UNIVERSIDAD DE COSTA RICA | ESCUELA DE MATEMATICA

Tópicos en la teoría de grupos | Examen Parcial 2

I Semestre 2014 | Nick Gill

Instructions: You may use any of the results covered in the lecture notes, including in exercises. Make sure that you state clearly the results that you use.

If a question asks you to prove a result from lectures, then you should sketch it as fully as possible, explicitly stating all other results that you use.

(1) Let V be a vector space of dimension n over a field k. Recall that $\mathrm{PG}_{n-1}(k)$ is the incidence structure $(V_1, \dots, V_{n-1}, I)$ where, for $i = 1, \dots, n-1$, V_i is the set of subspaces of V of dimension i and

$$I := \{(v_1, \dots, v_{n-1}) \in V_1 \times \cdots \times V_{n-1} \mid v_1 < v_2 < \cdots < v_{n-1}\}.$$

Prove the following facts:

(a) Any two elements of V_1 are incident with a unique element of V_2;

(b) Any element of V_2 is incident with at least three elements of V_1;

(c) Let P_1, P_2, P_3 be distinct elements of V_1 and let L_1, L_2, L_3 be distinct elements of V_2. Suppose that

- $P_1, P_2 < L_3$; $P_1, P_3 < L_2$ and $P_2, P_3 < L_1$.
- L_4 is an element of V_2 that does not contain P_1, P_2 or P_3 but does intersect L_1 and L_2 non-trivially.

Prove that L_4 intersects L_3 non-trivially;

(d) Prove that if $n = 3$, then any two distinct elements of V_2 are incident with a unique element of V_1;

(e) Prove that if $n > 3$, then there exist two elements of V_2 that are not both incident with the same element of V_1.

Answer.

(a) Let P_1, P_2 be two elements of V_1. Clearly the only element of V_2 that contains them both is the element $\langle P_1, P_2\rangle$.

(b) Let $L \in V_2$ be spanned by two vectors u and v. Then L is incident with the elements $\langle u\rangle$, $\langle v\rangle$ and $\langle u+v\rangle$, all of which are distinct.

(c) Let $P_i = \langle x_i\rangle$. The triangle condition implies that, for each i, $L_i = \langle x_j, x_k\rangle$ where $i \neq j \neq k \neq i$. Now, by assumption, L_4 contains vectors $x_2 + \lambda x_3$ and $x_1 + \mu x_3$ for some λ, μ in the field k. Then L_4 contains the vector

$$-\frac{\mu}{\lambda}(x_2 + \lambda x_3) + (x_1 + \mu x_3) = x_1 - -\frac{\mu}{\lambda}x_2$$

which is a non-trivial vector in L_3. The result follows.

(d) Suppose that $n = 3$ and let L_1, L_2 be distinct elements of V_2. If L_1 and L_2 intersected trivially, then one would have four linearly independent vectors, a contradiction. Thus L_1 and L_2 intersect non-trivially. Since L_1 and L_2 are distinct, their intersection is of dimension 1 - this intersection is the unique element of V_1 that is incident with both.

(e) Suppose that $n < 3$ and let L_1 be any element of V_2. Let X be any complement of L_1 in V and let L_2 be a 2-dimensional subspace of X. Then L_1 and L_2 intersect trivially, and so are not both incident with the same element of V_1.

(2) Let $G = \mathrm{GL}_2(3)$, the set of 2 by 2 invertible matrices over a field with 3 elements.

(a) Calculate the order of G;

(b) Prove that $\mathrm{SL}_2(3)$ contains the derived group of G;
(c) Prove that G is solvable (or soluble);
(d) Recall that a finite nilpotent group is the direct product of p-groups. Prove that G is not nilpotent.

Answer.
(a) $|\mathrm{GL}_2(3)| = (3^2-1)(3^2-3) = 48.$
(b) $\mathrm{SL}_2(3)$ is a normal subgroup of $\mathrm{GL}_2(3)$ of index 2. Hence the quotient $\mathrm{GL}_2(3)/\mathrm{SL}_2(3)$ is abelian and the result follows.
(c) We will show that there is a chain of subgroups

