

SP/150

(1) Compute  $|GL_n(\mathbb{F}_p)|$ .

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}; \text{ where } a_{ij} \in \mathbb{F}_p.$$

Solution: Consider the matrix:

To make this an invertible matrix, there are  $p^n - 1$  choices for the first column (take away the zero vector). Now, for the second choice we have to exclude from the total number of vectors those that are multiples of the first. So we have  $p^n - p$ . Likewise, the third vector cannot be a multiple of either the first or second so there are  $p^n - p^2$ . Extending this argument we get

$$|GL_n(\mathbb{F}_p)| = (p^n - 1)(p^n - p)(p^n - p^2) \dots (p^n - p^{n-1})$$

For example:  $|GL_2(\mathbb{F}_p)| = (p^2 - 1)(p^2 - p)$ ;  $|GL_3(\mathbb{F}_p)| = (p^3 - 1)(p^3 - p)(p^3 - p^2)$ .

(2) Let  $p$  be prime and let  $R_p$  denote the following set of matrices:

$$R_p = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{F}_p \right\}$$

10

(a) Prove that  $R_p$  is a commutative ring.

Pf: Need to check the following:

(0)  $R_p$  is closed under  $+$ :

Let  $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}, \begin{pmatrix} c & -d \\ d & c \end{pmatrix} \in R_p$ . Then  $\begin{pmatrix} a & -b \\ b & a \end{pmatrix} + \begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \begin{pmatrix} a+c & -(b+d) \\ b+d & a+c \end{pmatrix} \in R_p$

$R_p$  is closed under  $\cdot$ :

Let  $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}, \begin{pmatrix} c & -d \\ d & c \end{pmatrix} \in R_p$ . Then  $\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \begin{pmatrix} ac - bd & -(ad + bc) \\ ad + bc & ac - bd \end{pmatrix} \in R_p$

(1)  $(R, +)$  is an abelian group since:

(i) clearly  $+$  is associative because  $+$  is associative in  $(\mathbb{F}_p, +)$ .

(ii) the identity w.r.t.  $+$  is  $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -0 \\ 0 & 0 \end{pmatrix} \in R_p$ .

(iii) Given  $\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in R_p$  its inverse is  $\begin{pmatrix} -a & b \\ -b & -a \end{pmatrix} \in R_p$ .

(2)  $\cdot$  is associative (this is inherited from the fact that matrix multiplication is associative).

(3) Consider  $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -0 \\ 0 & 1 \end{pmatrix} \in R_p$ . clearly this is the multiplicative identity.

Let  $\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in R_p$ . then  $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$

(4) Need to show:  $\forall A, B, C \in R_p$ :  $A \cdot (B+C) \stackrel{?}{=} AB + AC$   
 $(A+B) \cdot C \stackrel{?}{=} AC + BC$

Let  $A = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ ,  $B = \begin{pmatrix} c & -d \\ d & c \end{pmatrix}$ ,  $C = \begin{pmatrix} e & -f \\ f & e \end{pmatrix}$ ;  $A, B, C \in R_p$ .

$$\begin{aligned}
 A \cdot (B+C) &= \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \cdot \left[ \begin{pmatrix} c & -d \\ d & c \end{pmatrix} + \begin{pmatrix} e & -f \\ f & e \end{pmatrix} \right] = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \cdot \begin{pmatrix} c+e & -(d+f) \\ d+f & c+e \end{pmatrix} = \\
 &= \begin{pmatrix} a(c+e) - b(d+f) & -a(d+f) - b(c+e) \\ a(d+f) + b(c+e) & a(c+e) - b(d+f) \end{pmatrix} = \begin{pmatrix} ac+ae - bd-bf & -ad-af - bc-be \\ ad+af + bc+be & ac+ae - bd-bf \end{pmatrix} \\
 &= \begin{pmatrix} ac-bd+ae-bf & -ad-bc-af-be \\ ad+bc+af+be & ac-bd+ae-bf \end{pmatrix} = \begin{pmatrix} ac-bd & -(ad+bc) \\ ad+bc & ac-bd \end{pmatrix} \begin{pmatrix} ae-bf & -(af+be) \\ af+be & ae-bf \end{pmatrix} \\
 &= \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} c & -d \\ d & c \end{pmatrix} + \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} e & -f \\ f & e \end{pmatrix} = AB + AC.
 \end{aligned}$$

the other direction, i.e.,  $(B+C) \cdot A = BA + CA$  follows similarly.

