Topics in Algebra solution

Sung Jong Lee, lovekrand.github.io

November 26, 2020

Problems in Section 5.1.

1. Prove that the mapping $\psi : F[x] \to F(a)$ defined by $h(x)\psi = h(a)$ is a homomorphism.

Proof. Let $f(x), g(x) \in F[x]$ where

$$f(x) = a_0 + a_1 x + \cdots a_n x^n,$$
$$g(x) = b_0 + b_1 x + \cdots b_m x^m.$$

Let $c_i = a_i + b_i$ for each valid i. In this case $a_i = 0, b_j = 0$ for $i > n+1, j > m+1$. Consequently, by setting $f(x) + g(x) = \sum_i^t c_i x^i$,

$$\begin{aligned}(f(x) + g(x))\psi &= \sum_{i=0}^{t} c_i a^i = \sum_{i=0}^{t} (a_i + b_i) a^i \\ &= \left(\sum_{i=0}^{t} (a_i) a^i + \sum_{i=0}^{t} (b_i) a^i \right) \\ &= f(a) + g(a) = f(x)\psi + g(x)\psi.\end{aligned}$$

Similarly for multiplication, set $c_i = \sum_k^i a_k b_{i-k}$ so that $f(x)g(x) = \sum_i^{m+n} c_i x^i$. Consequently,

$$(f(x)g(x))\psi = \sum_{i=0}^{m+n} c_i a^i = f(a)g(a) = f(x)\psi \cdot g(x)\psi.$$

Therefore, given ψ is clearly a homomorphism. □

2. Let F be a field and let $F[x]$ be the ring of polynomials in x over F. Let $g(x)$, of degree n, be in $F[x]$ and let $V = (g(x))$ be the ideal generated by $g(x)$ in $F[x]$. Prove that $F[x]/V$ is an n-dimensional vector space over F.

Proof. We claim that the set

$$\beta = \{1 + V, x + V, x^2 + V, \cdots, x^{n-1} + V\}$$

is a basis of $F[x]/V$. Suppose $f(x) + V \in F[x]/V$. Then by division algorithm, there is unique $r(x) \in F[x]$ such that $f(x) \equiv r(x) \bmod V$ with $deg(r(x)) < n = deg(g(x))$. So, we can write

$$r(x) = r_0 + r_1 x + \cdots + r_{n-1}x^{n-1}$$

for some $r_i \in F$, $0 \leq i \leq n-1$. Clearly,

$$\begin{aligned} f(x) + V = r(x) + V &= r_0 + r_1 x + \cdots + r_{n-1}x^{n-1} + V \\ &= r_0(1 + V) + r_1(x + V) + \cdots r_{n-1}(x^{n-1} + V) \end{aligned}$$

so that β spans $F[x]/V$. Now we show that β is linearly independent. Suppose

$$a_0(1 + V) + a_1(x + V) + \cdots + a_{n-1}(x^{n-1} + V) = a_0 + a_1 x + \cdots a_{n-1}x^{n-1} + V = V$$

for some $a_i \in F$ which are not all zero. Set $a(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$. Note that $a(x) \in V$ if and only if $a(x) = d(x)g(x)$ for some polynomial $d(x) \in F[x]$. But we know that $deg(a(x)) = n - 1 < n \leq deg(d(x)) + deg(g(x)) = deg(d(x)g(x))$ so that it is impossible that $a(x) \in V$, unless $a_i = 0$ for all i. Hence, β is a basis for $F[x]/V$, and the dimension of $F[x]/V$ is n. □

3. a) If V is a finite dimensional vector space over the field K, and if F is a subfield of K such that $[K : F]$ is finite, show that V is a finite-dimensional vector space over F and that moreover $\dim_F(V) = (\dim_K(V))([K : F])$.

Proof. Let $\beta_1 = \{v_1, v_2, \cdots v_n\}$ be a basis of V over field K, and $\beta_2 = \{w_1, w_2, \cdots w_m\}$ be a basis of K over field F. We claim that

$$\beta = \{v_1 w_1, v_1, w_2, \cdots, v_1 w_m, v_2 w_1, \cdots, v_2 w_m, \cdots, v_n w_1, \cdots, v_n w_m\}$$

is a basis of V over field F. Let $v \in V$. Then viewing V as a vector space over K, $v = k_1 v_1 + k_2 v_2 + \cdots k_n v_n$ for some $k_i \in K$. Now for each k_i, viewing K as a vector space over F, $k_i = f_{i1} w_1 + f_{i2} w_2 + \cdots + f_{im} w_m$, where $f_{ij} \in F$, $i = 1, \cdots, n$, $j = 1, 2, \cdots, m$. Plugging in the k_i's in v, we have