$$G \rhd K_1 \rhd K_2 \rhd K_3 \rhd \{1\}$$

such that each successive quotient is abelian. We take $K_1 = \mathrm{SL}_2(3)$ - it is of index 2, so is normal with abelian quotient.
Now $\mathrm{SL}_2(3)$ has a centre K_3 of order 2, thus the quotient K_1/K_3 is isomorphic to $\mathrm{PSL}_2(3)$ a group of order 12. Now $\mathrm{PSL}_2(3)$ has either 1 or 4 Sylow 3-subgroups and one can easily confirm that it has more than (1) (see the answer for part (3) below). Thus $\mathrm{PSL}_2(3)$ contains 8 elements of order 3. The remaining 4 elements must lie in a unique Sylow 2-subgroup, thus we take K_2 to be the this Sylow 2-subgroup (lifted to $\mathrm{SL}_2(3)$). It has index 3 in $\mathrm{PSL}_2(3)$ so is abelian, and K_3 has index 4 in K_2 so K_3/K_2 is abelian also, and the result follows.
An alternative answer: Simply observe that the smallest non-abelian simple group is $\mathrm{Alt}(5)$ of order 60. Since $|\mathrm{GL}_2(3)| < 60$, composition factors of $\mathrm{GL}_2(3)$ must be abelian and so $\mathrm{GL}_2(3)$ is solvable.
(d) If G is nilpotent, then, for any prime t dividing $|G|$, G has a unique Sylow t-subgroup. But letting $t=3$, we see that a Sylow t-subgroup of $\mathrm{GL}_2(3)$ has order 3 and there are more than one of these: for instance, the set of all strictly upper triangular matrices is one, and the set of all strictly lower triangular matrices is another.

(3) Let k be a field of characteristic 2. Let V be a vector space of dimension $n < \infty$ over k and let $\beta : V \times V \to k$ be a symmetric bilinear form. Define

$$U := \{x \in V \mid \beta(x,x) = 0\}.$$

(a) Prove that U is a vector subspace of V;
(b) Prove that, if k is finite and W is a 2-dimensional subspace of V, then $U \cap W$ is non-trivial;
(c) Prove that, if k is finite, then $\dim(U) \geq n-1$.

Answer.
(a) Let $x, y \in V$ satisfy $\beta(x,x) = 0$ and let $\lambda, \mu \in k$. Then

$$\begin{aligned} \beta(\lambda x + \mu y, \lambda x + \mu y) &= \lambda^2 \beta(x,x) + \lambda\mu\beta(x,y) + \mu\lambda\beta(y,x) + \lambda^2\beta(y,y) \\ &= \lambda\mu\beta(x,y) + \mu\lambda\beta(y,x) = 0 \end{aligned}$$

where the last equality follows from the fact that β is symmetric and k has characteristic 2. It follows immediately that U is a vector subspace of V.
(b) Let $W = \langle u, v\rangle$. If u and v are isotropic, then the result follows immediately. Suppose that this is not the case and observe that, for $\lambda \in k$,

$$\beta(u + \lambda v, u + \lambda v) = \beta(u,u) + \lambda^2 \beta(v,v).$$

Now, since k is finite, $\lambda \mapsto \lambda^2$ is an automorphism and so is surjective. In particular, there is a value of λ such that $\lambda^2 = \frac{-\beta(u,u)}{\beta(v,v)}$. For this value of λ, $u + \lambda v$ is isotropic, and the result follows.

(c) Suppows that $\dim(U) \leq n-2$, and let W be any complement of U in V. Then $W \cap U = \{1\}$ which is a contradiction of (2). The result follows.

(4) Let V be a vector space of dimension n over $\mathbb{F}_q$. Let W be a vector subspace of V of dimension m.
   (a) Assume that $m = 1$ and describe the stabilizer of W in the group $\mathrm{GL}_n(q)$.
   (b) Do the same without the assumption that $m = 1$.

When I say 'describe' here, I want you to emulate what I did in lectures: First, take an appropriate basis for V and describe those invertible matrices that lie in the stabilizer of W. Second describe the 'isomorphism class' of the stabilizer of W by identifying an important normal subgroup, and giving the structure of the corresponding quotient.

