Math 594. Solutions 1

1. Let V and W be finite-dimensional vector spaces over a field F. Let $G = \mathrm{GL}(V)$ and $H = \mathrm{GL}(W)$ be the associated general linear groups. Let X denote the vector space $\mathrm{Hom}_F(V, W)$ of linear maps from V to W, but viewed only as a set (i.e., we ignore that X has a natural structure of F-vector space via pointwise operations). Recall that X has a natural left H-action and right G-action through composition and inner composition respectively (i.e., $h.x = h \circ x$ while $x.g = x \circ g$).

(*i*) If $x = x'g$ for some $g \in G$ then since $g \in \mathrm{GL}(V)$, we have $gV = V$ and therefore $x(V) = x'(V)$. Conversely, suppose that $x(V) = x'(V) = U \subset W$. We first take a brief aside: Any surjective map $f : V \to U$ of finite dimensional vector spaces induces an injective map $f^* : U^* \to V^*$ via $f^*(a) = a \circ f$. Injectivity of f^* follows from the fact that given $a \neq b \in U^*$ we can find $u \in U$ such that $a(u) \neq b(u)$, and, since f is surjective, there exists $v \in V$ with $f(v) = u$ and hence $f^*(a)(v) \neq f^*(b)(v)$, i.e. $f^*(a) \neq f^*(b)$. Now since $x(V) = x'(V) = U$ we have two embeddings $x^* : U^* \hookrightarrow V^*$ and $x'^* : U^* \hookrightarrow V^*$. This gives an automorphism of V^* taking $x^*(U^*)$ to $x'^*(U^*)$. Taking the dual of this automorphism gives the required automorphism of V, using the identifications $V^{**} = V$, $U^{**} = U$, and $W^{**} = W$.

(*ii*) We claim that two elements of X lie in the same H orbit if and only if they have the same kernel in V. On direction is clear: if $x = hx'$ and $v \in \ker(x)$ then $0 = hx'(v)$. But since $h \in \mathrm{GL}(W)$, it has kernel 0 so that $x'(v) = 0$, i.e. $\ker(x) \subseteq \ker(x')$. Symmetry then gives equality. Conversely, suppose that $\ker(x) = \ker(x') = U \subset V$. Then we get two embeddings $x : V/U \hookrightarrow W$ $x' : V/U \hookrightarrow W$ which induce an automorphism of $x(V) \subset W$ that can lifted (again by extending a basis of $x(V)$ to a basis of W) to an automorphism h of W satisfying $x = hx'$.

(*iii*) In the case $W = F$ we have $X = \mathrm{Hom}_F(V, F) = V^*$. If $x \in V^*$ is not the zero map, then there exists $v \in V$ such that $x(v) = \alpha \neq 0$ so that $x(\lambda v) = \lambda\alpha$ for all $\lambda \in F$, i.e. the image of V under x is all of F. It follows by part (*i*) that there are precisely two orbits of G on V^*, namely, the orbit consisting of only the zero map, and the orbit consisting of all nonzero maps. In other words, G acts transitively on the set of lines in V^*. But as we show in Problem 3 (*i*), the set of lines in V^* is identified with the set of hyperplanes in V, and this identification is compatible with the action of G, so that G acts transitively on this set also.

2. Let F be a field, and define $S^1(F) = \{(a, b) \in F^2 \mid a^2 + b^2 = 1\}$.

(*i*) In the case $F = \mathbf{R}$, there is an obvious way to add points on the unit circle: namely, addition of angles. Recall that $S^1(\mathbf{R})$ is parameterized by $(\cos(\theta), \sin(\theta))$ and that we have the addition formulae

$$\cos(\theta + \phi) = \cos(\theta)\cos(\phi) - \sin(\theta)\sin(\phi)$$
$$\sin(\theta + \phi) = \sin(\theta)\cos(\phi) + \cos(\theta)\sin(\phi).$$

This suggests endowing $S^1(F)$ with a group structure by the rules

$$(a, b)(c, d) = (ac - bd, ad + bc)$$

and

$$(a, b)^{-1} = (a, -b).$$

It is not difficult to check that this makes $S^1(F)$ into an abelian group (one must check associativity and commutativity) with identity $(1, 0)$.