(5) • is commutative. Let  $A = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ ,  $B = \begin{pmatrix} c & -d \\ d & c \end{pmatrix}$ ,  $A, B \in R_p$ .

$$\begin{aligned}
 A \cdot B &= \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \begin{pmatrix} ac-bd & -(ad+bc) \\ ad+bc & ac-bd \end{pmatrix} = \begin{pmatrix} ca-db & -(da+cb) \\ da+cb & ca-db \end{pmatrix} \\
 &= \begin{pmatrix} c & -d \\ d & c \end{pmatrix} \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = B \cdot A \quad (+10)
 \end{aligned}$$

(1), (2), (3), (4) & (5)  $\Rightarrow R_p$  is a commutative ring.

(b) Prove that  $R_3$  and  $R_7$  are fields, but  $R_5$  is not. Try to determine for which primes  $p$  the ring  $R_p$  is a field.

Pf: By definition,  $R_p$  will be a field if every non-zero element has an inverse w.r.t. • that is, every non-zero matrix has an inverse. We know that a matrix is invertible iff determinant is not zero. Hence •

For  $R_3$ : Let  $\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in R_3 \setminus \{0\} \Rightarrow \det \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = a^2 + b^2$ ; where  $a \neq 0$  or  $b \neq 0$ .

Possibilities are:  $a=0 \Rightarrow b=1, 2$  so  $1^2 = 1 \neq 0 \pmod{3}$ ;  $2^2 = 4 \neq 0 \pmod{3}$ .  
 (similar case when  $b=0$ ).  
 Now, if  $a=1 \Rightarrow b=0, 1, 2 \Rightarrow 1^2 + 0^2 = 1 \neq 0 \pmod{3}$ ;  $1^2 + 1^2 = 2 \neq 0 \pmod{3}$ ;  $1^2 + 2^2 = 5 \neq 0 \pmod{3}$ .  
 (similar case when  $b=1$ ).  
 Finally, if  $a=2 \Rightarrow b=0, 1, 2 \Rightarrow 2^2 + 0^2 = 4 \neq 0 \pmod{3}$ ;  $2^2 + 1^2 = 5 \neq 0 \pmod{3}$ ;  $2^2 + 2^2 = 8 \neq 0 \pmod{3}$ .  
 (similar case when  $b=2$ ).

So every non-zero matrix in  $R_3$  is invertible w.r.t. • ( $\det \neq 0$ )

For  $R_7$ : we have a similar argument but need to check more cases.

Let us summarize this information on a table:

Addition is associative, so I computed only half the table values and copied for convenience.

a\b	0	1	2	3	4	5	6
0	X	1	4	2	2	4	1
1	1	2	5	3	3	5	2
2	4	5	1	6	6	1	5
3	2	3	6	4	4	6	3
4	2	3	6	4	4	7	3
5	4	5	1	6	7	1	7
6	1	2	5	3	3	7	2

Entries on the table are computed as follow:  
 $a^2 + b^2 \pmod{7}$ .

None of these are zero, therefore all elements of  $\mathbb{F}_7 \setminus \{0\}$  are invertible w.r.t.  $\cdot$ .

In general, primes  $p$  s.t.  $p \nmid a^2 + b^2$ , where  $a, b \in \mathbb{F}_p$  and not both  $a, b$  are zero; are going to make  $\mathbb{F}_p$  a field. Otherwise, if  $p \mid a^2 + b^2$  (same conditions for  $a, b$  as before); then  $\mathbb{F}_p \setminus \{0\}$  will contain a matrix such that its determinant is congruent with zero mod  $p$  and hence, not invertible.

(3) Let  $V$  be an  $F$ -vector space and let  $W$  be a subspace. Prove that there is a one-to-one correspondence between the subspaces of  $V/W$  and the subspaces of  $V$  that contain  $W$ .

Pf: we want to find a correspondence:  $\frac{V}{W} \rightarrow V/W$ . Consider:  $W_i \rightarrow \pi(W_i) = \{ \pi(x) \mid x \in W_i \}$ ; where  $\pi$  is the canonical map, i.e.,  $\pi(x) = x + W$ . We have shown that this is a well defined map. We need to show that  $\pi(W_i) \leq V/W$ . (i)  $0 \in V/W$  is s.t.  $0 = \vec{0} + W$ . So, since  $W \subseteq W_i$ ,  $W_i$  is a subspace  $0 \in W_i \Rightarrow 0 = 0 + W_i \in \pi(W_i)$ .