Answer. I give the answer for (2) only as (1) is a special case. Let $\{e_1, \dots, e_m\}$ be a basis for W and extend to a basis $\{e_1, \dots, e_n\}$ of V. One can check that (writing elements with respect to this basis) the stabilizer of W in $\mathrm{GL}_n(q)$ is precisely the group

$$G_W := \left\{ \left(\begin{array}{c|c} A_1 & 0 \\ \hline A_2 & A_3 \end{array} \right) \middle| A_1 \in \mathrm{GL}_m(q), A_2 \in M_{(n-m)\times m}(q), A_3 \in \mathrm{GL}_{n-m}(q) \right\}.$$

Define

$$U_W := \left\{ \left(\begin{array}{c|c} I & 0 \\ \hline A_2 & I \end{array} \right) \middle| A_2 \in M_{(n-m)\times m}(q) \right\}$$

and observe that U_W is an elementary abelian normal subgroup of G_W of order $q^{m(n-m)}$. Define, in addition,

$$L_W := \left\{ \left(\begin{array}{c|c} A_1 & 0 \\ \hline 0 & A_3 \end{array} \right) \middle| A_1 \in \mathrm{GL}_m(q), A_3 \in \mathrm{GL}_{n-m}(q) \right\}$$

and observe that L_W is a subgroup of G_W isomorphic to $\mathrm{GL}_m(q) \times \mathrm{GL}_{n-m}(q)$. Since $G_W = U_W \cdot L_W$ and $U_W \cap L_W = \{1\}$ we conclude that

$$G = U_W \rtimes L_w \cong U_W \rtimes (\mathrm{GL}_m(q) \times \mathrm{GL}_{n-m}(q)),$$

where U_W is elementary abelian of order $q^{m(n-m)}$.

(5) Do **ONE** of the following:
   (a) Sketch a proof of Witt's Lemma.
   (b) Sketch a proof of the fact that $\mathrm{PSL}_n(q)$ is simple for $n \geq 2$ unless $(n,q) \in \{(2,3)(3,3)\}$.

Answer. This question is book-work, so an answer will not be included here.

(6) Let V be a 2-dimensional vector space over a field $\mathbb{F}_q$. Fix a basis for V and define

$$Q_1 : V \to \mathbb{F}_q, \mathbf{x} \mapsto x_1 x_2$$

where $\mathbf{x} = (x_1, x_2)$.

(a) Show that Q_1 is a quadratic form, and write the polar form of Q_1.
(b) Show that (V, Q_1) is a hyperbolic line.
(c) Show that $\mathrm{Isom}(Q_1)$ is a dihedral group of order $2(q-1)$.

Define

$$Q_2 : V \to \mathbb{F}_q,\ \mathbf{x} \mapsto x_1^2 + x_1x_2 + \zeta x_2^2$$

where $\mathbf{x} = (x_1, x_2)$ and $f(t) = t^2 + t + \zeta$ is an irreducible polynomial over $\mathbb{F}_q$.

(d) Show that Q_2 is a quadratic form, and write the polar form of Q_2.
(e) Show that (V, Q_2) is an anisotropic orthogonal space.
(f) Define matrices,

$$A = \begin{pmatrix} -1 & 0 \\ -1 & 1 \end{pmatrix} \text{ and } B = \begin{pmatrix} 1 & -\frac{1}{\zeta} \\ 0 & -1 \end{pmatrix},$$

and show that the maps $\mathbf{x} \mapsto \mathbf{x} \cdot A$ and $\mathbf{x} \mapsto \mathbf{x} \cdot B$ are isometries of (V, Q_2). Conclude that $\mathrm{Isom}(Q_2)$ is non-abelian.

Answer.

(a) Q_1 is a homogeneous quadratic polynomial so is a quadratic form. Alternatively observe that, for any $c \in \mathbb{F}_q$,

$$Q(c\mathbf{x}) = cx_1cx_2 = c^2x_1x_2 = c^2Q(\mathbf{x}).$$

To complete the proof that Q_1 is a quadratic form, we observe that the polar form of Q_1 is

$$\begin{aligned} \beta_1(\mathbf{x}, \mathbf{y}) &= Q_1(\mathbf{x} + \mathbf{y}) - Q_1(\mathbf{x}) - Q_1(\mathbf{y}) \\ &= (x_1 + y_1)(x_2 + y_2) - x_1x_2 - y_1y_2 \\ &= x_1y_2 + x_2y_1 \\ &= \mathbf{x}^T \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \mathbf{y} \end{aligned}$$

(b) Let $\mathbf{u} = (1, 0)$ and $\mathbf{v} = (0, 1)$ and observe that $(\mathbf{u}, \mathbf{v})$ is a hyperbolic pair.

