Course 374 (Cryptography)

Sample Paper 2

Dr Timothy Murphy

GMB ?? Friday, ?? 2007 ??:00–??:00

Attempt 4 questions from Part A, and 2 questions from Part B.

Part B

7. Show that the number of elements in a finite field is a prime power p^e; and show that there is exactly one field (up to isomorphism) with p^e elements.

Answer:

(a) *Suppose k is a finite field of characteristic p. Then the elements $0, 1, 2, \ldots, p-1$ form a subfield isomorphic to $\mathbb{F}_p = \mathbb{Z}/(p)$.*

We can consider k as a vector space over this subfield $\mathbb{F}_p$. If the vector space is of dimension d with basis $e_1, \ldots, e_d$ then k consists of the p^d elements

$$x = \lambda_1 e_1 + \cdots + \lambda_d e_d,$$

with $\lambda_i \in \{0, 1, \ldots, p-1\}$.

(b) *We have to show*

i. *There exists a field containing p^n elements.*

ii. Two fields containing p^n elements are isomorphic;

i. Let

$$U_n(x) = x^{p^n} - x \in \mathbb{F}_p[x].$$

We can construct a splitting field K for $U_n(x)$, ie a field in which $U_n(x)$ factorises completely into linear factors, by repeatedly adjoining roots of $U_n(x)$:

$$\mathbb{F}_p = k_0 \subset k_1 \subset \cdots \subset k_r = K,$$

where

$$k_{i+1} = k_i(\theta_i).$$

More precisely, suppose $U_n(x)$ factorises over k_i into irreducible factors, as

$$U_n(x) = f_1(x) \cdots f_s(x).$$

If all the factors are linear, we are done. If not, say $f_1(x)$ is not linear, then we adjoin a root of $f_1(x)$, ie we set

$$k_{i+1} = k_i[x]/(f_1(x)).$$

This 'splits off' a new linear factor $(x - \theta_i)$, where θ_i is a root of $f_1(x)$, and so of $U_n(x)$. Since $U_n(x)$ has at most p^n such factors, the process must end after at most p^n iterations.
The polynomial $U_n(x)$ splits completely in K, say

$$U_n(x) = (x - \alpha_1) \cdots (x - \alpha_{p^n}).$$

The factors must be distinct, ie $U_n(x)$ is separable, since

$$U_n'(x) = 1$$

and so

$$\gcd(U_n(x), U_n'(x)) = 1.$$

We claim that the roots

$$k = \{\alpha_1, \ldots, \alpha_{p^n}\}$$

form a subfield of k, containing p^n elements. For suppose $\alpha, \beta \in k$. Then

$$\begin{aligned} \alpha^{p^n} = \alpha,\ \beta^{p^n} = \alpha &\implies (\alpha\beta)^{p^n} = \alpha\beta \\ &\implies \alpha\beta \in k, \end{aligned}$$

while also

$$(\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha+\beta \implies \alpha+\beta \in k.$$

Thus we have constructed a field with p^n elements.

ii. *Suppose k, k' are two field with p^n elements. We assume the following result:*

Lemma 1. *If k is a finite field then the multiplicative group*

$$k^\times = k \setminus \{0\}$$

is cyclic.

Let $\pi \in k$ be a generator of $k^\times$ (ie a primitive element of k). Suppose the minimal polynomial of π over $\mathbb{F}_p$ is $m(x)$.
We also assume the following result (an easy consequence of Lagrange's Theorem):

Lemma 2. *If the field k contains p^n elements, say*

$$k = \{\alpha_1, \ldots, \alpha_{p^n}\}$$

then

$$U_n(x) = \prod_{\alpha\in k}(x-\alpha).$$

It follows in particular that

$$U_n(\pi) = 0.$$

Hence

$$m(x) \mid U_n(x).$$

Passing to k', since

$$U_n(x) = \prod_{\alpha'\in k'}(x-\alpha')$$

and

$$m(x) \mid U_n(x)$$

it follows that there is an element $\pi' \in k'$ satisfying

$$m(\pi') = 0.$$

Since $m(x)$ is irreducible, it is the minimal polynomial of π'. Hence if $f(x) \in \mathbb{F}_p[x]$ then

$$f(\pi) = 0 \iff m(x) \mid f(x) \iff f(\pi') = 0.$$

In particular, π' is a primitive element of k', since

$$\begin{aligned}{\pi'}^d = 1 &\implies \pi' \text{ is a root of } x^r - 1\\ &\implies \pi \text{ is a root of } x^r - 1\\ &\implies \pi^d = 1.\end{aligned}$$

Now we define a map

$$\theta : k \to k'$$

by setting

$$\theta(\pi^r) = {\pi'}^r,$$

together with $0 \mapsto 0$. We note that θ is well-defined, since π, π' have the same order.