(ii) Let  $W_a, W_b \in \pi(W_i)$ .  $W_a = a + W_i, W_b = b + W_i, W_a + W_b = (a + W_i) + (b + W_i) = (a + b) + W_i$ .  $\Rightarrow W_a + W_b \in \pi(W_i)$ . So it is closed under addition. Let  $\alpha \in F, W_a \in \pi(W_i)$ , then  $\alpha W_a = \alpha(a + W_i) = \alpha a + W_i$ , so  $\alpha$  is closed under scalar multiplication. (iii)  $\pi^{-1}(0) = \{ x \in V \mid \pi(x) = 0 \} = W$ . (iv)  $\pi^{-1}(u) = \{ x \in V \mid \pi(x) = u \}$ . We need to show  $\pi^{-1}(u) \leq V$ ,  $W \subseteq \pi^{-1}(u)$  and we are done. Clearly, if  $x \in W$  then  $x \in \pi^{-1}(u)$ , since  $\pi(x) = 0 \in u + W$ . (v) Let  $v_1, v_2 \in \pi^{-1}(u)$ . Then  $\pi(v_1) = u = \pi(v_2)$ .  $\pi(v_1 + v_2) = \pi(v_1) + \pi(v_2) = u + u = u \Rightarrow v_1 + v_2 \in \pi^{-1}(u)$ . Finally let  $\alpha \in F, v_1 \in \pi^{-1}(u) \Rightarrow \pi(\alpha v_1) = \alpha \pi(v_1) = \alpha u = u \Rightarrow \alpha v_1 \in \pi^{-1}(u)$ .

Now, to prove the one-to-one correspondence, we could prove that the map is 1-1 and onto, or we could just exhibit an inverse function. So consider  $U \leq V/W \rightarrow \pi^{-1}(U) = \{ x \in V \mid \pi(x) \in U \}$ . We need to show  $\pi^{-1}(U) \leq V$ ,  $W \subseteq \pi^{-1}(U)$  and we are done. Clearly, if  $x \in W$  then  $x \in \pi^{-1}(U)$ , since  $\pi(x) = 0 \in U$ . (ii) Let  $v_1, v_2 \in \pi^{-1}(U)$ . Then  $\pi(v_1) = u \in U = \pi(v_2)$ .  $\pi(v_1 + v_2) = \pi(v_1) + \pi(v_2) = u + u = u \in U \Rightarrow v_1 + v_2 \in \pi^{-1}(U)$ . Finally let  $\alpha \in F, v_1 \in \pi^{-1}(U) \Rightarrow \pi(\alpha v_1) = \alpha \pi(v_1) = \alpha u = u \in U \Rightarrow \alpha v_1 \in \pi^{-1}(U)$ .   
 Moreover: (i) Since  $U \leq V/W, 0 + W \in U \Rightarrow 0 \in \pi^{-1}(U)$ . (ii) Let  $v_1, v_2 \in \pi^{-1}(U)$ . Then  $\pi(v_1) = u \in U = \pi(v_2)$ .  $\pi(v_1 + v_2) = \pi(v_1) + \pi(v_2) = u + u = u \in U \Rightarrow v_1 + v_2 \in \pi^{-1}(U)$ . Finally let  $\alpha \in F, v_1 \in \pi^{-1}(U) \Rightarrow \pi(\alpha v_1) = \alpha \pi(v_1) = \alpha u = u \in U \Rightarrow \alpha v_1 \in \pi^{-1}(U)$ .   
 (iii)  $\pi^{-1}(u) = \{ x \in V \mid \pi(x) = u \}$ . We need to show  $\pi^{-1}(u) \leq V$ ,  $W \subseteq \pi^{-1}(u)$  and we are done. Clearly, if  $x \in W$  then  $x \in \pi^{-1}(u)$ , since  $\pi(x) = 0 \in u + W$ . (iv) Let  $v_1, v_2 \in \pi^{-1}(u)$ . Then  $\pi(v_1) = u = \pi(v_2)$ .  $\pi(v_1 + v_2) = \pi(v_1) + \pi(v_2) = u + u = u \Rightarrow v_1 + v_2 \in \pi^{-1}(u)$ . Finally let  $\alpha \in F, v_1 \in \pi^{-1}(u) \Rightarrow \pi(\alpha v_1) = \alpha \pi(v_1) = \alpha u = u \Rightarrow \alpha v_1 \in \pi^{-1}(u)$ .

(4) Let  $V$  be an  $n$ -dimensional vector space over a field  $F$ . Define  $A_m = \{ f: V^m \rightarrow F \mid f \text{ is multilinear, alternating} \}$ . Note  $A_m$  is a  $F$ -v.s.

(a) Prove that if  $m > n$ , then  $A_m = 0$ .