(*ii*) Suppose that $\mathrm{char}(F) \neq 2$ and define $\phi_i : S^1(F) \to F^\times$ by $\phi_i(a, b) = a + bi$. Observe that

$$\phi_i((a, b)(c, d)) = (ac - bd) + (ad + bc)i = (a + bi)(c + di) = \phi_i(a, b)\phi_i(c, d)$$

so that ϕ_i is a group homomorphism since clearly $\phi(1, 0) = 1$. Now if $\phi(a, b) = a + bi = 1$ then since $(a + bi)(a - bi) = 1$ we also have $a - bi = 1$ and therefore $a = 1, b = 0$ since $2 \neq 0$ in F. Thus, ϕ_i is injective. Now suppose that $x \in F^\times \setminus \{0\}$. Let

$$a = \frac{1}{2}\left(x + \frac{1}{x}\right) \qquad b = \frac{1}{2i}\left(x - \frac{1}{x}\right).$$

Then we have $a + bi = x$ and $a - bi = 1/x$ and hence $(a, b) \in S^1(F)$. Since $x \in F^\times$ was chosen arbitrarily, ϕ_i is surjective and hence that ϕ_i is an isomorphism. With $\phi_{-i} = a - bi$, observe that $\phi_{-i} \circ \phi_i^{-1}(x) = x^{-1}$. Meanwhile, if $\mathrm{char}(F) = 2$, define $\phi : S^1(F) \to F$ by $\phi(a, b) = b$. We have

$$\phi((1-b, b)(1-d, d)) = (1-b)d + (1-d)b = b + d = \phi(1-b, b) + \phi(1-d, d),$$

so that ϕ is a group homomorphism as $\phi(1, 0) = 0$. The map ϕ is certainly injective as $\phi(a, b) = 0$ if and only if $(a, b) = (1, 0)$. To see surjectivity, observe that $a^2 + b^2 = (a + b)^2 = 1$ if and only if $a + b = 1$ so that every $(a, b) \in S^1(F)$ satisfies $a = 1 - b$, and it is clear that $(1 - b, b) \in S^1(F)$ maps to $b \in F$ under ϕ. Thus, ϕ is an isomorphism.

(*iii*) In a word: No. Since we have a field automorphism carrying i to $-i$, the field structure cannot "tell the difference" between the two.

3. Let $F = \mathbf{F}_p$ denote the "field with p elements" for a prime p (i.e., the integers mod p). Let V be an n-dimensional vector space over F, and $G = \mathrm{GL}(V)$. Note that V has size p^n (as one sees by choosing a basis). Assume $n > 0$.

(*i*) Let $Y = V - \{0\}$. Then $|Y| = p^n - 1$. Moreover, $F^\times$ acts on Y by scalar multiplication, and the orbits are precisely the non-zero parts of the lines, which consist of exactly $p - 1$ elements (the nonzero scalar multiples of a given vector). Since each orbit has size $p - 1$, there are $(p^n - 1)/(p - 1)$ orbits, i.e. $(p^n - 1)/(p - 1)$ lines in V. Now, for any hyperplane $H \subset V$, consider the subspace U of V^* given by $U = \{f \in V^* : f(H) = 0\}$. This is clearly a one dimensional space since any $f \in U$ is a map from V to V with kernel H so that we have the (noncanonical) identification $U \simeq V/H \simeq F$. But a one dimensional subspace of V^* is just a line in V^* so that hyperplanes in V correspond to lines in V^*. Since V^* has dimension n, there are $(p^n - 1)/(p - 1)$ hyperplanes in V by our considerations above.

(*ii*) Since G acts transitively on the set X of hyperplanes, for any hyperplane $x_0 \in X$, the orbit of x_0 under G is all of X. Since $|G| = |\mathrm{Orb_G(x_0)}||\mathrm{Stab_G(x_0)}|$, we find that $|G| = |X||\mathrm{Stab}_G(x_0)|$. Now we can extend any basis of x_0 to a basis for V and therefore, since any $h \in \mathrm{GL}(x_0)$ must take a basis to a basis, we can extend h to some $g \in \mathrm{GL}(V)$ with $g|_{x_0} = h$. It follows that the map $\mathrm{Stab}_G(x_0) \to \mathrm{GL}(x_0)$ is surjective, and obviously has kernel $\mathrm{Fix}_G(x_0)$. Thus we have $|\mathrm{Stab}_G(x_0)| = |\mathrm{GL}(x_0)||\mathrm{Fix}_G(x_0)|$.