$$\begin{aligned} v &= (f_{11} w_1 + f_{12} w_2 + \cdots f_{1m} w_m) v_1 + (f_{21} w_1 + f_{12} w_2 + \cdots f_{2m} w_m) v_2 + \cdots \\ &\quad + (f_{n1} w_1 + f_{n2} w_2 + \cdots f_{nm} w_m) v_n \\ &= \sum_{i,j} f_{ij}(v_i w_j). \end{aligned}$$

Hence we conclude that β spans V over field F. Moreover, suppose $\sum_{i,j} f_{ij}(v_i w_j) = 0$ for some $f_{ij} \in F$. This is equivalent to

$$\sum_{i,j} f_{ij}(v_i w_j) = 0 \iff \sum_j \left(\sum_i f_{ij} v_i \right) w_j = 0.$$

Since β_2 is a basis, the above forces us that $\sum_i (f_{ij} v_i) = 0$ for each j. But since β_1 is also a basis, it follows that $f_{ij} = 0$ for each i and j. Hence, β is linear independent, and forms a basis for V over F. Moreover, the relation of $\dim_F(V) = (\dim_K(V))([K : F])$ holds clearly. □

b) Show that Theorem 5.1.1 is a special case of the result of part a).

Proof. Just viewing the relationship of fields and subfields as vector spaces over some fields, the result is straightforward. □

4. a) Let R be the field of real numbers and Q be the field of rational numbers. In R, $\sqrt{2}$ and $\sqrt{3}$ are both algebraic over Q. Exhibit a polynomial of degree 4 over Q satisfied by $\sqrt{2} + \sqrt{3}$.

Solution. The polynomial $f(x) = x^4 - 10x^2 + 1$ satisfies $\sqrt{2} + \sqrt{3}$. □

b) What is the degree of $\sqrt{2} + \sqrt{3}$ over Q? Prove your answer.

Proof. We show $Q(\sqrt{2} + \sqrt{3}) = Q(\sqrt{2}, \sqrt{3})$. That $Q(\sqrt{2} + \sqrt{3}) \subset Q(\sqrt{2}, \sqrt{3})$ is clear. So we now show the opposite inclusion. It is enough to show that $\sqrt{2}, \sqrt{3}$ are in $Q(\sqrt{2} + \sqrt{3})$. Note that

$$(\sqrt{2} + \sqrt{3})^3 = 11\sqrt{2} + 9\sqrt{3},$$

so that $11\sqrt{2} + 9\sqrt{3} - 9(\sqrt{2} + \sqrt{3}) = 2\sqrt{2}$ and hence, $\sqrt{2} \in Q(\sqrt{2} + \sqrt{3})$. Similarly for $\sqrt{3}$, $\sqrt{3} \in Q(\sqrt{2} + \sqrt{3})$. Therefore, $Q(\sqrt{2} + \sqrt{3}) = Q(\sqrt{2}, \sqrt{3})$. Note that $\sqrt{3} \notin Q(\sqrt{2})$, so that $x^2 - 3$ is still the minimal polynomial in $Q(\sqrt{2})$ satisfying $\sqrt{3}$. Thus, $[Q(\sqrt{2}, \sqrt{3}), Q(\sqrt{2})] = 2$. Ultimately from

$$[Q(\sqrt{2}, \sqrt{3}), Q] = [Q(\sqrt{2}, \sqrt{3}), Q(\sqrt{2})][Q(\sqrt{2}), Q] = 2 \cdot 2 = 4,$$

we conclude that $[Q(\sqrt{2} + \sqrt{3}), Q] = 4$. □

c) What is the degree of $\sqrt{2}\sqrt{3}$ over Q?