Suppose

$$\alpha = \pi^r,\ \beta = \pi^s.$$

Then

$$\begin{aligned}\theta(\alpha\beta) &= \theta(\pi^{r+s})\\ &= {\pi'}^{r+s}\\ &= \theta(\alpha)\theta(\beta).\end{aligned}$$

Also

$$\alpha + \beta = \pi^t \implies f(\pi) = 0,$$

where

$$f(x) = x^r + x^s - x^t.$$

In this case

$$\begin{aligned}f(\pi') = 0 &\implies {\pi'}^r + {\pi'}^s = {\pi'}^t\\ &\implies \theta(\alpha) + \theta(\beta) = \theta(\alpha + \beta).\end{aligned}$$

It is trivial to show that these results also hold if one or more of $\alpha, \beta, \alpha + \beta$ is 0. Hence

$$\theta : k \to k'$$

is a ring-homomorphism.

Moreover, θ is injective since

$$\theta(\pi^r) = 0 \implies {\pi'}^r = 0 \implies \pi = 0.$$

which is impossible.

Hence θ is an isomorphism.

8. Show that a finite abelian group A is the direct sum of its p-primary parts A_p (consisting of the elements of order p^e for some e).

Determine whether the equation

$$y^2 + xy = x^3 + 1$$

defines an elliptic curve over each of the fields $\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_4, \mathbb{F}_5, \mathbb{F}_7, \mathbb{F}_8, \mathbb{F}_9$; and in those cases where it does, determine the group on the curve.

Answer:

(a) *Suppose*

$$|A| = n = p_1^{e_1} \cdots p_r^{e_r}$$

Let

$$q_i = \prod_{j \neq i} p_j^{e_j} = \frac{n}{p_i^{e_i}}.$$

Then $q_1, \ldots, q_r$ *are co-prime, and so (by the Chinese Remainder Theorem) we can find* $m_1, \ldots, m_r$ *such that*

$$m_1 q_1 + \cdots + m_r q_r = 1.$$

Thus if $a \in A$ *then*

$$a = m_1 q_1 a + \cdots + m_r q_r a.$$

But

$$m_i q_i a \in A_{p_i}$$

since

$$\begin{aligned} p_i^{e_i}(m_i q_i a) &= m_i (p_i^{e_i} q_i) a \\ &= m_i (na) \\ &= 0. \end{aligned}$$

Thus

$$A = A_{p_1} + \cdots + A_{p_r}.$$

It remains to show that the sum is direct. Suppose

$$a_1 + \cdots + a_r = 0,$$

where $a_i \in A_{p_i}$.

By Lagrange's Theorem,

$$p_j^{e_j} a_j = 0.$$

It follows that

$$q_i a_j = 0$$

if $i \neq j$. Hence

$$q_i a_i = 0$$

But since

$$\gcd(p_i^{e_i}, q_i) = 1$$

we can find r, s such that

$$r p_i^{e_i} + s q_i = 1.$$

Then

$$\begin{aligned} a_i &= r p_i^{e_i} a_i + s q_i a_i \\ &= 0 + 0. \end{aligned}$$

Thus

$$a_1 = \cdots = a_r = 0,$$

and so the sum is direct.

(b) $k = \mathbb{F}_2$ *The equation takes the homogeneous form*

$$F(X, Y, Z) \equiv Y^2 Z + XYZ + X^3 + Z^3 = 0.$$

We have

$$\begin{aligned} \partial F/\partial X &= YZ + X^2, \\ \partial F/\partial Y &= XZ, \\ \partial F/\partial Z &= Y^2 + XY + Z^2. \end{aligned}$$

