math123, Abstract Algebra II

Final Exam

Your name: *Alberto De Sole*

Problem	**Points**	**Your Grade**
1	10	
2	10	
3	15	
4	15	
5	15	
6	10	
7	15	
8	10	
9	10	
10	10	
11	15	
12	15	
Total	150	

Problem 1 (pt 10)

Given $a, b, c, d \in \mathbb{R}$, consider the map $\mathbb{R}^2 \times \mathbb{R}^2 \longrightarrow \mathbb{R}$ defined by

$$\begin{bmatrix} \alpha_1 \\ \alpha_2 \end{bmatrix} , \begin{bmatrix} \beta_1 \\ \beta_2 \end{bmatrix} \quad \mapsto \quad a\alpha_1\beta_1 + b\alpha_2\beta_2 + c\alpha_1\beta_2 + d\alpha_2\beta_1$$

For which values of $a, b, c, d \in \mathbb{R}$ this map defines a:

(a) bilinear form on $\mathbb{R}^2$?
(b) symmetric bilinear form on $\mathbb{R}^2$?
(c) positive definite (symmetric) bilinear form on $\mathbb{R}^2$?

Solution

The above map can be rewritten as:

$$X \ , \ Y \quad \mapsto \quad X^T A Y \ ,$$

where A is the 2x2 matrix:

$$A \ = \ \begin{bmatrix} a & c \\ d & b \end{bmatrix}$$

(a) It's always a bilinear form.
(b) Its is symmetric if and only of $d = c$.
(c) It is positive definite if and only if $d = c$ and $a > 0, ab - c^2 > 0$.

Problem 2 (pt 10)

Let V be a vector space over $\mathbb{R}$ with a positive definite, symmetric, bilinear form $(,)$. Suppose $\{v_1, \ldots, v_n\} \subset V$ is an orthonormal system, namely a collection of vectors (not necessarily spanning V) such that:

$$(v_i, v_j) \;=\; \delta_{i,j} \ .$$

(a) Prove that

$$\sum_{i=1}^{n} (v_i, v)^2 \;\leq\; (v, v) \ , \quad \forall v \in V \ .$$

(b) Prove that $\sum_{i=1}^{n} (v_i, v)^2 = (v, v), \ \forall v \in V$ if and only if $\{v_1, \ldots, v_n\}$ is a basis of V.

Solution

(a) Consider the vector

$$u \;=\; v - \sum_{i=1}^{n} (v_i, v) v_i \ .$$

Then we have:

$$\begin{aligned} 0 \;\leq\; (u, u) \;&=\; (v - \sum_{i=1}^{n} (v_i, v) v_i, v - \sum_{i=1}^{n} (v_i, v) v_i) \\ &=\; (v, v) - 2 \sum_{i=1}^{n} (v_i, v)^2 + \sum_{i,j=1}^{n} (v_i, v)(v_j, v)(v_i, v_j) \\ &=\; (v, v) - \sum_{i=1}^{n} (v_i, v)^2 \ . \end{aligned}$$

This proves (a).

(b) From the above equation we get:

$$(v, v) = \sum_{i=1}^{n} (v_i, v)^2 \quad \text{ if and only if } \quad v \;=\; \sum_{i=1}^{n} (v_i, v) v_i \ .$$

Hence in this case the vectors $\{v_i, i = 1, \ldots, n\}$ form a basis of V, thus proving (b).

Problem 3 (pt 15)

(a) Describe the Lie algebra $sl_2(\mathbb{C})$ of the Lie group $SL_2(\mathbb{C})$ (No proof is required in this part of the problem).

(b) Consider the adjoint representation of $SL_2(\mathbb{C})$ on its Lie algebra $sl_2(\mathbb{C})$. Find a non–degenerate, symmetric, bilinear form on $sl_2(\mathbb{C})$, which is invariant under the action of $SL_2(\mathbb{C})$.

