

Part A.

1. (a) Since this operation is weird, then we need to check everything about this group (to be).
 (i) Closure of $*$ in $S(G, H)$: We take $f, g \in S(G, H)$, we want to show that $f * g$ is an element of $S(G, H)$.

First of all, note that since $f, g \in S(G, H)$ and $x \in G$ then both $f(x)$ and $g(x)$ are in H . Moreover $*$ being closed in H forces $f(x) * g(x) \in H$. Hence, $(f * g)(x) \in H$ for all $x \in G$. So, $f * g$ takes elements in G to elements in H , but is it a function? We need to check that images are unique! But this is immediate, as both f and g are functions, and thus $f(x)$ and $g(x)$ are uniquely defined... and also is their product. It follows that $S(G, H)$ is closed under $*$.

- (ii) Associativity: Let $f, g, h \in S(G, H)$, then for any $x \in G$ we get

$$[f * (g * h)](x) = f(x) * (g * h)(x) = f(x) * [g(x) * h(x)]$$

but now using that $*$ is associative in H we get

$$f(x) * [g(x) * h(x)] = [f(x) * g(x)] * h(x)$$

which is $[(f * g) * h](x)$. Done.

- (iii) Identity? Let $f \in S(G, H)$ and let e be the constant function $e(x) = e_H$, where e_H is the identity of H . Note that

$$(f * e)(x) = f(x) * e(x) = f(x) * e_H = f(x)$$

for all $x \in G$, and thus $f * e = f$. Similarly, $e * f = f$. Hence, e is the identity of $S(G, H)$.

- (iv) Inverses? Let $f \in S(G, H)$. We want to find $g \in S(G, H)$ such that $f * g = e$. Consider $g(x) = f(x)^{-1}$, where the inverse is taken in H . Then,

$$(f * g)(x) = f(x) * g(x) = f(x) * f(x)^{-1} = e_H$$

and thus $f * g = e$. Done.

This group is Abelian if H is Abelian, as

$$(f * g)(x) = f(x) * g(x) = g(x) * f(x) = (g * f)(x)$$

for all $x \in G$.

If H is non-Abelian, then there are elements $a, b \in H$ such that $a * b \neq b * a$. Then, we define the constant functions $f(x) = a$ and $g(x) = b$, which are clearly in $S(G, H)$ and do not commute. Hence, $S(G, H)$ is Abelian if and only if H is Abelian.

2. (a) No. The largest possible order of an element in $\mathbb{Z}_6 \oplus \mathbb{Z}_6$ is 6. But \mathbb{Z}_{12} has an element of order 12 (any generator would do). Since the order of $\psi(x)$ divides the order of x , for all $x \in \mathbb{Z}_6 \oplus \mathbb{Z}_6$ then the largest order of an image under ψ is 6. Hence, the elements of order 12 in \mathbb{Z}_{12} are not in the range of ψ .
 (b) No. The homomorphic image of a cyclic group is cyclic. Having an onto homomorphism from $\mathbb{Z}_{81} \rightarrow \mathbb{Z}_3 \oplus \mathbb{Z}_3$ would imply $\mathbb{Z}_3 \oplus \mathbb{Z}_3$ is cyclic. A contradiction.
3. (a) Let R be a commutative ring with unity 1, and let a be a unit in R . Suppose that $b|c$ in R ; that is, $c = br$ for some $r \in R$. Then $c = (a^{-1}a)(br) = (ab)(a^{-1}r)$ (we used here that R is commutative, that a^{-1} exists in R and that multiplication is associative in a ring). But R is closed under multiplication, thus $a^{-1}r \in R$, and then $(ab)|c$, as desired. Conversely, suppose that $(ab)|c$ in R ; that is $c = (ab)s$ for some $s \in R$. Since R is commutative, it implies that $c = b(as)$, thus $b|c$ (since $as \in R$).

(b) First note that $0 \in S$ (since $a0 = 0$), thus $S \neq \emptyset$.

Let $x, y \in S$. Then $ax = 0 = ay$, and we have:

$$a(x - y) = ax - ay = 0 - 0 = 0 \quad \text{and} \quad a(xy) = (ax)y = 0y = 0$$

thus $x - y \in S$ and $xy \in S$. Then, by the subring test, S is a subring of R .

