Notes for abstract algebra

John Kerl

February 3, 2008

Abstract

The following are notes to help me prepare for the University of Arizona math department's Abstract Algebra qualifier in August 2006. Since abstract algebra is my least-weak subject, I won't have much to say here: I will document a few tricky problem solutions, and collect some handy facts.

This paper is under construction.

Contents

1 Disclaimer

There are many wonderful algebra texts. My personal favorite is Dummit and Foote [**DF**]. See also Grove [**Grove**], Hungerford [**Hun**], or Lang [**Lang**]. Friedberg et al. [**FIS**] is a nice reference for linear algebra. In this note, unlike my other qual-prep notes, I make no attempt to be comprehensive. Rather, I take the opportunity to present some problem solutions, preceded by some useful items. For example, I gather together in one handy reference all the criteria for diagonalizability of which I am aware.

2 Linear algebra

One might think this section should be contained in the discussion of modules — after all, a vector space is nothing more than a module over a field. However, each of the three UA quals contains an undergraduate component: for the algebra qual, this portion is over linear algebra. So, solutions to the linear-algebra problems need not require the use of graduate-level material.

Criteria for **diagonalizability**: an $n \times n$ matrix A is diagonalizable ...

- ...iff its minimal polynomial splits with distinct factors.
- ...if its characteristic polynomial splits with distinct factors. (This is sufficient, but not necessary: consider the identity matrix.)
- ...iff it is similar to a diagonal matrix, i.e. there exists an invertible $n \times n$ matrix Q and a diagonal matrix D such that $A = QDQ^{-1}$.
- ...iff the sum of the dimensions of its eigenspaces is equal to n.

Criteria for **non-diagonalizability**:

- The minimal polynomial doesn't split over the base field.
- The minimal polynomial has a double root.
- There is an eigenvalue λ such that $\ker(A - \lambda I)^2$ properly contains $\ker(A - \lambda I)$.

Example 2.1. $\triangleright$ To construct a matrix which is non-diagonalizable over $\mathbb{R}$, take a polynomial which doesn't split over $\mathbb{R}$: say, $\lambda^2 + 1$. Then write the **companion matrix** for that polynomial. In general, if $P(\lambda) = \lambda^n + a_{n-1}\lambda^{n-1} + \ldots + a_1\lambda + a_0$ is a monic polynomial, a companion matrix for $P(\lambda)$ is

$$\begin{bmatrix} -a_{n-1} & -a_{n-2} & \cdots & a_1 & a_0 \\ 1 & 0 & & & 0 \\ & 1 & \ddots & & \\ & & \ddots & & \\ 0 & & & 1 & 0 \end{bmatrix}.$$

That is, write the negated coefficients across the top, 1's on the subdiagonal, and 0's elsewhere. (One may find other conventions for the companion matrix. You can write various matrices, e.g. the transpose of the above, whose characteristic polynomial is what you desire.) For $P(\lambda) = \lambda^2 + 1$, we get

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

$\triangleleft$

Example 2.2. $\triangleright$ To construct a matrix which is non-diagonalizable over $\mathbb{C}$, we can't use the non-splitting property, since $\mathbb{C}$ is algebraically closed. We have to find an example where the minimal polynomial has a double root — say, a matrix which is non-zero but whose square is zero:

$$A = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$$

The characteristic polynomial of A is λ^2, which you can compute by taking $\det(A - \lambda I)$. The minimal polynomial has to divide the characteristic polynomial, and cannot be λ since A itself isn't zero. Thus, $\lambda = 0$ is a double root of the minimal polynomial. $\triangleleft$

3 Useful classes of matrices

Many qualifier problems are of the form *Give an example of ...*, or *Prove or disprove ...*. To be successful in providing examples and counterexamples, we need to have a **toolkit** of standard examples of things. One large class of examples has to do with matrices: we have rings of matrices and groups of invertible matrices; given a commutative ring R, we can obtain a non-commutative ring by, say, considering 2×2 matrices over R; and so on.

[xxx type me up]

Permutation matrices.

Rotation matrices: emphasize no real eigenvalues.

Projection matrices.