Pf: Let  $\{v_1, \dots, v_n\}$  be a basis for  $V$ . Let  $f \in A_m$  and  $u_1, \dots, u_m \in V$ . Consider  $f(u_1, \dots, u_m) = ?$ . Now, since  $u_1, \dots, u_m \in V$ ; we can write each of these vectors uniquely as linear combinations of elements in the basis. Therefore:

$$f(u_1, \dots, u_m) = f\left(\sum_{i=1}^n \alpha_{1i} v_i, \dots, \sum_{i=1}^n \alpha_{mi} v_i\right); \text{ for some scalars } \alpha_{ji}; 1 \leq j \leq m; 1 \leq i \leq n$$

However, since  $m > n$ , the set  $\{u_1, \dots, u_m\}$  must be linearly dependent.

So we can write at least one  $u_i$  as a linear combination of all other  $u$ 's. Without loss of generality, say  $u_1 = \sum_{i=2}^m \beta_i u_i$ . Then:

$$\begin{aligned} f(u_1, \dots, u_m) &= f\left(\sum_{i=2}^m \beta_i u_i, u_2, \dots, u_m\right) \\ &= \beta_2 f(u_2, u_2, \dots, u_m) + \beta_3 f(u_3, u_2, u_3, \dots, u_m) + \dots + \beta_m f(u_m, u_2, \dots, u_m) \\ &= \beta_2 \cdot 0 + \beta_3 \cdot 0 + \dots + \beta_m \cdot 0 \\ &= \boxed{0} \end{aligned}$$

since  $f$  is multilinear  
since  $f$  is alternating

Since the choice of  $u$ 's was arbitrary, we have that any function  $f \in A_m$  is zero always, hence  $A_m = 0$ . (10)

(b) Prove that if  $m \leq n$ , then the dimension of  $A_m$  is  $\binom{n}{m}$ .

Pf: We want to construct a basis for  $A_m$  and find that there are  $\binom{n}{m}$  vectors (i.e. functions  $f: V^m \rightarrow F$ ) in such basis. As usual, let  $\{v_1, \dots, v_n\}$  be a basis for  $V$ . claim:  $\{f_1, f_2, \dots, f_k\}$ , where  $k = \binom{n}{m}$  and  $f_i: V^m \rightarrow F$  are m.a. functions given by  $f_i(u_1, \dots, u_m) = \alpha_i f_i(v_{\alpha_1}, \dots, v_{\alpha_m})$ ; where  $\{v_{\alpha_1}, \dots, v_{\alpha_m}\}$  is a choice of  $\binom{n}{m}$   $v_i$ 's from the basis of  $V$ ; form a basis for  $A_m$ .

Pf: To conclude that  $\{f_1, \dots, f_k\}$  forms a basis it suffices to show that this is a linearly independent and spanning set. Now, since  $m \leq n$ , we can write each of  $u_i$  as linear combination of elements of the basis:  $f_i(u_1, \dots, u_m) = f_i\left(\sum_{j=1}^n \beta_{1j} v_j, \dots, \sum_{j=1}^n \beta_{mj} v_j\right)$ . Now, as shown before, some of the  $v_j$ 's will cancel leaving us with  $f_i = \alpha_i f(v_{\alpha_1}, \dots, v_{\alpha_m})$ , some choice of  $\binom{n}{m}$  vectors in the basis  $v_i$  exactly which depends of the choice of  $u_1, \dots, u_m$  but since these are arbitrary, we get the result.

(5) Each of the following is a basis of  $F_7^3$  over the field  $F_7$ .

$B = \left\{ \begin{pmatrix} -1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 3 \end{pmatrix} \right\}$ ,  $C = \left\{ \begin{pmatrix} 2 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 4 \\ 0 \\ 2 \end{pmatrix}, \begin{pmatrix} 0 \\ -1 \\ -1 \end{pmatrix} \right\}$ .

(+10)

(a) Find the change of basis matrix from  $B$  to  $C$  ( $P_{B,C}$ ), that is, find the matrix  $P$  such that  $P[v]_B = [v]_C$  for all  $v \in F_7^3$ .

Solution: We need to compute  $P = ([v_1]_C \ [v_2]_C \ [v_3]_C)$ , where  $v_1 = \begin{pmatrix} -1 \\ 1 \\ 1 \end{pmatrix}, v_2 = \begin{pmatrix} 0 \\ 2 \\ 3 \end{pmatrix}, v_3 = \begin{pmatrix} 1 \\ 0 \\ 3 \end{pmatrix}$ . For that purpose we need to solve the system  $\begin{bmatrix} 2 & 4 & 0 \\ 2 & 0 & 1 \\ 3 & 2 & -1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = v_i$ ; so that  $\begin{bmatrix} x \\ y \\ z \end{bmatrix} = [v_i]_C$ . Hence, let us invert the matrix  $\begin{bmatrix} 2 & 4 & 0 \\ 2 & 0 & 1 \\ 3 & 2 & -1 \end{bmatrix}$  and use it three times to compute  $[v_1]_C, [v_2]_C$  and  $[v_3]_C$ . (note:  $-1 \equiv 6 \pmod{7}$ ).

