Algebra Notes

Math 122 — Harvard University — Fall 2002

C. McMullen

December 6, 2002

1 Vector spaces and eigenvalues

The field $\mathbb{F}_p$. Here is a proof that inverses exist in $\mathbb{F}_p$. Given $a \neq 0$ in $\mathbb{F}_p$, define $\phi : \mathbb{F}_p \to \mathbb{F}_p$ by $\phi(x) = ax$. By the distributive law, ϕ is a homomorphism of $(\mathbb{F}_p, +)$ to itself. Also $\phi(1) = a \neq 0$. Thus $\operatorname{Ker} \phi$ is not the whole group $\mathbb{F}_p$. Since p is prime, the only other possibility is $\operatorname{Ker} \phi = (0)$. Thus ϕ is injective, and hence surjective. Therefore there exists a b such that $\phi(b) = ab = 1$. This shows a has an inverse in $\mathbb{F}_p$. ∎

Existence of a basis. Let $\mathcal{B}$ be a nonempty collection of subsets of V, such that whenever (B_α) is a nested collection with each $B_\alpha \in \mathcal{B}$, then $\bigcup B_\alpha$ is also in $\mathcal{B}$. Then the *Hausdorff maximal principle* asserts that $\mathcal{B}$ contains a maximal element M: meaning $M \in \mathcal{B}$ and if $M \subset B \in \mathcal{B}$ then $M = B$. This principle is equivalent to the Axiom of Choice.

Theorem 1.1 *Every vector space V has a basis.*

Proof. Let $\mathcal{B}$ be the collection of all linearly independent sets $B \subset V$. The empty set is linearly independent, so $\mathcal{B} \neq \emptyset$. Also the union of nested sets in $\mathcal{B}$ is still in $\mathcal{B}$: indeed, if vectors $v_1, \ldots, v_n$ lie in $\bigcup B_\alpha$, then all lie in some particular B_α, and hence they are linearly independent. By the Hausdorff maximal principle there exists a maximal linearly independent set M. Then $\operatorname{Span}(M) = V$ — else M is not maximal — and therefore M forms a basis. ∎

Eigenvalues of $A \in \mathbf{O}_n(\mathbb{R})$. Let $p(t) \in \mathbb{C}[t]$ be a polynomial of degree n, with $p(0) \neq 0$. Then $q(t) = t^n p(1/t)$ is another polynomial of degree n, whose roots whose roots are the reciprocals of the roots of $p(t)$.

Now suppose $p(t) = \det(tI - A)$ is the characteristic polynomial of a matrix $A \in \mathrm{SO}_n(\mathbb{R})$. Then $AA^t = I$, so we have:

$$\begin{aligned} t^n p(1/t) &= \det(tI)\det(t^{-1}AA^t - A) = \det(A)\det(A^t - tI) \\ &= (-1)^n \det(tI - A^t) = (-1)^n p(t). \end{aligned}$$

Thus the roots of $p(t)$, together with their multiplicities, are invariant under $r \mapsto 1/r$.

As a corollary, if n is odd then ± 1 must be a root of $p(t)$ (with odd multiplicity). In particular, this shows every element of $\mathrm{SO}_3(\mathbb{R})$ has an axis.

2 Wallpaper groups

There are 17 'types' of discrete, crystallographic subgroups Γ of the group G of rigid motions of $\mathbb{R}^2$. (Two subgroups are of the same *type* if they are conjugate by a map of the form $Ax + b$, $A \in \mathrm{GL}_2(\mathbb{R})$.)

For example, consider the case where Γ contains an element of order 4. Then the associated lattice L_Γ is a square lattice, which we can assume to be generated by $a = (1, 0)$ and $b = (0, 1)$. We can also normalize so that $\rho = \rho_{\pi/2}$ belongs to Γ.

In this case there are three possible types:

1. Γ preserves orientation; then it is generated by (t_a, ρ).
2. There is a point whose stabilizer Γ_p is the dihedral group D_4. Then Γ is generated by (t_a, ρ, r), where r is reflection in the x-axis.
3. The group Γ contains glide reflections but no simple reflections. Then Γ is generated by (t_a, ρ, r'), where r' is a glide reflection stabilizing the line $L = \mathbb{R} \times \{1/2\}$ and translating it by $1/2$.

Proof. First suppose Γ preserves orientation. Then any g in Γ has the form $t_c\rho^n$ for some c and n. But then $t_c \in \Gamma$ and therefore $c \in L_\Gamma$. This shows Γ is generated by (t_a, ρ).

Next suppose Γ contains an orientation-reversing element g. We may assume $Dg = r$. By the above argument, its orientation-preserving subgroup Γ_0 is generated by (t_a, ρ).

Label each point in the plane by the size of its stabilizer in Γ_0. The result is that for any $x, y \in \mathbb{Z}$, the point $(x/2, y/2)$ is labelled 4 when $x + y$ is even and 2 when $x + y$ is odd. All other points are labelled one.