Proof. Note that $\sqrt{2}\sqrt{3} = \sqrt{6}$ and $f(x) = x^2 - 6$ is the minimal polynomial over Q satisfying $\sqrt{6}$. Hence, $[Q(\sqrt{2}\sqrt{3}, Q] = 2$. □

5. With the same notation as in Problem 4, show that $\sqrt{2}+\sqrt[3]{5}$ is algebraic over Q of degree 6.

Proof. We know that $Q(\sqrt{2})$ and $Q(\sqrt[3]{5})$ are subfields of $Q(\sqrt{2}+\sqrt[3]{5})$, where each of their degree over Q are 2 and 3 respectively. Therefore, $6 \mid [Q(\sqrt{2}+\sqrt[3]{5}), Q]$. moreover,

$$f(x) = x^6 - 6x^5 - 10x^3 + 12x^2 - 60x + 17$$

satisfies $\sqrt{2}+\sqrt[3]{5}$. Thus, $[Q(\sqrt{2}+\sqrt[3]{5}), Q] \leq 6$. Therefore, $[Q(\sqrt{2}+\sqrt[3]{5}), Q] = 6$. □

6. a) Find an element $u \in R$ such that $Q(\sqrt{2}, \sqrt[3]{5}) = Q(u)$.

Solution. We claim that $Q(\sqrt{2}, \sqrt[3]{5}) = Q(\sqrt{2}+\sqrt[3]{5})$. $Q(\sqrt{2}+\sqrt[3]{5}) \subset Q(\sqrt{2}, \sqrt[3]{5})$ is clear. We show the opposite inclusion. It is enough to show that $\sqrt{2}, \sqrt[3]{5} \in Q(\sqrt{2}+\sqrt[3]{5})$. Let $x = \sqrt{2}+\sqrt[3]{5}$ and $y = \sqrt{2}$. Then

$$\begin{aligned}(x-y)^3 = 5 &\iff x^3 - 3x^2y + 3xy^2 - y^3 = x^3 - 3x^2y + 6x - 2y = 5 \\ &\iff y = \frac{x^3+6x-5}{3x^2+2}\end{aligned}$$

so that $y = \sqrt{2} \in Q(x) = Q(\sqrt{2}+\sqrt[3]{5})$. Using this fact, we have

$$\sqrt[3]{5} = \frac{3\sqrt{2}(x^2-2) - (x^3 - (5+2\sqrt{2})}{6}$$

so that $\sqrt[3]{5} \in Q(\sqrt{2}+\sqrt[3]{5})$. Therefore, $Q(\sqrt{2}, \sqrt[3]{5}) = Q(\sqrt{2}+\sqrt[3]{5})$. □

b) In $Q(\sqrt{2}, \sqrt[3]{5})$ characterize all the elements w such that $Q(w) \neq Q(\sqrt{2}, \sqrt[3]{5})$.

Solution. Consider $Q(w)$ for some w. Then $Q(w) = Q(\sqrt{2}, \sqrt[3]{5})$ if and only if $1, w, w^2, w^3, w^4, w^5$ spans $Q(\sqrt{2}, \sqrt[3]{5})$. □

7. a) Prove that $F(a,b) = F(b,a)$.

Proof. It is clear that $F(b) \subset (F(a), b)$. As $(F(b), a)$ being the smallest field containing $F(b)$ and a and $(F(a), b)$ being a field containing $F(b)$ and a, it follows that $(F(b), a) \subset (F(a), b)$. The opposite inclusion follows similarly. Therefore, $(F(b), a) = (F(a), b)$. Consequently, by the definition,

$$F(a,b) = (F(a), b) = (F(b), a) = F(b,a).$$

□

b) If $(i_1, i_2, \cdots, i_n)$ is any permutations of $(1, 2, \cdots, n)$, prove that

$$F(a_1, \cdots, a_n) = F(a_{i_1}, a_{i_2}, \cdots, a_{i_n}).$$

Proof. We prove induction on the size of n, the length of permutation of $(1, 2, \cdots, n)$. Case when $n = 2$ is the exactly the Problem 7 a). So we assume that $F(a_1, \cdots, a_n) = F(a_{i_1}, a_{i_2}, \cdots, a_{i_n})$ holds for some n. Suppose we are considering the permutation $(i_1, i_2, \cdots, i_n, i_{n+1})$. By the induction hypothesis,

$$\begin{aligned} F(a_{i_1}, a_{i_2}, \cdots, a_{i_n}, a_{i_{n+1}}) &= (F(a_{i_1}, a_{i_2}, \cdots, a_{i_n}), a_{i_{n+1}}) \\ &= (F(a_{i_{j_1}}, a_{i_{j_2}}, \cdots, a_{i_{j_n}}), a_{i_{n+1}}) \end{aligned}$$