(*iii*) From (*i*), we have $|X| = (p^n - 1)/(p - 1)$. Now any $f \in \mathrm{Fix_G(x_0)}$ must act as the identity on x_0. We let v_0 be any vector complementary to x_0. Then f can take v_0 to *any* vector not in x_0 since the only requirement on f is that it take a basis of V to a basis of V. Since $|x_0| = p^{n-1}$ and $|V| = p^n$, there are exactly $p^n - p^{n-1}$ choices for the image of v_0, and each such choice specifies a unique $f \in \mathrm{Fix_G(x_0)}$. Thus, $|\mathrm{Fix}_G(x_0)| = p^n - p^{n-1}$. Thus,

$$|G| = \frac{p^n - 1}{p - 1}(p^n - p^{n-1})|\mathrm{GL}(x_0)| = p^{n-1}(p^n - 1)|\mathrm{GL}(x_0)|.$$

Since for any one dimensional space W we have $|\mathrm{GL}(W)| = (p - 1)$, induction gives

$$|G| = \prod_{j=1}^{n} p^{j-1}(p^j - 1) = \prod_{j=1}^{n} p^{2j-(n+1)}(p^n - p^{n-j}) = p^{2\frac{n(n+1)}{2} - n(n+1)} \prod_{j=1}^{n}(p^n - p^{n-j}) = \prod_{j=1}^{n}(p^n - p^{n-j}).$$

(*iv*) There are $p^n - 1$ ways to specify the first column of any invertible $n \times n$ matrix with entries in $\mathbf{F}_p$ since the only requirement is that it not be the zero vector. Once this is chosen, we can specify any vector for the second column that is not in the span of the first. Since the span of the first vector is just its scalar multiples, there are $p^n - p$ choices for the second column. The third column can be any vector not in the span of the first two columns; there are $p^n - p^2$ such vectors, and so on. This gives

$$|G| = \prod_{j=1}^{n}(p^n - p^{n-j}),$$

exactly as in (*iii*).

4. Consider the action of $G = \mathrm{GL}_2(\mathbf{F}_3)$ on the set X of all 4 lines in $V = \mathbf{F}_3^2$. Let $\rho : G \to \mathrm{Aut}(X)$ be the action map for the natural left action of G on X.

(i) The four lines in V are the scalar multiples of the following four vectors:

$$\left\{ x_1 = \begin{pmatrix}1\\0\end{pmatrix},\ x_2 = \begin{pmatrix}0\\1\end{pmatrix},\ x_3 = \begin{pmatrix}1\\1\end{pmatrix},\ x_4 = \begin{pmatrix}1\\-1\end{pmatrix} \right\}.$$

We choose the ordering given above. My favorite six elements of G are

$$a = \begin{pmatrix}1 & 1\\0 & 1\end{pmatrix} \qquad b = \begin{pmatrix}0 & 1\\-1 & 0\end{pmatrix} \qquad c = \begin{pmatrix}0 & 1\\-1 & 1\end{pmatrix}$$

$$d = \begin{pmatrix}1 & 0\\1 & 1\end{pmatrix} \qquad e = \begin{pmatrix}-1 & 1\\1 & 1\end{pmatrix} \qquad f = \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}.$$

It is clear that none of these 6 elements are scalar multiples of eachother. Computing the cycle decomposition of $\rho(g)$ for the above six g is routine but tedious. We illustrate with a: One checks that over $\mathbf{F}_3$ we have

$$ax_1 = x_1 \qquad ax_2 = x_3 \qquad ax_3 = -x_4 \qquad ax_4 = -x_2,$$

from which it follows that $\rho(a) = (234)$. We summarize these calculations in the table below:

g	a	b	c	d	e	f
$\rho(g)$	(234)	$(12)(34)$	(123)	(134)	$(14)(23)$	(12)

(ii) Suppose that $\rho(g) = 1$. Then g fixes every line in V and thus, for each $v \in V$ we have $gv = \lambda_v v$ for some scalar λ_v possibly depending on v. However, let $w, v \in V$ be two linearly independent vectors (if $\dim(V) = 1$, the assertion is trivial). Then since $g \in \mathrm{GL}(V)$ we have

$$g(v + w) = \lambda_{v+w}(v + w) = gv + gw = \lambda_v v + \lambda_w w,$$

and the linear independence of v, w forces $\lambda_{v+w} = \lambda_v = \lambda_w$. It follows that $\lambda_v = \lambda$ is independent of v and $gv = \lambda v$ for all $v \in V$, i.e. g is scalar multiplication. Since $\mathbf{F}_3^\times = \pm 1$, it follows that the kernel of ρ is ± 1 so that $\rho(g) = \rho(g')$ if and only if $g = \pm g'$.