$$\left[ \begin{array}{ccc|ccc} 2 & 4 & 0 & 1 & 0 & 0 \\ 2 & 0 & 1 & 0 & 1 & 0 \\ 3 & 2 & 6 & 0 & 0 & 1 \end{array} \right] \xrightarrow{R_1=4R_1} \left[ \begin{array}{ccc|ccc} 1 & 2 & 0 & 4 & 0 & 0 \\ 2 & 0 & 1 & 0 & 1 & 0 \\ 3 & 2 & 6 & 0 & 0 & 1 \end{array} \right] \xrightarrow{\substack{R_3=R_3 \\ -R_1+R_2}} \left[ \begin{array}{ccc|ccc} 1 & 2 & 0 & 4 & 0 & 0 \\ 2 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 5 & 3 & 6 & 1 \end{array} \right] \xrightarrow{R_2=R_2-R_3} \left[ \begin{array}{ccc|ccc} 1 & 2 & 0 & 4 & 0 & 0 \\ 0 & 1 & 0 & 6 & 6 & 6 \\ 0 & 0 & 5 & 3 & 6 & 1 \end{array} \right]$$

$$\xrightarrow{R_2=2R_2} \left[ \begin{array}{ccc|ccc} 1 & 2 & 0 & 4 & 0 & 0 \\ 0 & 2 & 0 & 5 & 5 & 5 \\ 0 & 0 & 5 & 3 & 6 & 1 \end{array} \right] \xrightarrow{R_1=R_1-R_2} \left[ \begin{array}{ccc|ccc} 1 & 0 & 0 & 6 & 2 & 2 \\ 0 & 2 & 0 & 5 & 5 & 5 \\ 0 & 0 & 5 & 3 & 6 & 1 \end{array} \right] \xrightarrow{R_3=3R_3} \left[ \begin{array}{ccc|ccc} 1 & 0 & 0 & 6 & 2 & 2 \\ 0 & 2 & 0 & 5 & 5 & 5 \\ 0 & 0 & 1 & 2 & 4 & 3 \end{array} \right]$$

$$\xrightarrow{R_2=4R_2} \left[ \begin{array}{ccc|ccc} 1 & 0 & 0 & 6 & 2 & 2 \\ 0 & 1 & 0 & 6 & 6 & 6 \\ 0 & 0 & 1 & 2 & 4 & 3 \end{array} \right]. \text{ We can check that indeed: } \begin{pmatrix} 2 & 4 & 0 \\ 2 & 0 & 1 \\ 3 & 2 & 6 \end{pmatrix}^{-1} = \begin{pmatrix} 6 & 2 & 2 \\ 6 & 6 & 6 \\ 2 & 4 & 3 \end{pmatrix}$$

by:  $\begin{pmatrix} 2 & 4 & 0 \\ 2 & 0 & 1 \\ 3 & 2 & 6 \end{pmatrix} \begin{pmatrix} 6 & 2 & 2 \\ 6 & 6 & 6 \\ 2 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 6 & 2 & 2 \\ 6 & 6 & 6 \\ 2 & 4 & 3 \end{pmatrix} \begin{pmatrix} 2 & 4 & 0 \\ 2 & 0 & 1 \\ 3 & 2 & 6 \end{pmatrix}$ . Now we can compute:

$$[v_1]_C = \left[ \begin{pmatrix} -1 \\ 1 \\ 1 \end{pmatrix} \right]_C \Rightarrow \begin{bmatrix} 2 & 4 & 0 \\ 2 & 0 & 1 \\ 3 & 2 & -1 \end{bmatrix} [v_1]_C = \begin{bmatrix} -1 \\ 1 \\ 1 \end{bmatrix} \Rightarrow [v_1]_C = \begin{bmatrix} 6 & 2 & 2 \\ 6 & 6 & 6 \\ 2 & 4 & 3 \end{bmatrix} \begin{bmatrix} -1 \\ 1 \\ 1 \end{bmatrix} \Rightarrow [v_1]_C = \begin{bmatrix} 6 \\ 6 \\ 1 \end{bmatrix}$$