for some $j_i \in \{1, 2, \cdots, n+1\}$, $i_{j_1} \leq i_{j_2} \leq \cdots \leq i_{j_n}$. Then i_{j_n} is either $n+1$ or n. If $i_{j_n} = n$, we are done as it was mandatory that $a_{i_{n+1}} = a_{n+1}$. If $i_{j_n} = n+1$, by setting $G = F(a_{i_{j_1}}, a_{i_{j_2}}, \cdots a_{i_{j_{n-1}}})$,

$$\begin{aligned} (F(a_{i_{j_1}}, a_{i_{j_2}}, \cdots, a_{i_{j_n}}), a_{i_{n+1}}) &= (G(a_{i_{j_n}}), a_{i_{n+1}}) \\ &= G(a_{i_{j_n}}, a_{i_{n+1}}) = G(a_{i_{n+1}}, a_{i_{j_n}}) \\ &= ((F(a_{i_{j_1}}, a_{i_{j_2}}, \cdots a_{i_{j_{n-1}}}), a_{i_{n+1}}), a_{i_{j_n}}) \\ &= (F(a_{i_{j_1}}, a_{i_{j_2}}, \cdots a_{i_{j_{n-1}}}, a_{i_{n+1}}), a_{i_{j_n}}) \\ &= (F(a_1, \cdots, a_n), a_{n+1}) = F(a_1, \cdots, a_n, a_{n+1}). \end{aligned}$$

Hence by induction, we conclude that $F(a_1, \cdots, a_n) = F(a_{i_1}, a_{i_2}, \cdots, a_{i_n})$ for all permutation $(i_1, i_2, \cdots, i_n)$ of $(1, 2, \cdots, n)$. □

8. If $a, b \in K$ are algebraic over F of degrees m and n, respectively, and if m and n are relatively prime, prove that $F(a, b)$ is of degree mn over F.

Proof. From the fact that $F(a), F(b) \subset F(a, b)$, $\text{lcm}(m, n) = mn \mid F(a.b)$. But we know that $F(a, b) \leq mn$. Therefore, $[F(a, b), F] = mn$. □

9. Suppose that F is a field having a finite number of elements, q.
a) Prove that there is a prime number p such that $a + a + \cdots + a = 0$ for all $a \in F$.

Proof. As F an additive group with order q, $q \cdot 1 = 0$. Thus, F is of finite characteristic, with p, prime as its characteristic. Hence, $pa = 0$ for all $a \in F$. □

b) Prove that $q = p^n$ for some integer n.

Proof. Let $\phi : \mathbb{Z} \to F$ defined by $\phi(x) = x$. Then its kernel must consist of $p\mathbb{Z}$, and since $p\mathbb{Z}$ being the maximal ideal in $\mathbb{Z}$, the kernel is exactly $p\mathbb{Z}$ and hence $Z_p \simeq \phi(F)$. That is, F contains F_0, an isomorphic image of Z_p as its subfield. Now we can consider F as a vector space over F_0. Suppose $\dim_{F_0} F = [F : F_0] = n$. Then there are p^n possible elements in F. Hence, $q = p^n$ for some n. □

c) If $a \in F$, prove that $a^q = a$.

Proof. Considering F as a multiplicative group of order $q-1 = p^n - 1$, it is clear that $a^q = a$. □

d) If $b \in K$ is algebraic over F, prove $b^{q^m} = b$ for some $m > 0$.

Proof. Let $[F(b) : F] = m$ for some $m > 0$. Then $F(b)$ is an extension field of order q^m. Applying the assertion made in Problem 9 c), $b^{q^m} = b$. □

10. If a is any algebraic number, prove that there is a positive integer n such that na is an algebraic integer.

Proof. Let $f(x) \in \mathbb{Q}[x]$ such that $f(a) = 0$ with degree k. It is possible to reduce $f(x)$ into a polynomial $g(x) \in \mathbb{Z}[x]$ such that $g(a) = 0$. Denote g_i to be the coefficients of x^i of $g(x)$. Suppose $g_k = q > 0$(without loss of generality, q can be taken positive) it follows that

$$\begin{aligned} q^{k-1}g(x) &= \sum_{i=0}^{k}(q^{k-1}g_i)x^i = \sum_{i=0}^{k}(q^{k-i-1}g_i)(qx)^i \\ &\implies \sum_{i=0}^{k}(q^{k-i-1}g_i)(qa)^i = 0. \end{aligned}$$

It is clear that for each i, $q^{k-i-1}g_i \in \mathbb{Z}$. Further, $q^{k-1}g(x)$ is monic. Thus, qa is an algebraic integer. □

11. If the rational number r is also an algebraic integer, prove that r must be an ordinary integer.

Proof. Direct application of Problem 5 Section 3.10 gives that r is an integer. □

12. If a is an algebraic integer and m is an ordinary integer, prove
a) $a + m$ is an algebraic integer.

Proof. Let $f(x) \in \mathbb{Z}[x]$ be the monic polynomial satisfying a. Let $g(x) = f(x-m) \in \mathbb{Z}[x]$. Consequently, g is monic and $g(a+m) = f(a) = 0$, so that $a + m$ is also an algebraic integer. □

b) ma is an algebraic integer.