Shift matrices. Use as counterexample for $T : V \to V$ and $V = \ker(T) \oplus \operatorname{im}(T)$.

Elementary matrices E_{ij}: use to sketch pfs of simplicity of $M_n(K)$ and $Z(M_n(K))$.

4 Groups

Here are two criteria for solvability. One of them may be taken to be the definition, and the other may be proved equivalent. In [**Grove**], the first is taken to be the definition. First, some preliminary definitions.

Definition 4.1. Let G be a group, and let $x, y \in G$. The **commutator** of x and y, written $[x, y]$, is $xyx^{-1}y^{-1}$.

Definition 4.2. Let G be a group. The **derived subgroup** of G, written G', is generated by all the commutators $[x, y]$ where x and y range over all elements of G.

Definition 4.3. It is clear that $G' \leq G$. So, we can compute the derived subgroup of G'. The kth derived subgroup of G is written $G^{(k)}$.

How to show a subgroup is **normal**:

- By definition of normalcy: $H \lhd G$ iff for all $g \in G$, $gHg^{-1} \subseteq H$.
- Similarly: $H \lhd G$ iff for all $g \in G$ and all $h \in H$, $ghg^{-1} \in H$.

- $H \lhd G$ iff $H = \ker \phi$ for some homomorphism from G to some other group. (Kernels are normal.)
- If $H \subseteq G'$ then $H \lhd G$.

Definition 4.4. Let G be a group. A nested sequence of subgroups G_i

$$G = G_0 \geq G_1 \geq G_2 \dots$$

is called a **series**.

Definition 4.5. A series is called **normal** if

$$G \trianglerighteq G_i$$

for all i.

Definition 4.6. A series is called **subnormal** if

$$G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \dots .$$

Mnemonic 4.7. In a *sub*normal series, each G_i is normal in the *sub*group above it.

Definition 4.8. A subnormal series is called a **composition series** if it descends to 1, and if the G_i/G_{i+1} are all simple (i.e. G_{i+1} is a maximal normal subgroup of G_i) for all i.

Definition 4.9 (Definition of solvability)**.** Let G be a group. Then G is said to be **solvable** if $G^{(k)} = 1$ for some integer k.

Proposition 4.10 (Alternate criterion for solvability)**.** *A group G is **solvable** iff there exists a subnormal series, descending to 1 (i.e. $G_k = 1$ for some k), with abelian factors G_{i+1}/G_i.*

Remark 4.11. Usually we use the derived series for this purpose.

Definition 4.12. A group is said to be **nilpotent** if it satisfies an awkward ascending-series condition which I can never remember and, fortunately, which I don't think I ever *need* to remember.

There are two alternative characterizations which are often useful:

Proposition 4.13 (Alternate criterion for nilpotency)**.** *For $H < G$, let $[G, H]$ be the subgroup of G generated by all commutators $[g, h]$ for $g \in G$ and $h \in H$. Define $G_0 = G$, $G_1 = [G, G_0]$, and in general $G_{i+1} = [G, G_i]$. Then G is nilpotent iff the series descends to the trivial group, i.e. if there is an n such that $G_n = 1$.*

Proposition 4.14 (Alternate criterion for nilpotency: [**Grove**], theorem I.7.8.)**.** *G is nilpotent iff it is the direct product of its Sylow subgroups. In particular, if G is nilpotent, each Sylow subgroup is normal, and hence is unique.*

Proposition 4.15 (Sufficient condition for nilpotency)**.** *Finite p-groups are nilpotent.*

Mnemonic 4.16. If G is trivial, then $G_0 = 1$; if G is abelian, then $G_1 = 1$. Thus nilpotent groups are almost abelian in the sense that they descend to 1, just perhaps a bit slower than abelian groups do.

Mnemonic 4.17. Remember **CANSA**: cyclic groups $\subsetneq$ abelian groups $\subsetneq$ nilpotent groups $\subsetneq$ solvable groups $\subsetneq$ all groups. (See [**DF**], section 6.1.)