$$[v_2]_C = \left[ \begin{pmatrix} 0 \\ 2 \\ 3 \end{pmatrix} \right]_C \Rightarrow \begin{bmatrix} 2 & 4 & 0 \\ 2 & 0 & 1 \\ 3 & 2 & -1 \end{bmatrix} [v_2]_C = \begin{bmatrix} 0 \\ 2 \\ 3 \end{bmatrix} \Rightarrow [v_2]_C = \begin{bmatrix} 6 & 2 & 2 \\ 6 & 6 & 6 \\ 2 & 4 & 3 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \\ 3 \end{bmatrix} \Rightarrow [v_2]_C = \begin{bmatrix} 3 \\ 2 \\ 3 \end{bmatrix}$$

$$[v_3]_C = \left[ \begin{pmatrix} 1 \\ 0 \\ 3 \end{pmatrix} \right]_C \Rightarrow \begin{bmatrix} 2 & 4 & 0 \\ 2 & 0 & 1 \\ 3 & 2 & -1 \end{bmatrix} [v_3]_C = \begin{bmatrix} 1 \\ 0 \\ 3 \end{bmatrix} \Rightarrow [v_3]_C = \begin{bmatrix} 6 & 2 & 2 \\ 6 & 6 & 6 \\ 2 & 4 & 3 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 3 \end{bmatrix} \Rightarrow [v_3]_C = \begin{bmatrix} 5 \\ 3 \\ 4 \end{bmatrix}$$

Hence, the change of basis matrix  $P$  s.t.  $P[v]_B = [v]_C$  for all  $v \in F_7^3$  is

$$P = \begin{bmatrix} 6 & 3 & 5 \\ 6 & 2 & 3 \\ 1 & 3 & 4 \end{bmatrix}$$

e.g.  $[v_1]_B = \begin{bmatrix} -1 \\ 1 \\ 1 \end{bmatrix}$ ;  $P[v_1]_B = \begin{bmatrix} 6 \\ 6 \\ 1 \end{bmatrix} = [v_1]_C$ .

(b) Let  $A$  be the following matrix over  $F_7$ :

$$\begin{pmatrix} 1 & 0 & -1 \\ 2 & -2 & 0 \\ 3 & 1 & 1 \end{pmatrix}$$

Find the matrix  $L_A$  with respect to the basis  $B$ .

Solution. We want to find  $L_A = \pi_{E,B}^{-1} \pi_{E,B}(T)$ , where  $E = \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\}$  and  $B = \left\{ \begin{pmatrix} -1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 3 \end{pmatrix} \right\}$ ; that is:  $\pi_{E,B}(T) = \begin{pmatrix} [T(v_1)]_B & [T(v_2)]_B & [T(v_3)]_B \end{pmatrix}$   
 $= \begin{pmatrix} [T\left(\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}\right)]_B & [T\left(\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}\right)]_B & [T\left(\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}\right)]_B \end{pmatrix} = \begin{pmatrix} \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}_B & \begin{bmatrix} 0 \\ -2 \\ 1 \end{bmatrix}_B & \begin{bmatrix} -1 \\ 0 \\ 1 \end{bmatrix}_B \end{pmatrix}$ . Again let us invert

$$\begin{aligned} \left[ \begin{array}{ccc|ccc} 1 & 0 & 1 & 1 & 0 & 0 \\ -1 & 2 & 0 & 0 & 1 & 0 \\ 1 & 3 & 3 & 0 & 0 & 1 \end{array} \right] &\rightarrow \left[ \begin{array}{ccc|ccc} 1 & 0 & 1 & 1 & 0 & 0 \\ -1 & 2 & 0 & 0 & 1 & 0 \\ 0 & 5 & 3 & 0 & 1 & 1 \end{array} \right] &\rightarrow \left[ \begin{array}{ccc|ccc} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 2 & 1 & 1 & 1 & 0 \\ 0 & 5 & 3 & 0 & 1 & 1 \end{array} \right] \\ \rightarrow \left[ \begin{array}{ccc|ccc} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 2 & 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 0 & 3 & 3 \end{array} \right] &\rightarrow \left[ \begin{array}{ccc|ccc} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 6 & 1 & 5 & 4 \\ 0 & 1 & 2 & 0 & 3 & 3 \end{array} \right] &\rightarrow \left[ \begin{array}{ccc|ccc} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 6 & 1 & 5 & 4 \\ 0 & 0 & 3 & 6 & 5 & 6 \end{array} \right] \\ \rightarrow \left[ \begin{array}{ccc|ccc} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 6 & 1 & 5 & 4 \\ 0 & 0 & 1 & 2 & 4 & 2 \end{array} \right] &\rightarrow \left[ \begin{array}{ccc|ccc} 1 & 0 & 0 & 6 & 3 & 5 \\ 0 & 1 & 6 & 1 & 5 & 4 \\ 0 & 0 & 1 & 2 & 4 & 2 \end{array} \right] &\rightarrow \left[ \begin{array}{ccc|ccc} 1 & 0 & 0 & 6 & 3 & 5 \\ 0 & 1 & 0 & 3 & 2 & 6 \\ 0 & 0 & 1 & 2 & 4 & 2 \end{array} \right] \end{aligned}$$

