

Solutions to Test 1

Let p be a prime number, and \mathbb{F}_p the field of congruence classes modulo p . In problems 1–5, the group $G = GL_2(\mathbb{F}_p)$ is the group of all invertible 2×2 matrices with coefficients in \mathbb{F}_p .

Remark: In the solutions, we will use that the Abelian group $V = \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$ can be regarded as a 2-dimensional vector space over the field \mathbb{F}_p .

1. Prove that G is isomorphic to the automorphism group of the group $\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$. Find the order of G .

Solution: Let $v_1 = (1, 0)$, $v_2 = (0, 1)$ be two generators of $\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$. Then an automorphism π of $\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$ is uniquely defined by the images of g_1 and g_2 . Let $\pi(g_1) = a(\pi)g_1 + c(\pi)g_2$ and $\pi(g_2) = b(\pi)g_1 + d(\pi)g_2$, where $a(\pi)$, $b(\pi)$, $c(\pi)$ and $d(\pi)$ are integers. Since, $pv_1 = pv_2 = 0$, the automorphism π depends only on the congruence classes of $a(\pi)$, $b(\pi)$, $c(\pi)$ and $d(\pi)$ modulo p . Note that since the kernel of π is trivial, we have that $\pi(g_1)$ is not a multiple of $\pi(g_2)$, or equivalently, $a(\pi)d(\pi) - b(\pi)c(\pi) \not\equiv 0 \pmod{p}$. Hence, to any automorphism π we can assign an invertible over \mathbb{F}_p matrix with coefficients $a(\pi)$, $b(\pi)$, $c(\pi)$ and $d(\pi)$ modulo p . On the other hand, any invertible matrix over \mathbb{F}_p gives rise to an automorphism.

It is easy to check that the composition of automorphisms corresponds to the product of matrices.

To find $|G|$ note that there are $p^2 - 1$ ways to choose $\pi(g_1)$, since there are $p^2 - 1$ nonzero pairs (a, c) modulo p . Then there are only $p^2 - p$ ways to choose (b, d) , since we must reject all multiples of (a, c) , i.e. $(0, 0)$, (a, c) , \dots , $((p-1)a, (p-1)c)$. Hence, $|G| = (p^2 - 1)(p^2 - p)$.

Another method to find $|G|$ is to count all solutions of the equation $ad - bc \equiv 0 \pmod{p}$ and subtract this number from p^4 , which is the number of all possible quadruples (a, b, c, d) modulo p . If $a \neq 0$, then $d = bc/a$ is uniquely defined by a , b and c , which gives $p^2(p-1)$ solutions (b and c are any but $a \neq 0$). If $a = 0$, then either b or c is also zero, which leaves us with $2p^2 - p$ solutions.

2. Find the center of G . Find a normal non-abelian subgroup of G different from G .

Solution: We use the representation of G as $\text{Aut}(\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z})$. Denote the center of G by $Z(G)$. We prove that if $g \in Z(G)$, then $g(v)$ is proportional to v for any $v \in \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$. Indeed, if $g(v) = u$, and u and v are not proportional, then one can define an automorphism h such that $h(u) = v$ and $h(g(u)) = u + v$. Then $gh(u) = u \neq u + v = hg(u)$. Hence, $g(v)$ is always proportional to v . It is easy to show that the coefficient of proportionality must be the

same for all $v \in \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$. Thus $Z(G)$ consists of all scalar matrices (i.e. matrices of the form aI , where $a \in \mathbb{F}_p^*$ and I is the identity matrix).

A non-abelian normal subgroup of G is $SL_2(\mathbb{F}_p)$. This is the kernel of the homomorphism $\det : G \rightarrow \mathbb{F}_p^*$, which assigns to each matrix its determinant.

3. Let p be an odd prime. Prove that every element of order 2 in G is conjugate to a diagonal matrix with ± 1 's on the diagonal. How many elements of order 2 does G have?

Solution: Again we use the representation of G as $\text{Aut}(\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z})$. Let g be an element of order 2, and $v \in \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$ be a nonzero element. Clearly, if $g(v) = u$, then $g(u) = v$. We get that $g(u+v) = u+v$ and $g(u-v) = -(u-v)$. If u and v are not proportional, then so are $u+v$ and $u-v$. Here we use that $p \neq 2$. (otherwise, $-v = +v \pmod{2}$ and $u+v = u-v$). The matrix of g in the basis $\{u+v, u-v\}$ is the diagonal matrix with $+1$ and -1 on the diagonal, and it is conjugate to the matrix of g in the basis $(1, 0), (0, 1)$. It is easy to check that the centralizer of such a diagonal matrix consists of all diagonal matrices, so the centralizer has order $(p-1)^2$. If $g(v)$ and v are proportional for any v , then $g = -I \in Z(G)$. Hence, the total number of order 2 elements is $|G|/(p-1)^2 + 1 = p^2 + p + 1$.

4. Find a Sylow p -subgroup of G . How many of them does G have?

Solution: A Sylow p -subgroup of G has p elements. To find such a group it is enough to find an element $g \in G$ of order p . Try simple matrices. If g is diagonal, then $g^p = g$ by Fermat's theorem. Does not work. Try the matrix

$$g = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Since $g = I+N$, where N is nilpotent matrix ($N^2 = 0$), we have that $g^p = (I+N)^p = I+pN \equiv I \pmod{p}$. Hence, a Sylow subgroup consists of matrices

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix},$$

where $a = 0, \dots, p-1$. Note that the centralizer of this group has order divisible by $p(p-1)$. Indeed, the centralizer contains the group itself and the center of G . Hence, the number n_p of all Sylow p -subgroups divides $|G|/p(p-1) = p^2 - 1$. By Sylow's theorems $n_p \equiv 1 \pmod{p}$, so $n_p = 1$ or $n_p = p+1$. Note that

$$\left\{ \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}, a = 0, 1, \dots, p-1 \right\}$$

is also a Sylow subgroup so $n_p > 1$. Hence, $n_p = p+1$.

5. Prove that for $p = 2$ the group G is isomorphic to S_3 . Prove also that for $p = 3$ the quotient group $G/Z(G)$ (here $Z(G)$ is the center of G) is isomorphic to S_4 .

Solution: If $p = 2$, then $|G| = 6$. Since $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ has 3 nonzero elements, every nontrivial element $g \in G$ defines a nontrivial permutation of these 3 elements. This gives an injective homomorphism from G to S_3 . Since the orders of both groups are the same, this is an isomorphism.

Note that for any p the quotient group $G/Z(G)$ acts on the classes of proportional elements (=lines) in $\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$. Indeed, the left coset $gZ(G)$ sends the class $\{v, 2v, \dots, (p-1)v\}$ to the class $\{g(v), 2g(v), \dots, (p-1)g(v)\}$. This does not depend on the choice of the representative g , since $Z(G) = \{aI, a = 1, \dots, p-1\}$ maps each class to itself. In total, there are $(p^2-1)/(p-1) = p+1$ such classes. They form the projective line over \mathbb{F}_p ($=\mathbb{F}_p \sqcup \{\infty\}$).

If $p = 3$, then $|G/Z(G)| = 24$. There are 4 lines in $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$. Hence, there is an injective homomorphism from $G/Z(G)$ to S_4 , which must be an isomorphism.

Another approach to both problems would be to consider the action of G on its Sylow p -subgroups by conjugations. There are 3 of them in the first case, and 4 in the second. Then it is not hard to show that the kernel of this action is the center of G and nothing else.