Proof. Let $f(x) \in \mathbb{Z}[x]$ be the monic polynomial satisfying a, with degree k. Let $g(x) = m^k f(x) \in \mathbb{Z}[x]$. Denoting the coefficients of x^i of $f(x)$ by a_i, it follows that

$$0 = g(a) = m^k \sum_{i=0}^{k} a_i a^i = \sum_{i=0}^{k} m^{k-i} a_i (ma)^i$$

so that ma is an algebraic integer. □

13. If α is an algebraic integer satisfying $\alpha^3 + \alpha + 1 = 0$ and β is an algebraic integer satisfying $\beta^2 + \beta - 3 = 0$, prove that both $\alpha + \beta$ and $\alpha\beta$ are algebraic integers.

Proof. We use the method developed in Problem 14: Let $p = \alpha + \beta$. Then the Sylvester matrix M satisfying

$$Mv = pv, \quad v = (1, \alpha, \alpha^2, \beta, \alpha\beta, \alpha^2\beta)^t$$

has the property that its characteristic polynomial $\phi_M(x)$, which is also monic, satisfies p. That is, $\phi_M(p) = 0$. So we compute M and find its characteristic polynomial. Observe that:

$$pv = (\alpha+\beta)\begin{pmatrix} 1 \\ \alpha \\ \alpha^2 \\ \beta \\ \alpha\beta \\ \alpha^2\beta \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ -1 & -1 & 0 & 0 & 0 & 1 \\ 3 & 0 & 0 & -1 & 1 & 0 \\ 0 & 3 & 0 & 0 & -1 & -1 \\ 0 & 0 & 3 & -1 & -1 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ \alpha \\ \alpha^2 \\ \beta \\ \alpha\beta \\ \alpha^2\beta \end{pmatrix} = Mv.$$

Hence, $\phi_M(x) = \det(M - xI_6) = x^6 + 3x^5 - 4x^4 - 11x^3 + 25x^2 + 52x - 39$. Hence, $\alpha + \beta$ satisfies $\phi_M(x)$ and so that it is an algebraic integer. For $q = \alpha\beta$,

$$qv = (\alpha+\beta)\begin{pmatrix} 1 \\ \alpha \\ \alpha^2 \\ \beta \\ \alpha\beta \\ \alpha^2\beta \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & -1 & -1 & 0 \\ 0 & 3 & 0 & 0 & -1 & 0 \\ 0 & 0 & 3 & 0 & 0 & -1 \\ -3 & -3 & 0 & 1 & 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ \alpha \\ \alpha^2 \\ \beta \\ \alpha\beta \\ \alpha^2\beta \end{pmatrix} = M'v$$

so that $\phi_{M'}(x) = \det(M' - xI_6) = x^6 + 7x^4 - 10x^3 + 9x^2 - 9x - 27$. Hence, $\alpha\beta$ satisfies $\phi_{M'}(x)$ and so that it is an algebraic integer. □

14. a) Prove that the sum of two algebraic integers is an algebraic integer.
b) Prove that the product of two algebraic integers is an algebraic integer.

Proof. We prove a more general statement: Set of algebraic integers forms a ring. Let $\mathbb{Z}[\alpha, \beta] = \{f(\alpha, \beta) : f(x, y) \in \mathbb{Z}[x, y]\}$. It suffices to show that $p \in \mathbb{Z}[\alpha, \beta]$ is an algebraic integer. Given that

$$\alpha^n + a_1\alpha^{n-1} + a_2\alpha^{n-2} + \cdots + a_{n-1}\alpha + a_n = 0$$
$$\beta^m + b_1\beta^{m-1} + b_2\alpha^{m-2} + \cdots + b_{m-1}\beta + b_m = 0$$

where each $a_i, b_j \in \mathbb{Z}$,

$$\alpha^n = -a_1\alpha^{n-1} - a_2\alpha^{n-2} - \cdots - a_{n-1}\alpha - a_n$$
$$\beta^m = -b_1\beta^{m-1} - b_2\alpha^{m-2} - \cdots - b_{m-1}\beta - b_m$$