At a singular point,

$$XZ = 0 \implies X = 0 \text{ or } Z = 0.$$

But

$$X = 0 \implies YZ = 0,\ Y^2 + Z^2 = 0 \implies Y = Z = 0,$$

while

$$Z = 0 \implies X = 0 \implies Y = 0.$$

Thus there is no singular point, and we have an elliptic curve.
Returning to the inhomogeneous equation,

$$x = 0 \implies y^2 = 0 \implies y = 0,$$

while

$$x = 1 \implies y^2 + y = 0,$$

which is true for $y = 0, 1$.
Thus there are 3 affine points $(0,1),\ (1,0),\ (1,1)$ *on the curve, which together with the point at infinity gives a group of order 4.*
We have to determine if the group is

$$\mathbb{Z}/(4) \text{ or } \mathbb{Z}/(2) \oplus \mathbb{Z}/(2).$$

We can distinguish between these by the number of elements of order 2; the first group has 1, the second has 3.
Suppose $P = (x_0, y_0)$*, Then* $-P$ *is the point where the line* OP *through the point at infinity* $O = [0, 1, 0]$ *meets the curve again. This is the line*

$$x = x_0.$$

Thus P *is of order 2, ie* $-P = P$*, if and only if this line meets the curve just once.*
Since there is only 1 point with $x = 0$*, the line* $x = 0$ *meets the curve twice at* $A = (0, 0)$*. Thus* A *is of order 2.*
There are two points on the line $x = 1$*, so neither is of order 2.*
We conclude that the group is $\mathbb{Z}/(4)$*.*

$k = \mathbb{F}_3$ *Completing the square on the left, the equation becomes*

$$(y + x/2)^2 = x^3 + x^2/4 + 1,$$

ie

$$y'^2 = x^3 + x^2 + 1,$$

on setting $y' = y + x/2 = y - x$ *and noting that* $1/4 = 1 \bmod 3$.
The polynomial $p(x) = x^3 + x^2 + 1$ *is separable, since* $p'(x) = 2x$ *and so* $\gcd(p(x), p'(x)) = 1$*. Hence the curve is elliptic.*
The quadratic residues $\bmod 3$ *are* $0, 1$.

We draw up a table for x, x^3+x^2+1 and possible y:

x	x^3+x^2+1	y'
0	1	± 1
1	0	0
-1	1	± 1

Thus the curve has 6 points (including the point at infinity). There is only one abelian group of order 6, namely $\mathbb{Z}/(6)$, so we conclude that this is the group on the curve.

$k = \mathbb{F}_4$ *The argument in the case $k = \mathbb{F}_2$ shows that the curve is non-singular, ie an elliptic curve $\mathcal{E}(\mathbb{F}_4)$. Also*

$$\mathcal{E}(\mathbb{F}_2) = \mathbb{Z}/(4)$$

is a subgroup:

$$\mathcal{E}(\mathbb{F}_2) \subset \mathcal{E}(\mathbb{F}_4).$$

In particular, $\mathcal{E}(\mathbb{F}_4)$ is of order $4m$ for some m.
Suppose $P = (a, b) \in \mathcal{E}(\mathbb{F}_4)$. The line

$$OP : x = a$$

meets the curve where

$$y(y + a) = a^3 + 1.$$

Thus OP meets the curve again at

$$-P = (a, y + a).$$

Note that

$$-P = P \iff a = 0 \iff P = (0, 1).$$

It follows that there is just 1 point of order 2.
If $x \in \mathbb{F}_4^\times$ then

$$x^3 = 1,$$

and so the equation reduces to

$$y(y + x) = 0.$$

Thus there are 2 solutions $(x, 0)$, (x, x) for each $x \in \mathbb{F}_4 \setminus \mathbb{F}_2$. It follows that there are 8 points on the curve. Since there is a subgroup $\mathbb{Z}/(4)$ the group is either

$$\mathbb{Z}/(8) \text{ or } \mathbb{Z}/(4) \oplus \mathbb{Z}/(2).$$

Since there is only one point of order 2, we conclude that the group is $\mathbb{Z}/(8)$.

$k = \mathbb{F}_5$ *In this case* $1/4 = -1$ *and the curve takes the form*

$$y^2 = p(x) \equiv x^3 - x^2 + 1.$$

Since

$$p'(x) = 3x^2 - 2x = 3x(x + 1).$$

Since neither 0 nor 1 is a root of $p(x)$*, the polynomial is separable, and the curve is elliptic.*
The quadratic residues mod5 *are* $\{0, \pm 1\}$.
We draw up a table as before:

x	$x^3 - x^2 + 1$	y
0	1	± 1
1	1	± 1
2	0	0
-1	-1	± 2
-2	-1	± 2

Thus there are $9 + 1 = 10$ *points on the curve. Hence the group is* $\mathbb{Z}/(10)$.