(c) Deduce that there is a group homomorphism

$$SL_2(\mathbb{C}) \ \rightarrow O_3(\mathbb{C}) \ .$$

Extra Credit (pt 5)

(d) Prove that the kernel of this homomorphism is: $\{\pm\mathbb{1}\} \subset SL_2(\mathbb{C})$.

(e) Argue that the image of this homomorphism has to be in $SO_3(\mathbb{C})$.

(f) Accept (without proving it) that the image is equal to $SO_3(\mathbb{C})$, and deduce that there is a group isomorphism:

$$SL_2(\mathbb{C})/\{\pm\mathbb{1}\} \ \xrightarrow{\sim} SO_3(\mathbb{C}) \ .$$

Solution

(a) By definition $sl_2(\mathbb{C})$ is the collection of matrices A such that $\det(e^t A) = e^{t\mathrm{Tr}(A)} = 1, \ \forall t \in \mathbb{R}$. Hence:

$$sl_2(\mathbb{C}) \ = \ \{A \in \mathrm{Mat}_{2\times 2}(\mathbb{C}) \mid \mathrm{Tr}(A) = 0\} \ .$$

(b) It is given by the Killing form:

$$(A, B) \ = \ \mathrm{Tr}(AB) \ .$$

It is clearly non degenerate, and it is invariant since:

$$(PAP^{-1}, PBP^{-1}) \ = \ \mathrm{Tr}(PAP^{-1}PBP^{-1}) \ = \ \mathrm{Tr}(AB) \ = \ (A, B) \ .$$

(c) $sl_2(\mathbb{C})$ is a three–dimensional vector space over $\mathbb{C}$. Hence the adjoint representation of $SL_2(\mathbb{C})$ on $sl_2(\mathbb{C})$ gives a group homomorphism $SL_2(\mathbb{C}) \longrightarrow GL_3(\mathbb{C})$. Since there is a symmetric invariant bilinear form on $sl_2(\mathbb{C})$, it means that the image of this group homomorphism is isomorphic to a subgroup of $O_3(\mathbb{C})$.

(d) Suppose $P \in \mathrm{Ker}(T)$. We then have:

$$(\mathrm{ad}(P))(A) \ = \ PAP^{-1} \ = \ A \ , \ \ \forall A \in sl_2(\mathbb{C}) \ .$$

In particular:

$$PAP^{-1} \ = \ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \ = \ \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \ = \ A$$

from which we get $b = c = 0, \ d = a^{-1}$. Moreover we have:

$$PAP^{-1} \ = \ \begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a^{-1} & 0 \\ 0 & a \end{bmatrix} \ = \ \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \ = \ A \ ,$$

from which we get $a = \pm 1$. Hence $\mathrm{Ker}(\mathrm{ad}) = \{\pm\mathbb{1}\}$.

(e) Since $SL_2(\mathbb{C})$ is a connected Lie group, since $\mathrm{ad}(\mathbb{1}_2) = \mathbb{1}_3$, and since the function $\det(\mathrm{ad}(P))$ on $SL_2(\mathbb{C})$ is continuous with values ± 1, we conclude that it must be: $\det(\mathrm{ad}(P)) = 1, \ \forall P \in SL_2(\mathbb{C})$. Namely

$$\mathrm{ad} \ : \ \ SL_2(\mathbb{C}) \ \longrightarrow \ SO_3(\mathbb{C}) \ .$$

(f) Since $\mathrm{Ker}(\mathrm{ad}) = \{\pm \mathbb{1}\}$ and $\mathrm{Im}(\mathrm{ad}) = SO_3(\mathbb{C})$, we conclude that

$$SL_2(\mathbb{C})/\{\pm \mathbb{1}\} \xrightarrow{\sim} SO_3(\mathbb{C}) \ .$$

Problem 4 (pt 15)

(a) Determine the character table of the symmetric group $G = S_3$.
Extra Credit (pt 5)
(b) The group G acts on itself by conjugation. Determine the character χ of the associated representation ρ. (**Note**: it is not the regular representation).
(c) Write χ as a sum of irreducible characters.
(d) Write the representation ρ as a direct sum of the irreducible representations of G.