(iii) By Problem 3 (iii) or (iv) we know that $|\mathrm{GL}_2(\mathbf{F}_3)| = 48$. Since $|\mathfrak{S}_4| = 24$ and $|\ker(\rho)| = 2$, we see that ρ is surjective.

(iv) Extra credit: We choose coordinates in V and suppose that we have three (distinct) lines given by the span of the three (nonproportional) vectors

$$v_1 = \begin{pmatrix}a_1\\b_1\end{pmatrix},\ v_2 = \begin{pmatrix}a_2\\b_2\end{pmatrix},\ v_3 = \begin{pmatrix}a_3\\b_3\end{pmatrix}.$$

We claim that there is a 2×2 invertible matrix

$$\alpha = \begin{pmatrix}x & y\\z & w\end{pmatrix}$$

such that $\alpha e_1 = \lambda_1 v_1,\ \alpha e_2 = \lambda_2 v_2,\ \alpha(e_1 + e_2) = \lambda_3 v_3$ for scalars λ_i and e_i the standard basis. Indeed, it is enough to find λ_i satisfying

$$\lambda_1 a_1 + \lambda_2 a_2 = \lambda_3 a_3$$
$$\lambda_1 b_1 + \lambda_2 b_2 = \lambda_3 b_3$$

as you will check. This is clearly possible since we have two equations in three unknowns. Moreover, since the three lines we started out with are distinct, we obtain an invertible matrix. Finally, since we can take e_1, e_2, e_3 to *any* three nonproportional vectors, $\mathrm{GL}(V)$ acts triply transitively on the lines in V.

5. Let G be a group.

(i) Let n be the least positive integer such that $g^n = 1$, and suppose that $g^m = 1$ for some $m \in \mathbf{Z}$. Since $\mathbf{Z}$ is Euclidean, we may write $m = nq + r$ for some $q \in \mathbf{Z}$ and $0 \le r < n$. We then find that $1 = g^m = g^{nq+r} = (g^n)^q g^r = g^r$. If $r > 0$, this contradicts our choice of n. It follows that $r = 0$ and $n|m$. Now if $d|n$ and g has order n then g^d has order n/d. To see this, observe that $(g^d)^{(n/d)} = g^n = 1$ and if there exists $0 < r < n/d$ with $(g^d)^r = 1$ then $rd < n$, contradicting the fact that n is the order of g.

(ii) There are lots of examples. Here is one: Consider the group $\mathrm{SL}_2(\mathbf{Z})$ of 2×2 integer matrices of determinant 1. One easily checks that

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

and

$$B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$

are elements of G satisfying $A^2 = B^3 = 1$. However,

$$AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

clearly has infinite order.

(iii) Suppose that G is cyclic of order n and let g_0 be a generator of G. Since every element of G is of the form g_0^j for some j, we have, for any $g = g_0^i, h = g_0^j \in G$, $gh = g_0^i g_0^j = g_0^{i+j} = g_0^j g_0^i = hg$ so that G is abelian. Moreover, define $\phi : \mathbf{Z}/n \to G$ by $\phi(i \bmod n) = g_0^i$. Observe that this is well defined since it does not depend on the choice of representative i: indeed, if $j \equiv i \bmod n$ then for some integer m we have $j = i + mn$ so that $g_0^j = g_0^{i+mn} = g_0^i (g_0^n)^m = g_0^i$. This is obviously a homomorphism as $g_0^{i+j} = g_0^i g_0^j$. Moreover, it is injective since if $g_0^i = 1$ then by part (i) we have $n|i$, that is, $i \equiv 0 \bmod n$. Since $\mathbf{Z}/n$ and G both have size n, ϕ is an isomorphism. It follows that up to non-canonical isomorphism (observe that we had to choose a generator) there is one cyclic group of order n for each positive integer n, e.g. $\mathbf{Z}/n$.