$k = \mathbb{F}_7$ *Since* $1/4 = 2$ *in this case, the equation is*

$$y^2 = p(x) \equiv x^3 + 2x^2 + 1.$$

We have

$$p'(x) = 3x^2 + 4x = 3x(x - 1).$$

Since neither 0 nor 1 is a root of $p(x)$*, the polynomial is separable, and the curve is elliptic.*
The quadratic residues mod7 *are* $\{0, 1, 2, -3\}$.
We draw up a table as before:

x	$x^3 + 2x^2 + 1$	y
0	1	± 1
1	-3	± 2
2	2	± 3
3	-3	± 2
-1	2	± 3
-2	1	± 1
-3	-1	$-$

Thus there are $12 + 1 = 13$ *points on the curve. Hence the group is* $\mathbb{Z}/(13)$.

$k = \mathbb{F}_8$ *The argument in the cases* $\mathbb{F}_2$ *and* $\mathbb{F}_4$ *remains valid here; the curve is non-singular and so elliptic.*

As before, we can write the equation as

$$y(y + x) = x^3 + 1.$$

Thus the points appear in pairs $P = (x, y)$, $-P = (x, y + x)$, *except when* $x = 0$, *in which case there is just one point* $(0, 1)$ *of order 2.*

Also, as in the case $\mathbb{F}_4$,

$$\mathcal{E}(\mathbb{F}_2) = \mathbb{Z}/(4) \subset \mathcal{E}(\mathbb{F}_8),$$

and in particular there are $4n$ *points for some* n.

[But note that $\mathbb{F}_4$ *is* not *a subfield of* $\mathbb{F}_8$.*]*

The Frobenius automorphism

$$\Phi : (x, y) \mapsto (x^2, y^2)$$

has order 3; so either

$$\Phi(P) = P \iff P \in \mathcal{E}(\mathbb{F}_2)$$

or else there is a triplet of points

$$\{P,\ \Phi P,\ \Phi^2 P\}.$$

It follows that the number of points in $\mathcal{E}(\mathbb{F}_8) \setminus \mathcal{E}(\mathbb{F}_2)$ *is divisible by 3, as well as 4.*

Since there are at most 2 values of y *for each of the 8 values of* x, *there are at most 16 points on the curve (there is just one point for* $x = 0$ *to balance the additional point at infinity).*

It follows that the curve contains either 4 or 16 points.

Hasse's Theorem tells us that the number N *of points on the curve satisfies*

$$|N - 9| \leq 2\sqrt{8} < 6,$$

from which it follows that

$$4 \leq N \leq 14.$$

Hence $N = 4$, *and so the group is* $\mathbb{Z}/(4)$.

$k = \mathbb{F}_9$ *As in the case* $\mathbb{F}_3$*, we can complete the square on the left and the curve takes the form*

$$y^2 = p(x) \equiv x^3 + x^2 + 1.$$

We know that

$$\mathcal{E}(\mathbb{F}_3) = \mathbb{Z}/(6) \subset \mathcal{E}(\mathbb{F}_9).$$

In particular the curve has $6m$ *points for some* m*.*
Recall that the point (x, y) *is of order 2 if* $y = 0$ *and* $p(x) = 0$*.*
We know that $(1, 0)$ *is one such point. In fact*

$$p(x) = (x - 1)(x^2 - x - 1).$$

The polynomial $g(x) = x^2 - x - 1$ *is irreducible over* $\mathbb{F}_3$ *(since none of* $\{0, \pm 1\}$ *are roots). It follows that*

$$\mathbb{F}_9 = \mathbb{F}_3[x]/(g(x)).$$

Hence

$$g(x) = (x - \alpha)(x - \beta)$$

with $\alpha, \beta \in \mathbb{F}_9$*.*
Thus there are 3 points of order 2 on the curve. Hence the 2-primary part of the group contains at least 4 points, and so the curve contains $12n$ *points for some* n*.*
There are at most 2 points for each $x \in \mathbb{F}_9$*. [In fact only 1 for* $x = 1, \alpha, \beta$*.] It follows that the curve has 12 points. Since there are 3 points of order 2, the 2-primary part is* $\mathbb{Z}/(2) \oplus \mathbb{Z}/(2)$*. Hence the group is*

$$\mathbb{Z}/(2) \oplus \mathbb{Z}/(2) \oplus \mathbb{Z}/(3) = \mathbb{Z}/(6) \oplus \mathbb{Z}/(2).$$

9. Show that the map

$$\Phi : x \mapsto x^p$$

is an automorphism of the finite field $\mathbb{F}_{p^e}$; and show that every automorphism of this field is of the form Φ^r for some r.