Solution

(a) There are three conjugacy classes in S_3:

$$C_1 = \{e\} \ , \ C_x = \{(1,2,3),(2,1,3)\} \ , \ C_a = \{(1,2),(1,3),(2,3)\} \ .$$

Hence there are three non isomorphic irredicuble representations: $\rho_1 = \mathbb{C}$, ρ_2, ρ_3. By the dimension formula their dimensions satisfy:

$$d_1 = 1 \ , \quad 1 + d_2^2 + d_3^2 = 6 \ .$$

So the only possibility is $d_2 = 1$, $d_3 = 2$. The character table will look like:

	(1)	(2)	(3)
	e	x	a
χ_1	1	1	1
χ_2	1	α	β
χ_3	2	γ	δ

Since ρ_2 is one–dimensional, and since x has order 3, we conclude that $\alpha = 1, e^{2\pi i/3}, e^{4\pi i/3}$. Similarly, since a has order 2, we conclude that $\beta = \pm 1$. By orthogonality condition we have:

$$0 \ = < \chi_1, \chi_2 > = \ 1 + 2\alpha + 3\beta \ ,$$

which is possible only if $\alpha = 1$ and $\beta = -1$. We can now impose orthogonality conditions to find:

$$\begin{aligned} 0 \ &= \ < \chi_1, \chi_3 > = \ 2 + 2\gamma + 3\delta \ , \\ 0 \ &= \ < \chi_2, \chi_3 > = \ 2 + 2\gamma - 3\delta \ , \end{aligned}$$

which implies $\gamma = -1, \delta = 0$. In conclusion the character table is:

	(1)	(2)	(3)
	e	x	a
χ_1	1	1	1
χ_2	1	1	-1
χ_3	2	-1	0

(b) Let ρ be the representation of $G = S_3$ on the space $\mathbb{C}[G] = \oplus_{g \in G} \mathbb{C}g$, defined by conjugation, and let χ be the corresponding character. By definition:

$$\begin{aligned} \chi(e) &= \dim \rho \ = \ 6 \ , \\ \chi(x) &= \mathrm{Tr}\rho(x) \ = \ \#\{g \in S_3 \mid xgx^{-1} = g\} \\ &= \#\{e, (1,2,3), (2,1,3)\} \ = \ 3 \ , \\ \chi(a) &= \mathrm{Tr}\rho(a) \ = \ \#\{g \in S_3 \mid aga^{-1} = g\} \\ &= \#\{e, (1,2)\} \ = \ 2 \ . \end{aligned}$$

(c) The coefficients of the linear combination $\chi = \sum k_i \chi_i$ can be easily found by taking inner products: $k_i = < \chi, \chi_i >$. In conclusion one gets:

$$\chi \ = \ 3\chi_1 + \chi_2 + \chi_3 \ .$$

(d) By the above result, we immediately get:

$$\rho \ = \ \rho_1^{\oplus 3} \oplus \rho_2 \oplus \rho_3 \ .$$

Problem 5 (pt 15)

1. Let G be a group with a finite–dimensional representation ρ on a vector space V.
   (a) Define a ring structure on the space $E(V)$ of all G–invariant linear transformations $T:\ V \to V$.
   (b) What can you say about $E(V)$ if V is an irreducible representation?
2. Let R be a ring and let M be a module over R.
   (a) Define a ring structure on the space $E(M)$ of all module homomorphisms $T:\ M \to M$.
   (b) Prove that, if M is irreducible, then every non–zero element $T \in E(M)$ is invertible.