4. (a) For i positive we get that $\phi(g^i) = \phi(g^{i-1}g) = \phi(g^{i-1})\phi(g)$. So, if we knew that $\phi(g^{i-1}) = \phi(g)^{i-1}$ then we would be done, as

$$\phi(g^i) = \phi(g^{i-1})\phi(g) = \phi(g)^{i-1}\phi(g) = \phi(g)^i$$

Note that we have just set an induction argument. That is, proving the i -case by assuming the $(i - 1)$ -case. Since the case $i = 2$ holds trivially, then the induction is done.

For i negative, let us first look at $\phi(g^{-1}) = \phi(g)^{-1}$. Then putting this case together with the positive i case above will solve the case for all negative i 's.

Recall that $\phi(e) = e$. Then, $e = \phi(e) = \phi(gg^{-1}) = \phi(g)\phi(g^{-1})$, which means that $\phi(g^{-1})$ is the inverse of $\phi(g)$. Done.

Now let us consider $-i$ for i positive. We need to show that $\phi(g^{-i}) = \phi(g)^{-i}$:

$$\phi(g^{-i}) = \phi((g^i)^{-1}) = \phi(g^i)^{-1} = (\phi(g)^i)^{-1} = \phi(g)^{-i}$$

The case $i = 0$ is trivial.

(b) Assume that $G = \langle g \rangle$. We know, from part (a) that $\phi(g^i) = \phi(g)^i$. Since every element in the domain of ϕ looks like g^i , for some $i \in \mathbb{Z}$, then every element in the image of G must look like $\phi(g)^i$. But since ϕ is onto then every element in H looks like $\phi(g)^i$. It follows that $\phi(g)$ generates H .

5. (a) Consider the functions $\sigma = (a_1a_2 \cdots a_k)$ and $\tau = (a_1a_k) \cdots (a_1a_3)(a_1a_2)$. We want to show $\sigma = \tau$, so we need to show $\sigma(x) = \tau(x)$, for all $x \in \{1, 2, 3, \dots, n\}$.

If $x = a_i$ for some i , then $\sigma(a_i) = a_{i+1 \bmod k}$. On the other hand, we have three cases:

(i) If $x = a_1$ then $\tau(a_1) = a_2$, as a_2 only appears in the far-most right transposition only. This is consistent with having $\sigma(a_1) = a_2$.

(ii) If $x = a_k$ then $\tau(a_k) = a_1$, as a_k only appears in the far-most left transposition only. This is consistent with having $\sigma(a_k) = a_1$.

(iii) If $x \neq a_1, a_k$ then a_i appears exactly once in the transpositions of τ . Hence, a_i will be fixed by whatever is to the right of $(a_1a_k) \cdots (a_1a_{i+1})(a_1a_i)$ (in the product of transpositions of τ). Now it is easy to see that a_i will be first moved to a_1 and then to a_{i+1} . Since a_{i+1} does not appear anymore in this product then $\tau(a_i) = a_{i+1}$, which is consistent with what σ does.

If $x \neq a_i$, for all i then both σ and τ fix this element.

Now consider the functions $\sigma = (a_1a_2 \cdots a_k)$ and $\tau = (a_1a_2)(a_2a_3) \cdots (a_{k-1}a_k)$. We want to show $\sigma = \tau$, so we need to show $\sigma(x) = \tau(x)$, for all $x \in \{1, 2, 3, \dots, n\}$.

If $x = a_i$ for some i , then $\sigma(a_i) = a_{i+1 \bmod k}$. On the other hand, we notice that every $a_i \neq a_1, a_k$ appears in exactly two cycles in τ . Hence, we need to take cases again:

(I) If $x = a_1$ then $\tau(a_1) = a_2$, as only the cycle (a_1a_2) affects a_1 . We are done because $\sigma(a_1) = a_2$.

(II) If $x = a_k$, then the first transposition on the right sends a_k to a_{k-1} , but then the next one sends a_{k-1} to a_{k-2} , and so on, until reaching a_1 . It follows that $\tau(a_k) = a_1$, which is exactly what σ does to a_k .