(iv) Let G be cyclic of order n. Let $\phi_i : G \to G$ be the map $\phi_i(g) = g^i$. We have $\phi_i(gh) = (gh)^i = g^i h^i = \phi_i(g)\phi_i(h)$ since G is abelian. Since $\phi_i(1) = 1$, we see that ϕ_i is a homomorphism. Now suppose that $\phi_i(g) = 1$ for some $g \in G$. Then if d is the order of g we see that $d|i$. Thus, if $(i, n) = 1$ we must have $d = 1$ since $d|n$, whence $g = 1$. Conversely, suppose that $(i, n) = m > 1$. Part (i) shows that there is a $g_1 \in G$ of order n/m, so that $\phi_i(g_1) = 1$. Therefore, ϕ_i is injective (and hence an isomorphism by a counting argument) if and only if $i \in (\mathbf{Z}/n)^\times$. Finally, suppose that $\varphi \in \mathrm{End}_{\mathrm{group}}(G)$ and let $g_0 \in G$ be a generator. It is clear that φ is completely determined by $\varphi(g_0)$. Moreover, we must have $\varphi(g_0) = g_0^i$ for some i, whence $\varphi(g) = g^i$ for all $g \in G$. It follows that every endomorphism of G is of the form ϕ_i for some i. But we have seen that ϕ_i is an automorphism if and only if $i \in (\mathbf{Z}/n)^\times$. We thus define a map $(\mathbf{Z}/n)^\times \to \mathrm{Aut}_{\mathrm{group}}(G)$ by $i \bmod n \mapsto \phi_i$. This is bijective and well defined as we have noted, and is a homomorphism since $\phi_i \circ \phi_j(g) = g^{ji} = \phi_{ij}(g)$ for all $g \in G$. We thus have an isomorphism of groups $\mathrm{Aut}_{\mathrm{group}}(G) \simeq (\mathbf{Z}/n)^\times$. Observe that this isomorphism does not depend on any choice of generator of G.

6. Fix $n > 1$. For $\sigma \in \mathfrak{S}_n$ and a pair $\{i, j\}$ of distinct integers between 1 and n (inclusive), note that $(\sigma(i) - \sigma(j))/(i - j) = (\sigma(j) - \sigma(i))/(j - i)$, so this ratio does not depend on the ordering among i and j. Define

$$\varepsilon_n(\sigma) = \prod_{\{i,j\}} \frac{\sigma(i) - \sigma(j)}{i - j},$$

where the product is taken over unordered pairs of distinct integers between 1 and n.

(i) We have the following table:

1	(12)	(13)	(23)	(123)	(132)
1	-1	-1	-1	1	1

In general, we have

$$\begin{aligned} \varepsilon_n(\sigma)^2 &= \prod_{\{i,j\}} \frac{\sigma(i) - \sigma(j)}{i - j} \frac{\sigma(j) - \sigma(i)}{j - i} \\ &= \prod_{\substack{i,j \\ i \neq j}} \frac{\sigma(i) - \sigma(j)}{i - j} \\ &= 1, \end{aligned}$$

since any $\sigma \in \mathfrak{S}_n$ is a bijection of the set $\{1, 2, \ldots, n\}$ so that for every $i \neq j$ in $\{1, 2, \ldots, n\}$ and any $\sigma \in \mathfrak{S}_n$, there is a unique pair $k \neq l \in \{1, 2, \ldots, n\}$ with $\sigma(i) = k$ and $\sigma(j) = l$. It follows that $\varepsilon_n(\sigma) = \pm 1$.