Solution

1. (a) The ring structure on $E(V)$ is defined as follows:
   $$(T_1 + T_2)(v) \ = \ T_1(v) + T_2(v)\ , \quad (T_1 T_2)(v) \ = \ T_1(T_2(v))\ .$$
   (b) By Schur's lemma, if V is irreducible, then:
   $$E(V) \ = \ \{\lambda \mathbb{1}\ ,\ \lambda \in \mathbb{C}\} \ \simeq \ \mathbb{C}\ .$$
2. (a) The ring structure on $E(M)$ is defined the same way as before:
   $$(T_1 + T_2)(v) \ = \ T_1(v) + T_2(v)\ , \quad (T_1 T_2)(v) \ = \ T_1(T_2(v))\ .$$
   (b) Both $\mathrm{Ker}(T)$ and $\mathrm{Im}(T)$ are submodules of M. Hence, if M is irreducible, they must be equal to either 0 or to M itself. Moreover, if T is non–zero, we have $\mathrm{Ker}(T) \neq M$ and $\mathrm{Im}(T) \neq 0$. In conclusion, we get $\mathrm{Ker}(T) = 0$ and $\mathrm{Im}(T) = M$, which means that T is a bijection, hence it is invertible.

Problem 6 (pt 10)

Give a classification of all abelian groups G of order 1000, with the condition that $50g = 0,\ \forall g \in G$ (I am using additive notation for G).

Solution

By Classification of abelian groups, we have:

$$G \ = \ \mathbb{Z}/(d_1) \oplus \mathbb{Z}/(d_2) \oplus \cdots \oplus \mathbb{Z}/(d_r) \oplus \mathbb{Z}^k \ ,$$

where $k \geq 0$ and $2 \leq d_1 | d_2 | \cdots | d_r$. Since, by assumption, G is finite of order 1000, we immediately get

$$k \ = \ 0 \quad \text{and} \quad 1000 \ = \ 2^3 \times 5^3 \ = \ d_1 d_2 \ldots d_r \ .$$

Moreover, by the condition that $50g = 0 \forall g \in G$, we also get

$$d_i \mid 50 \ = \ 2^2 \times 5 \ , \quad \forall i = 1, \ldots, r \ .$$

It is then easy to check that the only possibilities for the d_i's are: $d_1 = d_2 = d_3 = 10$, or $d_1 = 2, d_2 = 10, d_3 = 50$. In conclusion, the classification is as follows:

$$\begin{aligned} G &= \mathbb{Z}/(10)^{\oplus 3} \ , \\ G &= \mathbb{Z}/(2) \oplus \mathbb{Z}/(10) \oplus \mathbb{Z}/(50) \ . \end{aligned}$$

Problem 7 (pt 15)

Let V be a module over the ring $R = \mathbb{Q}[t]$, with generators $v_1,\ v_2$ and relations:

$$\begin{aligned} v_1 + tv_2 &= 0\ , \\ t^2(1-t^3)v_1 + (1-t^3)v_2 &= 0\ . \end{aligned}$$

(a) Find $v_0 \in V$ such that V is generated by v_0 (Express it in terms of v_1 and v_2.

(b) Find a generator of the ideal $I \subset \mathbb{Q}[t]$ consisting of elements $g \in \mathbb{Q}[t]$ such that $gv_0 = 0$.

(c) What is the dimension of V as vector space over $\mathbb{Q}$?

(d) Choose a basis for V over $\mathbb{Q}$ and write the matrix for the linear transformation $T(v) = tv$.

Solution

(a) We can use the diagonalization algorithm to get:

$$A \ = \ \begin{bmatrix} 1 & t^2(1-t^3) \\ t & (1-t^3) \end{bmatrix} \ \to \ \begin{bmatrix} 1 & 0 \\ t & (1-t^3)^2 \end{bmatrix} \ \to \ \begin{bmatrix} 1 & 0 \\ 0 & (1-t^3)^2 \end{bmatrix}\ ,$$

which gives the following identity:

$$A \ = \ \begin{bmatrix} 1 & 0 \\ t & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & (1-t^3)^2 \end{bmatrix} \begin{bmatrix} 1 & t^2(1-t^3) \\ 0 & 1 \end{bmatrix} \ = \ PDQ\ .$$

The module V is generated by $\mathcal{B} = [v_1, v_2]$, with relations $\mathcal{B}A = 0$. Hence, using the above identity, V is also generated by $\mathcal{B}' = \mathcal{B}P = [v_1 + tv_2, v_2]$, with relations $\mathcal{B}'D = 0$. Or, equivalently, V is generated by $v_0 = v_2$, with relation:

$$(1-t^3)^2 v_0 \ = \ 0\ .$$

(b) By the above result, the ideal I is generated by $g = (1-t^3)^2$.