(III) If $x \neq a_1, a_k$ then the first cycle (on the right) that moves a_i is $(a_i a_{i+1})$, which sends a_i to a_{i+1} . At this point there are no a_{i+1} 's on the cycles to the left of $(a_i a_{i+1})$, and thus $\tau(a_i) = a_{i+1}$. Just like σ .

Since every permutation is a product of cycles, and each cycle is a product of transpositions, then it follows that each permutation is a product of transpositions.

(b) If we can get all transpositions out of products of $(12), (13), \dots, (1n)$ then, by part (a), we would be done.

We already have all transposition of the form $(1b)$, so let us consider (ab) , where a and b are both different from 1 and, of course $a \neq b$. But that is easy, as

$$(1a)(1b)(1a) = (ab)$$

6. See problem 6 in Spring '08 exam and problem 1 in spring '11 exam.

7. Let $p(x) \in \mathbb{R}[x]$. The factor theorem says that if $p(\alpha) = 0$, for some $\alpha \in \mathbb{R}$ then $p(x) = (x - \alpha)q(x)$, for some $q(x) \in \mathbb{R}[x]$. Hence, using this theorem twice we can re-write I as

$$I = \{p(x) \in \mathbb{R}[x]; p(x) = x(x - 1)r(x), \text{ for some } r(x) \in \mathbb{R}[x]\}$$

which is the set of all multiples (in $\mathbb{R}[x]$) of the polynomial $t(x) = x(x - 1)$. It follows that I is the principal ideal of $\mathbb{R}[x]$ generated by $t(x) = x(x - 1)$, which is most of the times denoted $t(x)\mathbb{R}[x]$.

8. If $\sqrt{d} \in \mathbb{Q}$, then $\mathbb{Q}[\sqrt{d}] \subseteq \mathbb{Q}$ (by closure of \mathbb{Q}). On the other hand, if considering the elements of $\mathbb{Q}[\sqrt{d}]$ with $b = 0$ we get $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{d}]$. It follows that, in this case, $\mathbb{Q} = \mathbb{Q}[\sqrt{d}]$.

For $\sqrt{d} \notin \mathbb{Q}$. It suffices to show that $\mathbb{Q}[\sqrt{d}]$ is a subfield of \mathbb{R} . First we observe that $0 = 0 + 0 \cdot d \in \mathbb{Q}[\sqrt{d}]$, so $\mathbb{Q}[\sqrt{d}] \neq \emptyset$.

Let $a_1 + b_1\sqrt{d}, a_2 + b_2\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$, thus $a_1, a_2, b_1, b_2 \in \mathbb{Q}$. Then

$$(a_1 + b_1\sqrt{d}) - (a_2 + b_2\sqrt{d}) = (a_1 - a_2) + (b_1 - b_2)\sqrt{d} \in \mathbb{Q}[\sqrt{d}].$$

Assume that $a_2 + b_2\sqrt{d} \neq 0$, i.e., $a_2 \neq 0$ and $b_2 \neq 0$. Then we observe that

$$(a_2 + b_2\sqrt{d})^{-1} = \frac{1}{a_2 + b_2\sqrt{d}} = \frac{a_2 - b_2\sqrt{d}}{a_2^2 - db_2^2} = \frac{a_2}{a_2^2 - db_2^2} + \frac{-b_2}{a_2^2 - db_2^2}\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$$

since $a_2^2 - db_2^2 \neq 0$ (here using that d is not a square) and $\frac{a_2}{a_2^2 - db_2^2}, \frac{-b_2}{a_2^2 - db_2^2} \in \mathbb{Q}$.

Then we have

$$\begin{aligned} (a_1 + b_1\sqrt{d})(a_2 + b_2\sqrt{d})^{-1} &= (a_1 + b_1\sqrt{d}) \left(\frac{a_2}{a_2^2 - db_2^2} - \frac{b_2}{a_2^2 - db_2^2}\sqrt{d} \right) \\ &= \frac{a_1a_2 - b_1b_2d}{a_2^2 - db_2^2} + \frac{-a_1b_2 + b_1a_2}{a_2^2 - db_2^2}\sqrt{d} \in \mathbb{Q}[\sqrt{d}]. \end{aligned}$$

Then, by the subfield test, $\mathbb{Q}[\sqrt{d}]$ is a subfield of \mathbb{R} . Done.