This pattern must be preserved by g, since $g\Gamma_0 g^{-1} = \Gamma_0$. As a result, g is a glide (or simple) reflection through a line of the form $\mathbb{R} \times \{y\}$, where $2y \in \mathbb{Z}$. Conjugating by a translation, we can assume $y = 0$ or $y = 1$. When $y = 0$, we can compose with a translation so $g = r$. When $y = 1/2$, we can do the same to get $g = r'$. Finally we note that we cannot have both r and r' in Γ, since their product rr' is translation by a vector not in L_Γ. ∎

3 Simple groups

Here is an example of how to use the Sylow theorems to classify simple groups.

Theorem 3.1 *There is no simple group of order 24.*

Proof. Let $|G| = 24$. Since $24 = 3 \cdot 8$, we have Sylow subgroups of orders 3 and 8. The number of such subgroups satisfies:

$$s_3 = 1 \bmod 3, s_3|8, \implies s_3 = 1 \text{ or } 4.$$
$$s_8 = 1 \bmod 2, s_8|3, \implies s_8 = 1 \text{ or } 3.$$

If either s_3 or s_8 is 1, then we have a normal Sylow subgroup, and hence G is not simple. On the other hand, if $s_8 = 3$, then the action of G by conjugation on its subgroups of order 8 determines a map $\phi : G \to S_3$. By the second Sylow theorem, the image of G in S_3 acts *transitively* on the set 3 subgroups of order 8. Thus the image is nontrivial, so $\mathrm{Ker}(\phi) \neq G$. Since $|S_3| = 6 < |G| = 24$, $\mathrm{Ker}(\phi) \neq (e)$. Thus $\mathrm{Ker}(\phi)$ is a nontrivial normal subgroup, and G is not simple. ∎

4 Semidirect products

Here is a very important generalization of the notion of a product of groups. Let G and H be groups, and let $\phi : H \to \mathrm{Aut}(G)$ be a homomorphism. With ϕ understood, it is convenient to use the notation

$$g^h = \phi(h)(g);$$

the fact that $\phi(h)$ is an automorphism of G implies $(g_1 g_2)^h = g_1^h g_2^h$.

We can now form a new group $S = G \ltimes_\phi H$, the *semidirect product* of G and H. (Often the ϕ is understood and suppressed.)

As a set, S consists of all pairs (g, h). We interpret such a pair as the product gh; thus any element of S can be uniquely expressed as such a product.

What about products in the other order? The crucial relation is that we define:

$$hg = g^h h.$$

Using this relation, any product of elements of S can be rewritten uniquely in the form gh again. For example:

$$g_1 h_1 g_2 h_2 = g_1 g_2^{h_1} h_1 h_2.$$

An equivalent and more formal defintion is that S consists of the ordered pairs (g, h) with the group law $(g_1, h_1)(g_2, h_2) = (g_1 g_2^{h_1}, h_1 h_2)$.

Note that G is always a *normal* subgroup of $S = G \ltimes H$, and $S/G \cong H$.

Recognizing semidirect products. The basic result is:

Theorem 4.1 *Let S be a group containing subgroups G and H such that:*

1. *G is normal,*
2. *$GH = \{gh \,:\, g \in G, h \in H\} = S$, and*
3. *$G \cap H = \{e\}$.*

Then S is isomorphic to $G \ltimes_\phi H$, where $\phi(h)(g) = hgh^{-1} \in G$.

Remark. Since G is normal, GH is always a *subgroup* of S. This often helps in verifying that $GH = S$.

Examples.

1. The group $\mathbb{Z}/n$ admits an automorphism of order 2 given by $\alpha(k) = -k$. Thus there is a map $\phi : \mathbb{Z}/2 \to \mathrm{Aut}(\mathbb{Z}/n)$. The resulting semidirect product is the usual dihedral group:
$$D_n \;=\; \langle r, \rho \,:\, r^2 = \rho^n = 1, r\rho r^{-1} = \rho^{-1} \rangle.$$
2. If ϕ is trivial, so $g^h = g$, then the semidirect product becomes the ordinary product of groups $G \times H$.
3. The group of motions of the plane is given by $M = \mathbb{R}^2 \ltimes \mathrm{O}_2(\mathbb{R})$.
4. The orthogonal group itself is the semidirect product $\mathrm{O}_2 = \mathrm{SO}_2(\mathbb{R}) \ltimes \mathbb{Z}/2$, since we have $r\rho_\theta r^{-1} = \rho_{-\theta}$.
5. The group $\mathbb{Z}/7$ admits an automorphism of the form $\alpha(k) = 2k$. We have $\alpha(\alpha(\alpha(k))) = 8k = k \bmod 7$, so α has order 3 in $\mathrm{Aut}(\mathbb{Z}/7)$. Thus there is a *nonabelian* group of order 21 given by $S = \mathbb{Z}/7 \ltimes_\phi \mathbb{Z}/3$.

Note the following special case.

Corollary 4.2 *If $S = GH$, $G \cap H = \{e\}$, and G and H are both normal, then S is isomorphic to $G \times H$.*

Proof. We have $S \cong (S/H) \times (S/G) \cong G \times H$. ∎