(c) $V \simeq \mathbb{Q}[t]/(1-t^3)^2$ is a 6–dimensional vector space over $\mathbb{Q}$.

(d) If we choose the basis $v_0, tv_0, \ldots, t^5 v_0$, we have the relation

$$t(t^5 v_0) \ = \ -v_0 + 2t^3 v_0\ ,$$

so the matrix of T becomes:

$$T \ = \ \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 2 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}\ .$$

Problem 8 (pt 10)

Can $\sqrt[8]{7}$ be constructed by ruler and compass? (Explain your answer)

Solution

Yes, since $\mathbb{Q} \subset \mathbb{Q}[\sqrt{7}] \subset \mathbb{Q}[\sqrt[4]{7}] \subset \mathbb{Q}[\sqrt[8]{7}]$, is a sequence of field extensions of degree 2.

Problem 9 (pt 10)

Let $P(x) \in \mathbb{Q}[x]$ be a polynomial with a root $\alpha = a + \sqrt{m}b$, where $m \in \mathbb{Z}$ is square–free and $a, b \in \mathbb{Q}$. Prove or disprove: $\beta = a - \sqrt{m}b$ is a root of $P(x)$.

Solution

Consider the field extension $\mathbb{Q} \subset K = \mathbb{Q}[\sqrt{m}]$. There is a field automorphism of K which fixes $\mathbb{Q}$, defined in the following way:

$$\begin{array}{rccc} \sigma \ : & \mathbb{Q}[\sqrt{m}] & \longrightarrow & \mathbb{Q}[\sqrt{m}] \\ & s + t\sqrt{m} & \mapsto & s - t\sqrt{m} \end{array}$$

Since $P(x) \in \mathbb{Q}[x]$, and since α is a root of $P(x)$, we then get:

$$0 \ = \ \sigma(P(\alpha)) \ = \ P(\sigma(\alpha)) \ = \ P(\beta) \ ,$$

which proves that β is also a root of $P(x)$.

Problem 10 (pt 10)

Determine the number of monic irreducible polynomials of degree 3 over $\mathbb{F}_5$.

Solution

By the theory of field extensions of finite fields, we know that:

$$x^{5^3} - x \;=\; \prod_{\left(\begin{array}{c} f(x)\in\mathbb{F}_5[x] \\ \text{monic irred} \\ \text{of deg } d|3 \end{array}\right)} f(x) \;=\; \prod_{i\in\mathbb{F}_5}(x-i) \prod_{\left(\begin{array}{c} P(x)\in\mathbb{F}_5[x] \\ \text{monic irred} \\ \text{of } d=3 \end{array}\right)} P(x)$$

The left hand side is a monic polynomial of degree 125, while the right hand side is a monic polymonial of degree $5 + 3\#\{\text{monic irred polyn's of degree } 3\}$. We thus conclude that

$$\#\{\text{monic irred polyn's of degree } 3\} \;=\; \frac{125-5}{3} \;=\; 40\ .$$

Problem 11 (pt 15)

Let $\mathbb{Q} \subset K$ be a splitting field extension for the polynomial $x^n - 1$.

(a) Find an isomorphism between the Galois group $G(K/\mathbb{Q})$ and the cyclic group of order $\Phi(n)$ (Where $\Phi(n)$ denotes the Euler's function, namely the number of integers $k = 1, \ldots, n$ which are relatively prime to n).

(b) Prove that $[K : \mathbb{Q}] = \Phi(n)$.