(This is nice, but doesn't come up nearly as often as FEPUI for rings (mnemonic 10.2).) All these inclusions are proper. Examples:

- $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ is abelian but not cyclic.
- The quaternion unit group is nilpotent but not abelian.
- $\mathcal{S}_4$ is solvable but not nilpotent. (Use Grove's I.7.8: there are 3 conjugate $\mathcal{D}_4$'s in $\mathcal{S}_4$, which are Sylow-2 subgroups of $\mathcal{S}_4$.)
- $\mathcal{S}_n$ is not solvable for $n \geq 5$.

5 Group actions

normal subgroups vs. orbit-stabilizer — ?

orbit-stabilizer formula

6 Semidirect products

Definition 6.1. Let G be a group with $N \lhd G$ and $K \subseteq G$. Furthermore suppose that $G = NK$ and $N \cap K = \{1\}$. If K acts on N (formally, if there is a homomorphism $K \to \mathrm{Aut}(N)$), we write

$$N \rtimes K$$

and call this the **semidirect product** of N and K. We sometimes write the action of $k \in K$ on $n \in N$ as n^k. Since $G = NK$, any $g \in G$ may be written in the form (n, k). Multiplication in G is

$$(n_1, k_1)(n_2, k_2) = (n_1 {n_2}^{k_1}, k_1 k_2).$$

Remark 6.2. How does inversion work? Given (n, k) we need to find (m, j) such that $(n, k)(m, j) = (1, 1)$. This gives

$$(1, 1) = (n, k)(m, j) = (nm^k, kj)$$

which forces $j = k^{-1}$. Then, in the first slot, $nm^k = 1$ forces

$$\begin{array}{rcl} m^k & = & n^{-1} \\ m & = & (n^{-1})^{k^{-1}}. \end{array}$$

Thus,

$$(n, k)^{-1} = ((n^{-1})^{k^{-1}}, k^{-1}).$$

Example 6.3. ▷ Dihedral groups may be written as

$$\mathcal{D}_n = \mathcal{C}_n \rtimes \mathcal{C}_2 = \langle \rho \rangle \rtimes \langle \phi \rangle$$

where ρ is the rotation of order n and ϕ is the flip. The flip acts on the rotations by inverting them:

$$\rho^i \phi^j \rho^k \phi^\ell = \begin{cases} \rho^{i+k} \phi^{j+\ell}, & j \text{ even} \\ \rho^{i-k} \phi^{j+\ell}, & j \text{ odd} \end{cases}$$

which is to say (since there are only two distinct powers of ϕ)

$$\begin{array}{rcl} \rho^i \rho^k \phi^\ell & = & \rho^{i+k} \phi^\ell \\ \rho^i \phi \rho^k \phi^\ell & = & \rho^{i-k} \phi^{1+\ell}. \end{array}$$

This is the familiar transposition rule

$$\phi \rho^k = \rho^{-k} \phi.$$

◁

Example 6.4. ▷ The T group (the other non-abelian group of order 12, besides $\mathcal{A}_4$ and $\mathcal{D}_6$) is

$$T = \mathbb{Z}_3 \rtimes \mathbb{Z}_4$$

where $\mathbb{Z}_4$ acts on $\mathbb{Z}_3$ by inversion. That is, 1 and 3 in $\mathbb{Z}_4$ negate elements of $\mathbb{Z}_3$; 0 and 2 in $\mathbb{Z}_4$ leave elements of $\mathbb{Z}_3$ alone. ◁

Example 6.5. ▷ Let $\mathcal{V}_4 = \{e, a, b, c\}$ be the Klein-four group as usual. Let $\mathcal{S}_3$ act on $\mathcal{V}_4$ by permuting the symbols a, b, and c. Then we can write the semidirect product

$$\mathcal{V}_4 \rtimes \mathcal{S}_3.$$

It can be shown (I won't here) that this is isomorphic to $\mathcal{S}_4$. ◁

7 A semidirect product example

Note: This section is perhaps not qualifier material. Something came up in the 2006-07 511 course which was "obvious" to the speaker, but not as obvious to everyone in the audience. Here I work through a detailed (albeit inelegant) computation, from first principles, in order to increase the level of obviousness. Moreover, the techniques here elucidate the kind of brainstorming one might need to resort to during an exam, on scratch paper, as part of an attempt to conjecture a more elegant solution to be turned in.