(c) Let $g \in \mathrm{GL}_2(q)$ and write g as a matrix with respect to the given basis:

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Now g is an isometry if and only if, for all $\mathbf{x} \in V$, $Q_1(\mathbf{x}g) = Q_1(\mathbf{x})$. Now observe that

$$\mathbf{x}g = \begin{pmatrix} ax_1 + cx_2 \\ bx_1 + cx_2 \end{pmatrix}$$

Thus g is an isometry if and only if, for all $x_1, x_2 \in V$,

$$(ax_1 + cx_2)(bx_1 + dx_2) = x_1x_2.$$

If $x_1 = 0$, then we obtain immediately that $c = 0$ or $d = 0$. If $x_2 = 0$, then we obtain immediately that $a = 0$ or $b = 0$. In order that g is invertible we have, then, two cases:

(i) Suppose $a = d = 0$. Then $Q_1(\mathbf{x}g) = bcx_1x_2$ and g is an isometry if and only if $c = b^{-1}$.
(ii) Suppose $b = c = 0$. Then $Q_1(\mathbf{x}g) = adx_1x_2$ and g is an isometry if and only if $a = d^{-1}$.

We conclude immediately that $\mathrm{Isom}(Q_1)$ is a group of order $2(q-1)$. The set of matrices from (a) clearly form a cyclic group of order $q-1$, while the set of matrices in (b) all have order 2, thus the group is dihedral.

(d) Again Q_2 is a homogeneous quadratic polynomial so is a quadratic form. The polar form of Q_2 is

$$\begin{aligned}\beta_1(\mathbf{x},\mathbf{y}) =& Q_1(\mathbf{x}+\mathbf{y}) - Q_1(\mathbf{x}) - Q_1(\mathbf{y})\\ =&(x_1+y_1)^2 + (x_1+y_1)(x_2+y_2) + \zeta(x_2+y_2)^2 - x_1^2\\ &- x_1x_2 - \zeta x_2^2 - y_1^2 - y_1y_2 - \zeta y_2^2\\ =&2x_1y_1 + x_1y_2 + x_2y_1 + 2\zeta x_2y_2\\ =&\mathbf{x}^T\begin{pmatrix}2 & 1\\ 1 & 2\zeta\end{pmatrix}\mathbf{y}\end{aligned}$$

(e) Suppose that $\mathbf{x} = (x_1, x_2) \in V$ is isotropic, i.e.

$$x_1^2 + x_1x_2 + \zeta x_2^2 = 0 \tag{1}$$

If $x_2 \neq 0$, then, dividing both sides by x_2^2, we obtain that

$$(\frac{x_1}{x_2})^2 + \frac{x_1}{x_2} + \zeta = 0$$

and $\frac{x_1}{x_2}$ is a root of the polynomial $f(t) = t^2 + 2 + \zeta$ in $\mathbb{F}_q$. But $f(t)$ is irreducible and we have a contradiction.
If, on the other hand, $x_2 = 0$, then (1) implies that $x_1 = 0$ and the result follows.

(f) Observe that $\mathbf{x}\cdot A = (-y_1 - y_2, y_2)$, and therefore,

$$\begin{aligned}Q_2(\mathbf{x}\cdot A) &= (-y_1-y_2)^2 + (-y_1-y_2)y_2 + \zeta y_2^2\\ &= y_1^2 + y_1y_2 + \zeta y_2^2 = Q_2(\mathbf{x})\end{aligned}$$

as required.
Similarly, observe that $\mathbf{x}\cdot B = (y_1, -y_2 - \frac{1}{\zeta}y_1)$, and therefore,

$$\begin{aligned}Q_2(\mathbf{x}\cdot B) &= y_1^2 + y_1(-y_2 - \frac{1}{\zeta}y_1) + \zeta(-y_2 - \frac{1}{\zeta}y_1)^2\\ &= y_1^2 + y_1y_2 + \zeta y_2^2 = Q_2(\mathbf{x})\end{aligned}$$

as required.
Finally observe that

$$AB = \begin{pmatrix}-1 & \frac{1}{\zeta}\\ -1 & \frac{1}{\zeta}-1\end{pmatrix} \text{ and } BA = \begin{pmatrix}\frac{1}{\zeta}+1 & -\frac{1}{\zeta}\\ 1 & -1\end{pmatrix},$$

Since these two matrices do not commute and both lie in $\mathrm{Isom}(Q_2)$, we conclude that $\mathrm{Isom}(Q_2)$ is non-abelian.