Find an irreducible polynomial f(x) of degree 5 over $\mathbb{F}_2$. Hence or otherwise determine the group on the elliptic curve

$$y^2 + y = x^3 + x$$

over $\mathbb{F}_{2^5}$.

Answer:

(a) *We have*

$$\begin{aligned}\Phi(xy) &= (xy)^p \\ &= x^p y^p \\ &= \Phi(x)\Phi(y)\end{aligned}$$

while

$$\begin{aligned}\Phi(x+y) &= (x+y)^p \\ &= x^p + y^p \\ &= \Phi(x) + \Phi(y),\end{aligned}$$

since

$$p \mid \binom{n}{r}$$

for $r = 1, \ldots, n-1$.

Thus Φ *is a ring-homomorphism. Moreover,* Φ *is injective since*

$$\Phi(x) = 0 \implies x^p = 0 \implies x = 0.$$

Hence Φ *is bijective (since the field is finite), ie* Φ *is an automorphism.*

(b) *Suppose* Θ *is an automorphism of* $k = \mathbb{F}_{p^e}$. *By definition* $\Theta(1) = 1$. *Hence* Θ *leaves invariant the elements of the prime subfield* $\mathbb{F}_p$.

We assume the following result:

Lemma 3. *Suppose* $f(x)$ *is an irreducible polynomial of degree* e *over* $\mathbb{F}_p$. *Then* $f(x)$ *factorizes completely over* $\mathbb{F}_{p^e}$*; and if* α *is one root then the others are*

$$\Phi(\alpha), \Phi^2(\alpha), \Phi^{e-1}(\alpha).$$

[This follows from the fact that the polynomial

$$\prod_{0 \le i < e} (x - \Phi^i \alpha)$$

is fixed under Φ*, and so has coefficients in* $\mathbb{F}_p$*.]*

Let π *be a primitive element of* k. *Then* Θ *is completely determined by* $\Theta(\pi)$*, since*

$$\Theta(\pi^r) = \Theta(\pi)^r.$$

Suppose $m(x)$ is the minimal polynomial of π over $\mathbb{F}_p$. Then Θ leaves $m(x)$ invariant, since it leaves $\mathbb{F}_p$ invariant. It follows that Θ permutes the roots of $m(x)$.

But by the Lemma, these roots are $\pi, \Phi\pi, \ldots, \Phi^{e-1}\pi$. Hence

$$\Theta\pi = \Phi^r\pi$$

for some r. It follows that

$$\Theta = \Phi^r.$$

(c) *If a polynomial of degree 5 is reducible then it must have a factor of degree 1 or 2.*

There is just one irreducible polynomial of degred 2 over $\mathbb{F}_2$, namely $m(x) = x^2 + x + 1$. Thus a polynomial $f(x) \in \mathbb{F}_2[x]$ of degree 5 is irreducible unless it is divisible by $x, x+1$ or $m(x)$.

Also

$$x^3 \equiv 1 \bmod m(x),$$

since

$$x^3 - 1 = (x-1)m(x).$$

Let

$$f(x) = x^5 + x^2 + 1.$$

Then

$$f(0) = f(1) = 1,$$

while

$$f(x) \equiv x^2 + x^2 + 1 = 1 \bmod m(x)$$

since $x^5 \equiv x^2$. Hence $f(x)$ is irreducible.

(d) *Let us first verify that the curve is non-singular. The equation takes homogeneous form*

$$F(X,Y,Z) = Y^2Z + YZ^2 + X^3 + XZ^2 = 0.$$

We have

$$\begin{aligned}
\partial F/\partial X &= X^2 + Z^2,\\
\partial F/\partial Y &= Z^2,\\
\partial F/\partial Z &= Y^2.
\end{aligned}$$

Thus at a singular point,

$$Y = Z = 0 \implies X = 0.$$

Hence there are no singular points, and the curve is elliptic.