Consider the semidirect product $\mathbb{Z}_m \rtimes_\phi \mathbb{Z}_n$. Recall that multiplication in $\mathbb{Z}_m \rtimes_\phi \mathbb{Z}_n$, written additively, is

$$(a, b) + (c, d) = (a + [\phi(b)](c), b + d).$$

Then ϕ must be a homomorphism from $\mathbb{Z}_n$ into $\mathrm{Aut}(\mathbb{Z}_m)$. Here I describe the possibilities for ϕ and compute the center of these groups, starting with $m = 7$ and $n = 3$ as a concrete example.

Some notation: For brevity (I am not a number theorist), let $\mathbb{Z}_m$ denote $\mathbb{Z}/m\mathbb{Z}$. Really, $\mathbb{Z}_m$ is a commutative ring with 1. As such, it has an **additive group**: all the elements of the ring, with addition as the operation, forgetting about multiplication. Also, the invertible elements of the ring form a group called the **unit group** or **multiplicative group** (which possesses a subgroup structure). When I write $\mathbb{Z}_m$ in this section, I refer to the additive group of the ring. When I write $\mathbb{Z}_m^\times$ I refer to the multiplicative group.

Structure of the additive group: Recall that $\mathbb{Z}_m$ is always cyclic of order m; 1 is always a generator. (Any element relatively prime to m is also a generator. There are $\Phi(m)$ of these, where Φ is Euler's totient function. In particular, if m is prime, then any non-zero element of $\mathbb{Z}_m$ is a generator.)

Structure and subgroup structure of the multiplicative group: $\mathbb{Z}_m^\times$ has order $\Phi(m)$. In particular, recall that when m is prime, $\Phi(m) = m - 1$ and $\mathbb{Z}_m^\times$ is cyclic. Here, 1 is not a generator (except when $m = 2$). In general, we have to search for generators. For example, with $m = 7$, $2^3 = 1$ so 2 is not a generator. On the other hand, 3 has order 6 mod 7 and so 3 is a generator. Here are powers of 3 mod 7:

k	1	2	3	4	5	6
3^k	3	2	6	4	5	1

In fact, we can use this to write down orders of elements of the isomorphic cyclic groups $\mathbb{Z}_6$ and $\mathbb{Z}_7^\times$:

$x \in \mathbb{Z}_6$	1	2	3	4	5	6
$\lvert x\rvert$	6	3	2	3	6	1
$x \in \mathbb{Z}_7^\times$	3	2	6	4	5	1
$\lvert x\rvert$	6	3	2	3	6	1

So, $\mathbb{Z}_7^\times$ has two generators: 3 and 5. A cyclic group of order s has a unique subgroup for each divisor d of s. Here, $\mathbb{Z}_7^\times$ has a subgroup of order 2, generated by 6: this is $\{1, 6\}$. It also has a subgroup of order 3, generated by 2 or 4: this is $\{1, 2, 4\}$.

Structure of the automorphism group: Since $\mathbb{Z}_7$ is cyclic, any homomorphism from $\mathbb{Z}_7$ to itself, and in particular any automorphism, is specified by its action on $\mathbb{Z}_7$'s 1: $\sigma(x) = x\sigma(1)$. Since 7 is prime, there are 6 generators for $\mathbb{Z}_7$: all the non-zero elements. Thus, 1 may map to any generator. So, the elements of $\mathrm{Aut}(\mathbb{Z}_7)$ are as follows:

$\mathbb{Z}_7$	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
0	0	0	0	0	0	0
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Note that $\sigma_i(x) = ix$, i.e. the ith automorphism is just multiplication by i. How do we compose automorphisms? We have $\sigma_i(\sigma_j(x)) = ijx$ for any test point x, so $\sigma_i \circ \sigma_j$ is σ_{ij}. So, arithmetic on the i's and j's is done in the multiplicative group $\mathbb{Z}_7^\times$. This substantiates what we already know about $\mathrm{Aut}(\mathbb{Z}_7)$, namely, that it is isomorphic to $\mathbb{Z}_7^\times$ which in turn is isomorphic to $\mathbb{Z}_6$. Given the above information about $\mathbb{Z}_7^\times$, we see that $\mathrm{Aut}(\mathbb{Z}_7)$ is cyclic, generated by either σ_3 or σ_5.