(c) Prove that the polynomial $x^n - 1$ admits the following irreducible factor of degree $\Phi(n)$:

$$P(x) = \prod_{\gcd(k,n)=1} (x - e^{2k\pi i/n}) \ \in \ \mathbb{Q}[x] \ .$$

Solution

(a) The roots of $x^n - 1$ are $\zeta_n = e^{2\pi i/n}, \zeta_n^2, \ldots, \zeta_n^{n-1}$, so the splitting field is $K = \mathbb{Q}[\zeta_n]$. The isomorphism is given by:

$$\begin{array}{ccc} G(K/\mathbb{Q}) & \longrightarrow & \left\{ \begin{array}{c} \text{multiplicative group of all} \\ k =\leq n-1 \text{ such that } gcd(k,n) = 1 \end{array} \right\} \\ (\sigma : \ \zeta_n \mapsto \zeta_n^s) & \mapsto & s \end{array}$$

(b) It follows from Galois theory that $[K : \mathbb{Q}] = |G(K/\mathbb{Q})| = \Phi(n)$.

(c) In a Galois extension, the irreducible polynomial $P(x) \in \mathbb{Q}[x]$ of ζ_n is:

$$P(x) \ = \ \prod_{\sigma \in G(K\mathbb{Q})} (x - \sigma(\zeta_n)) \ = \ \prod_{\gcd(k,n)=1} (x - \zeta_n^k) \ .$$

Problem 12 (pt 15)

Consider the polynomial $P(x) = x^5 - 2 \in \mathbb{Q}[x]$.

(a) What are the five complex roots of $P(x)$?
(b) Let K be the splitting field for $P(x)$ over $\mathbb{Q}$. Determine the degree of K over $\mathbb{Q}$.
(c) Suppose $g(x) \in \mathbb{Q}[x]$ is a polynomial irreducible of degree 4, with all its roots in K. What is the degree of the splitting field for $g(x)$ over $\mathbb{Q}$?

Solution

(a) The roots of $P(x)$ are $\sqrt[5]{2},\ \sqrt[5]{2}\zeta_5,\ \sqrt[5]{2}\zeta_5^2,\ \sqrt[5]{2}\zeta_5^3,\ \sqrt[5]{2}\zeta_5^4$, where $\zeta_5 = e^{2\pi i/5}$.

(b) The splitting field K is obtained as follows

$$\mathbb{Q} \ \subset\ \mathbb{Q}[\sqrt[5]{2}] \ \subset\ \mathbb{Q}[\sqrt[5]{2}, \zeta_5] = K\ .$$

The first extension is of degree 5, and the second extension is of degree 4. Hence, by tower law, K has degree 20 over $\mathbb{Q}$.

(c) Let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ be the roots of $g(x)$, and let L be the splitting field of $g(x)$. The field L is obtained as follows:

$$\mathbb{Q} \ \subset\ \mathbb{Q}[\alpha_1] \ \subset\ \cdots \ \subset\ \mathbb{Q}[\alpha_1, \alpha_2, \alpha_3, \alpha_4] \ =\ L\ .$$

Hence, by tower law,

$$[L : \mathbb{Q}] \ =\ [\mathbb{Q}[\alpha_1] : \mathbb{Q}][\mathbb{Q}[\alpha_1, \alpha_2] : \mathbb{Q}[\alpha_1]] \cdots [L : \mathbb{Q}[\alpha_1, \alpha_2, \alpha_3]]\ .$$

Since $g(x)$ is irreducible of degree 4, we have $[\mathbb{Q}[\alpha_1] : \mathbb{Q}] = 4$ and $[\mathbb{Q}[\alpha_1, \alpha_2] : \mathbb{Q}[\alpha_1]], \ldots, [L : \mathbb{Q}[\alpha_1, \alpha_2, \alpha_3]] \leq 3$. Moreover, we have $\mathbb{Q} \ \subset\ L \ \subset\ K$, hence by tower law

$$[L : \mathbb{Q}] \mid [K : \mathbb{Q}] = 20 = 4 \times 5\ .$$

It then follows that $[L : \mathbb{Q}] = 4$.