Three ideas help us determine the group on the curve:

i. *Consider the points on the curve defined over* $\mathbb{F}_2$*, forming the subgroup* $\mathcal{E}(\mathbb{F}_2) \subset \mathcal{E}(\mathbb{F}_{2^5})$*. It is readily verified that all 4 affine points*

$$(0,0),\ (0,1),\ (1,0),\ (1,1)$$

lie on the curve. Adding the point at infinity, it follows that

$$\mathcal{E}(\mathbb{F}_2) = \mathbb{Z}/(5).$$

In particular $\mathcal{E}(\mathbb{F}_{2^5})$ *contains* $5m$ *points, for some* m.

ii. *The equation can be written*

$$y(y+1) = x^3 + x.$$

It follows that if $P = (a, b)$ *is on the curve then so is* $-P = (a, b+1)$*. (This second point is* $-P$ *because it is the point where the line*

$$OP : x = a$$

meets the curve again.)
We see in particular that there are no points of order 2 on $\mathcal{E}(\mathbb{F}_{2^5})$*. So the number* N *of points is odd:* $5, 15, \ldots$.

iii. *Hasse's Theorem tells us that*

$$|N - 33| \le 2\sqrt{32} = 8\sqrt{2}.$$

Since $[8\sqrt{2}] = 11$*, this yields*

$$22 \le N \le 44.$$

Thus

$$N = 25 \text{ or } 35.$$

This leaves 3 possible cases:

$$\mathbb{Z}/(25),\ \mathbb{Z}/(35) \text{ and } \mathbb{Z}/(5) \oplus \mathbb{Z}/(5).$$

iv. *Consider the action of the Frobenius automorphism*

$$\Phi : (x, y) \mapsto (x^2, y^2) : \mathcal{E}(\mathbb{F}_{2^5}) \to \mathcal{E}(\mathbb{F}_{2^5}).$$

The fixed points of this map are precisely the 5 points of $\mathcal{E}(\mathbb{F}_2)$. *Moreover,*

$$\Phi^5 = I.$$

Thus the group

$$\langle \Phi \rangle = C_5$$

acts on the group on the curve; and the fixed elements under this action form a subgroup of order 5.

This last observation allows us to distinguish between the 3 cases.

An automorphism θ *of the group* $\mathbb{Z}/(n)$ *is completely determined by*

$$\theta(\bar{1}) = \bar{a}.$$

Moreover, a *must be invertible* $\bmod n$. *It follows that*

$$\mathrm{Aut}(\mathbb{Z}/(n)) = (\mathbb{Z}/n)^\times.$$

This group has $\phi(n)$ *elements; and since*

$$\phi(35) = \phi(5)\phi(7) = 4 \cdot 6 = 24,$$

the automorphism group of $\mathbb{Z}/(35)$ *cannot contain an element of order 5; so this case is impossible.*

The group $A = \mathbb{Z}/(25)$ *has just one subgroup* B *with 5 elements. If an automorphism*

$$\theta : A \to A$$

has $\ker\theta = B$ *then* $\mathrm{im}\,\theta = B$ *and so* $\theta^2 = 0$, *contradicting the assumption that* θ *is an automorphism.*

We are left with only 1 possibility; the group must be $\mathbb{Z}/(5) \oplus \mathbb{Z}/(5)$.

[Although not necessary for this question, it is worth noting that we can regard the group $\mathbb{Z}/(5) \oplus \mathbb{Z}/(5)$ *as a 2-dimensional vector space over the field* $\mathbb{F}_5$.

Thus the automorphism group of this group is $\mathrm{GL}(2, \mathbb{F}_5)$, *the group of invertible* 2×2 *matrices over the field* $\mathbb{F}_5$.

We can construct such a matrix by first choosing a non-zero vector for first column; this can be done in $5^2 - 1 = 24$ *ways. Then any* *vector can be chosen for the second row, except for the 5 scalar products of the first row. This can be done in* $5^2 - 5 = 20$ *ways. It follows that the automorphism group in this case has 480 elements. By Sylow's Theorem, the subgroups of order 5 are all conjugate; a typical one is formed by the matrices*

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \qquad (a \in \mathbb{F}_5).$$

It is readily verified that this automorphism subgroup leaves invariant a 1-dimensional subspace containing 5 vectors.]