Part B.

1. (a) To find the first column vector of the transition matrix, we must find scalars a_1, a_2 and a_3 such that

$$a_1(1) + a_2(x+1) + a_3(x^2+x+1) = 1.$$

By inspection we see that the solution is $a_1 = 1, a_2 = 0$, and $a_3 = 0$. Therefore,

$$[1]_{B'} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}.$$

The second and third column vectors of the transition matrix can be found by solving the equations

$$b_1(1) + b_2(x+1) + b_3(x^2+x+1) = x$$

and

$$c_1(1) + c_2(x+1) + c_3(x^2+x+1) = x^2,$$

respectively. The solutions are given by $b_1 = -1, b_2 = 1$, and $b_3 = 0$, and $c_1 = 0, c_2 = -1$, and $c_3 = 1$. Hence, the transition matrix is

$$P_{B' \leftarrow B} = \begin{bmatrix} 1 & -1 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix}.$$

Remark: This can also be done by finding the inverse of $P_{B \leftarrow B'} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$, which is

obtained by ‘hanging’ the coordinates of the vectors $\{1, 1+x, 1+x+x^2\}$ in the standard basis.

- (b) The coordinate vector of $p(x) = 3 - x + 2x^2$ relative to B is given by

$$[p(x)]_B = \begin{bmatrix} 3 \\ -1 \\ 2 \end{bmatrix},$$

and therefore

$$[p(x)]_{B'} = P_{B' \leftarrow B} [p(x)]_B = \begin{bmatrix} 1 & -1 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 3 \\ -1 \\ 2 \end{bmatrix} = \begin{bmatrix} 4 \\ -3 \\ 2 \end{bmatrix}$$

is the coordinate vector of $p(x) = 3 - x + 2x^2$ relative to B' .

Notice also that $3 - x + 2x^2 = 4(1) - 3(x+1) + 2(x^2+x+1)$.

2. Using the Gram-Schmidt process, we have that $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ is an orthogonal basis, where $\mathbf{v}_1 = \mathbf{u}_1 = (0, 0, -1, 0)$, $\mathbf{v}_2 = \mathbf{u}_2 = (1, 3, 0, 0)$ (since $\mathbf{u}_1 \cdot \mathbf{u}_2 = 0$), and $\mathbf{v}_3 = (1, 0, 1, 1) - \frac{-1}{1}(0, 0, -1, 0) - \frac{1}{10}(1, 3, 0, 0) = (\frac{9}{10}, -\frac{3}{10}, 0, 1)$.

We have $|\mathbf{v}_1| = 1$, $|\mathbf{v}_2| = \sqrt{10}$, and $|\mathbf{v}_3| = \frac{\sqrt{190}}{10}$. Therefore an orthonormal basis is $\{(0, 0, -1, 0), \frac{1}{\sqrt{10}}(1, 3, 0, 0), \frac{10}{\sqrt{190}}(\frac{9}{10}, -\frac{3}{10}, 0, 1)\}$.

3. Since A is upper triangular, its eigenvalues are its diagonal entries, and A can thus be

diagonalized (since it has distinct eigenvalues). Thus, we will have $S^{-1}AS = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 9 \end{bmatrix}$,

where S is a matrix whose columns are eigenvectors of A for the respective eigenvalues.

The matrix $B = S \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{bmatrix} S^{-1}$ will then be the square root of A . Carrying out the computations, one obtains

$$S = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}, \quad S^{-1} = \begin{bmatrix} 1 & -1 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix}, \quad \text{giving } B = \begin{bmatrix} 1 & 1 & -1 \\ 0 & 2 & 1 \\ 0 & 0 & 3 \end{bmatrix}.$$

Remark: Another approach to this problem would be to assume that a square root of A , call it B , is upper triangular (not so crazy to assume, as these matrices form a subring of $M_3(\mathbb{C})$). Since $\det(A) = 36$ then $\det(B) = 6$. It follows that

$$B = \begin{bmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & 6/(ad) \end{bmatrix}$$

Easy computations show that $a = 1$ and $d = 2$. After that, all other values follow easily.