so that $\mathbb{Z}[\alpha, \beta]$ is set of linear combinations of $\alpha^i\beta^j$, $0 \le i \le n-1$, $0 \le j \le m-1$ over $\mathbb{Z}$. Note that for each $0 \le k \le n-1$, $0 \le l \le m-1$, $p\alpha^k\beta^l \in \mathbb{Z}[\alpha, \beta]$ so that

$$p\alpha^k\beta^l = \sum_{i,j} c_{i,j}^{k,l}\alpha_i\beta_j.$$

Let

$$v = \begin{pmatrix} \alpha^0\beta^0 & \alpha^1\beta^0 & \cdots & \alpha^{n-1}\beta & \alpha^0\beta^1 & \cdots & \alpha^{n-1}\beta & \cdots & \alpha^{n-1}\beta^{m-1} \end{pmatrix}^t,$$

$$M = \begin{pmatrix} c_{0,0}^{0,0} & c_{1,0}^{0,0} & \cdots & c_{n-1,0}^{0,0} & c_{0,1}^{0,0} & \cdots & c_{n-1,1}^{0,0} & \cdots & c_{n-1,m-1}^{0,0} \\ c_{0,0}^{1,0} & c_{1,0}^{1,0} & \cdots & c_{n-1,0}^{1,0} & c_{0,1}^{1,0} & \cdots & c_{n-1,1}^{1,0} & \cdots & c_{n-1,m-1}^{1,0} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ c_{0,0}^{n-1,0} & c_{1,0}^{n-1,0} & \cdots & c_{n-1,0}^{n-1,0} & c_{0,1}^{n-1,0} & \cdots & c_{n-1,1}^{n-1,0} & \cdots & c_{n-1,m-1}^{n-1,0} \\ c_{0,0}^{0,1} & c_{1,0}^{0,1} & \cdots & c_{n-1,0}^{0,1} & c_{0,1}^{0,1} & \cdots & c_{n-1,1}^{0,1} & \cdots & c_{n-1,m-1}^{0,1} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ c_{0,0}^{n-1,1} & c_{1,0}^{n-1,1} & \cdots & c_{n-1,0}^{n-1,1} & c_{0,1}^{n-1,1} & \cdots & c_{n-1,1}^{n-1,1} & \cdots & c_{n-1,m-1}^{n-1,1} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ c_{0,0}^{n-1,m-1} & c_{1,0}^{n-1,m-1} & \cdots & c_{n-1,0}^{n-1,m-1} & c_{0,1}^{n-1,m-1} & \cdots & c_{n-1,1}^{n-1,m-1} & \cdots & c_{n-1,m-1}^{n-1,m-1} \end{pmatrix},$$

so that we have the equivalent system of linear equations

$$pv = Mv$$

as above. Since $v \neq 0$, we can consider p as an eigenvalue of the matrix M. Thus, the characteristic polynomial $\phi_M(x)$ of M satisfies p. Recall that $\phi_M(x)$ is monic polynomial in $\mathbb{Z}$. Hence, p is an algebraic integer. □

15. a) Prove that $\sin 1^\circ$ is an algebraic integer.

Proof. By De moivre's Theorem,

$$[\cos 1^\circ + i \sin 1^\circ]^{90} = 0.$$

Now consider the real part of the above. Then we obtain

$$\sum_{k:even}^{90} \binom{90}{k} (\cos 1^\circ)^{90-k} (\sin 1^\circ)^k = \sum_{k:even}^{90} \binom{90}{k} (1 - \sin^2 1^\circ)^{\frac{90-k}{2}} (\sin 1^\circ)^k = 0.$$

Therefore, $\sin 1^\circ$ is an algebraic number. □

b) From part a) prove that $\sin m^\circ$ is an algebraic number for any integer m.

Proof. Similarly as the part a),

$$[\cos m^\circ + i \sin m^\circ]^{180} = \pm 1.$$

Considering the real part of the above, we obtain

$$\sum_{k:even}^{180} \binom{180}{k} (\cos m^\circ)^{180-k} (\sin m^\circ)^k = \sum_{k:even}^{180} \binom{180}{k} (1 - \sin^2 m^\circ)^{\frac{180-k}{2}} (\sin m^\circ)^k = \pm 1.$$

This implies that $\sin m^\circ$ is also an algebraic number. □