = ((ax + b) + I)^n = (ax + b)^n + I = xc + I$ for some element c since $b^n + I = 0$. However, this implies $0 = (x + I)(y + I)(c + I) = y + I$, which is a contradiction. Therefore, $x + I$ must be nilpotent in $A + I$. By symmetry, $y + I$ must be nilpotent in $A + I$.

We have shown that every zero divisor in A/I is nilpotent, which is precisely the definition of a primary ideal.

Exercise. (8) Let $F = \{\operatorname{ann}(x) \mid 0 \neq x \in A\}$. Since A is Noetherian, F has a maximal element. We claim that every maximal element $\operatorname{ann}(x)$ in F is a prime ideal. Let $\operatorname{ann}(x)$ be a maximal element in F. Suppose $ab \in \operatorname{ann}(x)$ and $b \notin \operatorname{ann}(x)$. Since $\operatorname{ann}(x) \subset \operatorname{ann}(bx)$ and $\operatorname{ann}(x)$ is a maximal element, $\operatorname{ann}(x) = \operatorname{ann}(bx)$. Since $ab \in \operatorname{ann}(x)$, $abx = 0$, so $a \in \operatorname{ann}(bx)$. Therefore, $a \in \operatorname{ann}(x)$.

Let a be a zero divisor of A. Then $ay = 0$ for some $y \neq 0$ in $A/(0) = A$. In other words, $a \in \operatorname{ann}(y) \in F$. By the argument above, $a \in \operatorname{ann}(x)$ for some associated prime of (0) containing $\operatorname{ann}(y)$. The other direction is trivial from the definition of an associated prime.

Exercise. (9) Let $x \in (q : b)$. Then $xb \in q$. Since $b \notin q$, $x^n \in q$ for some $n \geq 1$. However, this implies $x \in p$. Since $(q : b) \subset p$, $\sqrt{(q : b)} \subset \sqrt{p} = p$. Clearly, $q \subset (q : b)$, so $p = \sqrt{q} \subset \sqrt{(q : b)}$. Therefore, $p = \sqrt{(q : b)}$.

We will now show that $\sqrt{(q : b)}$ is primary. Let x, y be chosen such that $xy \in (q : b)$. If $y^n \in (q : b)$ for some $n \geq 1$, we are done. In other words, if $y \in \sqrt{(q : b)} = p$, then we are done. Suppose otherwise. Then $xyb \in q$, so $(xb)y \in q$. This implies $xb \in q$ because $y \notin \sqrt{q}$. This implies $x \in (q : b)$, and we are done.

Exercise. (10) We will prove that there exists $n \in \mathbb{N}$ such that $N = \{m \in M \mid x^n m \in N\} \cap (x^n M + N)$ since the given problem statement does not make much sense. One direction is obvious because for any $n \in \mathbb{N}$, $N \subset \{m \in M \mid x^n m \in N\} \cap (x^n M + N)$. We will show the opposite direction. Let $A_n = \{m \in M \mid x^n m \in N\}$ for each n. Then $A_1 \subset A_2 \subset \cdots$ is an ascending chain of ideals. R is Noetherian, so there exists $n \in \mathbb{N}$ after which the chain stabilizes. Let $x^n a + b \in A_n \cap (x^n M + N)$ where $a \in M$ and $b \in N$. Then $x^n(x^n a + b) \in N$. Since $b \in N$, this implies $x^{2n} a \in N$. In other words, $a \in A_{2n}$. Since the chain stabilizes, $A_{2n} = A_n$. Thus $a \in A_n$, thus $x^n a \in N$. Hence, $x^n a + b \in N$.