One can indeed verify that  $\begin{bmatrix} 1 & 0 & 1 \\ -1 & 2 & 0 \\ 1 & 3 & 3 \end{bmatrix}^{-1} = \begin{bmatrix} 6 & 3 & 5 \\ 3 & 2 & 6 \\ 2 & 4 & 2 \end{bmatrix}$ , since

$$\begin{bmatrix} 1 & 0 & 1 \\ -1 & 2 & 0 \\ 1 & 3 & 3 \end{bmatrix} \begin{bmatrix} 6 & 3 & 5 \\ 3 & 2 & 6 \\ 2 & 4 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 6 & 3 & 5 \\ 3 & 2 & 6 \\ 2 & 4 & 2 \end{bmatrix} \begin{bmatrix} -1 & 0 & 1 \\ 1 & 2 & 0 \\ 1 & 3 & 3 \end{bmatrix}$$

therefore,  $\begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}_B = \begin{bmatrix} 6 & 3 & 5 \\ 3 & 2 & 6 \\ 2 & 4 & 2 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix} = \begin{bmatrix} 6 \\ 4 \\ 2 \end{bmatrix}$   
 $\begin{bmatrix} 0 \\ -2 \\ 1 \end{bmatrix}_B = \begin{bmatrix} 6 & 3 & 5 \\ 3 & 2 & 6 \\ 2 & 4 & 2 \end{bmatrix} \begin{bmatrix} 0 \\ -2 \\ 1 \end{bmatrix} = \begin{bmatrix} 6 \\ 2 \\ 1 \end{bmatrix}$   
 $\begin{bmatrix} -1 \\ 0 \\ 1 \end{bmatrix}_B = \begin{bmatrix} 6 & 3 & 5 \\ 3 & 2 & 6 \\ 2 & 4 & 2 \end{bmatrix} \begin{bmatrix} -1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 6 \\ 3 \\ 0 \end{bmatrix}$

$$\Rightarrow L_A = \begin{bmatrix} 6 & 6 & 6 \\ 4 & 2 & 3 \\ 2 & 1 & 0 \end{bmatrix}$$

↳ with respect to the basis  $B$ .

(c) Use your answer to (a) to find the matrix  $L_A$  w.r.t. the basis  $C$ .

Solution: By (a) we get that  $\pi_C(L_A) = P \pi_B(L_A) P^{-1}$ . We have  $P$ , all we need to do is compute  $P^{-1}$ .

$$\left[ \begin{array}{ccc|ccc} 6 & 3 & 5 & 1 & 0 & 0 \\ 6 & 2 & 3 & 0 & 1 & 0 \\ 1 & 3 & 4 & 0 & 0 & 1 \end{array} \right] \xrightarrow{R_2 = R_2 - R_1} \left[ \begin{array}{ccc|ccc} 6 & 3 & 5 & 1 & 0 & 0 \\ 0 & 6 & 5 & 6 & 1 & 0 \\ 1 & 3 & 4 & 0 & 0 & 1 \end{array} \right] \xrightarrow{R_1 = R_1 - R_3} \left[ \begin{array}{ccc|ccc} 5 & 0 & 1 & 1 & 0 & 6 \\ 0 & 6 & 5 & 6 & 1 & 0 \\ 1 & 3 & 4 & 0 & 0 & 1 \end{array} \right]$$

1403 - Fall 2013 - HW8 - Enrique Areyan

$$\left[ \begin{array}{ccc|ccc} 5 & 0 & 1 & 1 & 0 & 6 \\ 0 & 6 & 5 & 6 & 1 & 0 \\ 1 & 3 & 4 & 0 & 0 & 1 \end{array} \right] \xrightarrow{R_3=4R_3} \left[ \begin{array}{ccc|ccc} 5 & 0 & 1 & 1 & 0 & 6 \\ 0 & 6 & 5 & 6 & 1 & 0 \\ 4 & 5 & 2 & 0 & 0 & 4 \end{array} \right] \xrightarrow{R_1=R_1-R_3} \left[ \begin{array}{ccc|ccc} 1 & 2 & 6 & 1 & 0 & 2 \\ 0 & 6 & 5 & 6 & 1 & 0 \\ 4 & 5 & 2 & 0 & 0 & 4 \end{array} \right]$$