4. Since V is n -dimensional, there exist a linearly independent set $\{v_1, v_2, \dots, v_n\}$ that spans V . We wish to add some of the v_1, v_2, \dots, v_n to B' to form a basis of V . If $v_1 \in \text{span}(B')$, then let $S = B'$; otherwise, set $S = \{b_1, b_2, \dots, b_m, v_1\}$. Do this for each of the vectors v_2, v_3, \dots, v_n (i.e., if $v_k \in S$, then leave S unchanged; otherwise, add v_k to S). After each step, the set S is still linearly independent, since v_k was only added to the set if v_k was not in the span of the previous set of vectors. After n steps, $v_k \in \text{span}(S)$ for all $k = 1, 2, \dots, n$. Since $\{v_1, v_2, \dots, v_n\}$ spanned V , S spans V , and thus, S is a basis for V . So, letting b_m, b_{m+1}, \dots, b_n be equal to the vectors from $\{v_1, v_2, \dots, v_n\}$ that were added to S and defining $B = S$, we are done.

5. Since R is in reduced row echelon form, we must have

$$\mathbf{d} = \begin{bmatrix} 4 \\ 0 \\ 0 \end{bmatrix}.$$

The other two vectors provide solutions to the homogeneous system, and show that R has rank 1. Since R is in reduced row echelon form, the bottom two rows must be all 0, and the top row must be orthogonal to the vectors

$$\begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix} \quad \begin{bmatrix} 5 \\ 0 \\ 1 \end{bmatrix}$$

A few computations show that this vector could be $[1 - 2 - 5]^T$. Hence,

$$R = \begin{bmatrix} 1 & -2 & -5 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

6. Set $A\mathbf{x} = \mathbf{0}$. Then the solution space is $\left\{ \begin{bmatrix} 3z \\ -4z \\ z \\ 0 \end{bmatrix} \mid z \in \mathbb{R} \right\}$. Therefore it is of dimension 1,

and a basis is $\left\{ \begin{bmatrix} 3 \\ -4 \\ 1 \\ 0 \end{bmatrix} \right\}$.

Since A is 3×4 , the image is a subspace of \mathbb{R}^3 . Moreover, the dimension of the image is 3 since the dimension of the kernel is 1. A 3-dimensional subspace of \mathbb{R}^3 must be \mathbb{R}^3 itself, so we may use the standard basis $\{[1, 0, 0]^T, [0, 1, 0]^T, [0, 0, 1]^T\}$.

7. (a) Since the matrix $-A$ is obtained from A by multiplying each of the rows of A by -1 , and there are an odd number of rows, $\det(-A) = (-1)^n \det(A) = -\det(A)$. Since A is skew-symmetric, $\det(A) = \det(A^T) = \det(-A) = -\det(A)$. Thus, $\det(A) = 0$, and A is not invertible.
- (b) If n is even, then it could go either way. For example, the matrix

$$A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

is a 2×2 skew-symmetric matrix that is invertible. However, the matrix

$$A = \begin{bmatrix} 0 & 1 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{bmatrix}$$

is skew-symmetric, but is clearly not invertible.

8. (a) Suppose that $B\mathbf{v} \neq \mathbf{0}$ and $AB\mathbf{v} = \lambda\mathbf{v}$ for some $\lambda \in \mathbb{R}$. Then $A(B\mathbf{v}) = \lambda\mathbf{v}$. Left-multiply each side by B , and obtain $BA(B\mathbf{v}) = B(\lambda\mathbf{v}) = \lambda(B\mathbf{v})$. This equation says that $B\mathbf{v}$ is an eigenvector of BA , because $B\mathbf{v} \neq \mathbf{0}$.
- (b) Suppose that $A\mathbf{v} = \lambda\mathbf{v}$, with $\mathbf{v} \neq \mathbf{0}$. Then

$$\begin{aligned} (5I - 3A + A^2)\mathbf{v} &= 5\mathbf{v} - 3A\mathbf{v} + A(A\mathbf{v}) \\ &= 5\mathbf{v} - 3\lambda\mathbf{v} + \lambda^2\mathbf{v} \\ &= (5 - 3\lambda + \lambda^2)\mathbf{v}. \end{aligned}$$

Hence \mathbf{v} is an eigenvector of $5I - 3A + A^2$ with eigenvalue $5 - 3\lambda + \lambda^2$.