(ii) We have

$$\begin{aligned}
\varepsilon_n(\sigma\tau) &= \prod_{\{i,j\}} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{i - j} \\
&= \prod_{\{i,j\}} \frac{\sigma(i) - \sigma(j)}{\tau^{-1}(i) - \tau^{-1}(j)} \\
&= \prod_{\{i,j\}} \frac{\sigma(i) - \sigma(j)}{i - j} \frac{i - j}{\tau^{-1}(i) - \tau^{-1}(j)} \\
&= \prod_{\{i,j\}} \frac{\sigma(i) - \sigma(j)}{i - j} \prod_{\{l,k\}} \frac{l - k}{\tau^{-1}(l) - \tau^{-1}(k)} \\
&= \prod_{\{i,j\}} \frac{\sigma(i) - \sigma(j)}{i - j} \prod_{\{l,k\}} \frac{\tau(l) - \tau(k)}{l - k} \\
&= \varepsilon_n(\sigma)\varepsilon_n(\tau),
\end{aligned}$$

since, again, any $\sigma \in \mathfrak{S}_n$ is a bijection of the set $\{1, 2, \ldots, n\}$. Clearly $1, (12) = \sigma \in \mathfrak{S}_n$ for all $n > 1$ and $\varepsilon_n(1) = 1$ while

$$\begin{aligned}
\varepsilon_n(\sigma) &= \frac{\sigma(1) - \sigma(2)}{1 - 2} \prod_{\substack{\{i,j\} \\ i,j \notin \{1,2\}}} \frac{\sigma(i) - \sigma(j)}{i - j} \prod_{j \neq 1,2} \frac{\sigma(1) - \sigma(j)}{1 - j} \frac{\sigma(2) - \sigma(j)}{2 - j} \\
&= \frac{2 - 1}{1 - 2} \prod_{j \neq 1,2} \frac{2 - j}{1 - j} \frac{1 - j}{2 - j} \\
&= -1,
\end{aligned}$$

since $\sigma = (12)$ fixes every $j \neq 1, 2$. Hence, $\varepsilon_n : \mathfrak{S}_n \to \{\pm 1\}$ is a surjective group homomorphism.

7. Let A be an abelian group, $a, a' \in A$ elements with respective finite orders n and n'.

(i) Set $n_i = n/p_i^{e_i}$ and let $a_i = a_i^n$. Then certainly $a_i^{p_i^{e_i}} = 1$. Let a_i have order r_i. Then problem 5 (i) shows that we must have $r_i | p_i^{e_i}$ so that $r_i = p_i^{b_i}$ for some $b_i \leq e_i$. But then $a^{n_i p_i^{b_i}} = 1$ so that $n | n_i p_i^{b_i}$. Since the p_i are distinct, it follows that $(p_i^{e_i}, n_i) = 1$ so that $p_i^{e_i} | p_i^{b_i}$ whence $e_i \leq b_i$. Hence, $b_i = e_i$ and a_i has order $p_i^{e_i}$. An identical argument works for a' and n'.

(ii) Suppose that aa' has order r. Then $1 = (aa')^{rn} = a'^{rn}$ (since A is abelian) so that $n' | rn$. Since $(n, n') = 1$ we must have $n' | r$. Similarly, $n | r$. Again, since $(n, n') = 1$ this implies that $nn' | r$. But $(aa')^{nn'} = 1$, so that aa' has order nn'. Now suppose that $(n, n') = d$. Write $n = \prod p_i^{u_i}$ and $n' = \prod p_i^{v_i}$ where the set of primes in both products is the same but u_i, v_i are possibly 0. By part (i), there exists x_i of order $p_i^{\max\{u_i, v_i\}}$ for each i. Since the p_i are distinct, if follows from the above and induction that $\prod x_i$ has order $\prod p_i^{\max\{u_i, v_i\}} = \mathrm{lcm}(n, n')$.

(iii) Let F be a commutative field and let $x \in F$ have maximal order m. If $y \in F$ has order n then $n | m$. Otherwise, by part (ii) there exists an element of order $\mathrm{lcm}(m, n) > m$, contradicting the maximality of m. It follows that every $y \in F^\times$ is a root of $X^m - 1 = 0$. Since this has at most m roots, we must have $|F^\times| \leq m$. On the other hand, $x \in F^\times$ and by the choice of m, $\{1, x, x^2, \ldots, x^{m-1}\}$ are all distinct. It follows that $|F^\times| = m$ and hence an element of maximal order is a generator for $F^\times$ and $F^\times$ is cyclic. The generators for $\mathbf{F}_{17}^\times$ and $\mathbf{F}_{31}^\times$ are listed in the following table:

$\mathbf{F}_{17}^\times$	3	10	5	11	14	7	12	6
$\mathbf{F}_{31}^\times$	3	17	13	24	22	12	11	21