$$\xrightarrow{R_3=R_3-4R_1} \left[ \begin{array}{ccc|ccc} 1 & 2 & 6 & 1 & 0 & 2 \\ 0 & 6 & 5 & 6 & 1 & 0 \\ 0 & 4 & 6 & 3 & 0 & 3 \end{array} \right] \xrightarrow{R_2=R_2-R_3} \left[ \begin{array}{ccc|ccc} 1 & 2 & 6 & 1 & 0 & 2 \\ 0 & 2 & 6 & 3 & 1 & 4 \\ 0 & 4 & 6 & 3 & 0 & 3 \end{array} \right] \xrightarrow{R_2=R_2-R_3} \left[ \begin{array}{ccc|ccc} 1 & 2 & 6 & 1 & 0 & 2 \\ 0 & 5 & 0 & 0 & 1 & 1 \\ 0 & 4 & 6 & 3 & 0 & 3 \end{array} \right]$$

$$\xrightarrow{R_2=3R_2} \left[ \begin{array}{ccc|ccc} 1 & 2 & 6 & 1 & 0 & 2 \\ 0 & 1 & 0 & 0 & 3 & 3 \\ 0 & 4 & 6 & 3 & 0 & 3 \end{array} \right] \xrightarrow{R_1=R_1-R_2} \left[ \begin{array}{ccc|ccc} 1 & 5 & 6 & 1 & 0 & 6 \\ 0 & 1 & 0 & 0 & 3 & 3 \\ 0 & 4 & 6 & 3 & 0 & 3 \end{array} \right] \xrightarrow{R_3=R_3-4R_2} \left[ \begin{array}{ccc|ccc} 1 & 5 & 6 & 1 & 0 & 6 \\ 0 & 1 & 0 & 0 & 3 & 3 \\ 0 & 0 & 6 & 3 & 2 & 5 \end{array} \right]$$

$$\xrightarrow{R_1=R_1-5R_2} \left[ \begin{array}{ccc|ccc} 1 & 0 & 6 & 1 & 0 & 6 \\ 0 & 1 & 0 & 0 & 3 & 3 \\ 0 & 0 & 6 & 3 & 2 & 5 \end{array} \right] \xrightarrow{R_3=6R_3} \left[ \begin{array}{ccc|ccc} 1 & 0 & 6 & 1 & 0 & 6 \\ 0 & 1 & 0 & 0 & 3 & 3 \\ 0 & 0 & 1 & 4 & 5 & 2 \end{array} \right]$$

Hence,  $P^{-1} = \begin{bmatrix} 5 & 6 & 5 \\ 0 & 3 & 3 \\ 4 & 5 & 2 \end{bmatrix}$ . Indeed we can check that:

$$P P^{-1} = \begin{bmatrix} 6 & 3 & 5 \\ 6 & 2 & 3 \\ 1 & 3 & 4 \end{bmatrix} \cdot \begin{bmatrix} 5 & 6 & 5 \\ 0 & 3 & 3 \\ 4 & 5 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 5 & 6 & 5 \\ 0 & 3 & 3 \\ 4 & 5 & 2 \end{bmatrix} \cdot \begin{bmatrix} 6 & 3 & 5 \\ 6 & 2 & 3 \\ 1 & 3 & 4 \end{bmatrix}$$

Therefore, the matrix  $LA$  w.r.t. the basis  $C$  is

$$P M_B(LA) P^{-1} = \begin{bmatrix} 6 & 3 & 5 \\ 6 & 2 & 3 \\ 1 & 3 & 4 \end{bmatrix} \begin{bmatrix} 6 & 6 & 6 \\ 4 & 2 & 3 \\ 2 & 1 & 0 \end{bmatrix} \begin{bmatrix} 5 & 6 & 5 \\ 0 & 3 & 3 \\ 4 & 5 & 2 \end{bmatrix}$$

$$= \begin{bmatrix} 6 & 3 & 5 \\ 6 & 2 & 3 \\ 1 & 3 & 4 \end{bmatrix} \begin{bmatrix} 5 & 0 & 4 \\ 4 & 3 & 4 \\ 3 & 1 & 6 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & 3 \\ 5 & 2 & 1 \\ 1 & 6 & 5 \end{bmatrix}$$

$\rightarrow$  matrix  $LA$  w.r.t. basis  $C$ .

$\begin{pmatrix} 2 & 0 & 2 \\ 4 & 4 & 1 \\ 3 & 1 & 1 \end{pmatrix}$

$\begin{pmatrix} 4 & 1 & 0 \end{pmatrix}$