(7) Let V be a vector space of dimension n over $\mathbb{F}_q$ equipped with a non-degenerate alternating bilinear form β. Let $G = \mathrm{Sp}_n(q)$ be the isometry group of β. Let W be a vector subspace of V of dimension m and let G_W be the stabilizer of W in G.
  (a) Assume that $m = 1$ and describe G_W;
  (b) Assume that W is non-degenerate and describe G_W;
  (c) Show that if G_W is maximal in G, then $G_W = G_U$ where U is either a non-degenerate or a totally isotropic subspace of V.

When I say 'describe' here, I want you to emulate what I did in lectures: First, take an appropriate basis for V and describe those elements of $\mathrm{Sp}_n(q)$ that lie in the stabilizer of W.

Second describe the 'isomorphism class' of the stabilizer of W by identifying an important normal subgroup, and giving the structure of the corresponding quotient.

Answer.

(a) Take an (ordered) basis for V to be $\{v_1, \ldots, v_r, w_r, \ldots, w_1\}$. Since $\mathrm{Sp}_{2r}(k)$ acts transitively on the set of points of its polar space, we can take $\omega = \langle w_1 \rangle$.

One can check that $G_{\langle w_1 \rangle}$ contains the following two subgroups:

(2)
$$H := \left\{ g := \left(\begin{array}{c|ccc|c} a & 0 & \cdots & 0 & 0 \\ \hline 0 & & & & 0 \\ \vdots & & A & & \vdots \\ 0 & & & & 0 \\ \hline 0 & 0 & \cdots & 0 & a^{-1} \end{array} \right) \middle| \, a \in \mathbb{F}_q^*, A \in \mathrm{Sp}_{2r-2}(k) \right\};$$
$$Q := \left\{ g := \left(\begin{array}{c|ccc|c} 1 & a_1 & \cdots & a_{2r-2} & a_{2r-1} \\ \hline 0 & & & & b_{2r-2} \\ \vdots & & I & & \vdots \\ 0 & & & & b_1 \\ \hline 0 & 0 & \cdots & 0 & 1 \end{array} \right) \middle| \begin{array}{l} a_1, \ldots, a_{2r-1}, b_1, \ldots, b_{2r-2} \in k, \\ b_i = \begin{cases} -a_i, & \text{if } i \leq r-1; \\ a_i, & \text{otherwise}; \end{cases} \end{array} \right\}.$$

The following facts are virtually self-evident:

(i) $Q \cap H = \{1\}$;
(ii) $|G_{\langle w_1 \rangle}| = |Q| \cdot |H|$ (using the orbit stabilizer theorem and the fact that G is transitive on 1-dimensional subspaces of V);
(iii) Q is isomorphic to the additive group $(k^{2r-1}, +)$;
(iv) The map $H \to Sp_{2r-2}(k) \times \mathrm{GL}_1(q), g \mapsto (A, a)$ is an isomorphism.

The first two items imply that $G_{\langle w_1 \rangle} = Q \cdot H$. One can easily check that H normalizes Q, and thus Q is normal in $G_{\langle w_1 \rangle}$ and we conclude that $G_{\langle w_1 \rangle} = Q \rtimes H$. Now the last two items imply that

$$G_\omega \cong Q \rtimes (\mathrm{Sp}_{2r-2}(k) \times GL_1(k))$$

where Q is an abelian group isomorphic to the additive group $(k^{2r-1}, +)$.

(b) Observe that if W is non-degenerate, then $V = W \oplus W^\perp$ and both W and $W^\perp$ are non-degenerate. If $v \in V$, then $v = w_1 + w_2$ for some $w_1 \in W, w_2 \in W^\perp$ and $\beta(v) = \beta(w_1) + \beta(w_2)$. Thus if g preserves $\beta(w_1)$, then it preserves $\beta(w_2)$, i.e. G_W stabilizes W and $W^\perp$. We conclude that, if $\dim(W) = 2s$, then $G_W \cong \mathrm{Sp}_{2s}(q) \times \mathrm{Sp}_{2(r-s)}(q)$.

(c) Suppose that W is a vector subspace of V that is neither non-degenerate, nor totally isotropic. Then W is a degenerate symplectic subspace of V and so $\mathrm{Rad}(W)$ is a proper non-trivial subspace of W. By definition $\mathrm{Rad}(W)$ is totally isotropic and, clearly, if $W^g = W$ for some $g \in G$, then $\mathrm{Rad}(W)^g = \mathrm{Rad}(W)$. Thus the stabilizer of W is a subgroup of the stabilizer of $\mathrm{Rad}(W)$ and we are done.