Recall that for any group homomorphism $\psi : A \to B$, given an element $a \in A$ of order s, the order of $\psi(a)$ in B must divide the order of a in A. This is because, if $a^s = e_A$, $\psi(a^s) = \psi(a)^s = e_B$.

To construct the semidirect product $\mathbb{Z}_7 \rtimes_\phi \mathbb{Z}_3$, we need ϕ to be a homomorphism from $\mathbb{Z}_3$ to $\mathrm{Aut}(\mathbb{Z}_7)$. The possible homomorphisms from the order-3 cyclic group $\mathbb{Z}_3$ to the order-6 cyclic group $\mathbb{Z}_7^\times$ are specified by the image of $\mathbb{Z}_3$'s 1. It can map to σ_1 (trivial homomorphism), σ_2 (monomomorphism), or σ_4 (monomomorphism):

$\mathbb{Z}_3$	ϕ_1	ϕ_2	ϕ_3
0	σ_1	σ_1	σ_1
1	σ_1	σ_2	σ_4
2	σ_1	σ_4	σ_2

Now I want to parameterize the possible ϕ's as simply as possible. The automorphism $\sigma_t = \phi(1)$ must be of order dividing 3. This means that $\sigma_t^3 = \sigma_1$. Since the arithmetic in $\mathrm{Aut}(\mathbb{Z}_7)$ is that of the multiplicative group $\mathbb{Z}_7^\times$, this means that $t^3 \equiv 1 \pmod 7$.

At this point we can write the semidirect-product arithmetic without any reference to ϕ. We know that $\phi(b) = b\phi(1) = (\sigma_t)^b$, and furthermore that $\sigma_t(x) = tx$. This means that for $c \in \mathbb{Z}_7$,

$$[\phi(b)](c) = [\sigma_t]^b(c) = t^b c$$

So the group arithmetic is

$$(a, b) + (c, d) = (a + [\phi(b)](c), b + d) = (a + ct^b, b + d).$$

Now we can ask about the center of $\mathbb{Z}_7 \rtimes_\phi \mathbb{Z}_3$. If $t = 1$, i.e. if ϕ is the trivial map, then we have the abelian group $\mathbb{Z}_7 \oplus \mathbb{Z}_3$. Now suppose we have $t = 2$, i.e. $\phi(1) = \sigma_2$. What is the center? We know that (a, b) is in the center if it commutes with all (c, d). A standard trick is to say that *in particular*, (a, b) must commute with our *judicious choice* of (c, d). Just as a guess, let's try putting $c = 1$ and $d = 0$. Then

$$\begin{aligned}
(a, b) + (c, d) &= (a + ct^b, b + d) \\
(c, d) + (a, b) &= (c + at^d, d + b) \\
(a, b) + (1, 0) &= (a + t^b, b) \\
(1, 0) + (a, b) &= (1 + a, b).
\end{aligned}$$

For these two to be equal forces $t^b \equiv 1 \pmod 7$ for $b \in \mathbb{Z}_3$. We have $t = 2$ and choices of b are 0, 1, and 2, so $t^b \equiv 1 \pmod 7$ only for $b = 0$. This means that $b = 0$ for any (a, b) in the center of $\mathbb{Z}_7 \rtimes_\phi \mathbb{Z}_3$.

At this point we need to make a second judicious choice. We have

$$\begin{aligned} (a, 0) + (c, d) &= (a + c, d) \\ (c, d) + (a, 0) &= (c + at^d, d). \end{aligned}$$

For these two to be equal requires

$$a - at^d = a(1 - t^d) = 0.$$

Choose $d = 1$ to get

$$a - 2a = a(1 - 2) = 6a = 0$$

which forces $a = 0$. This, together with $b = 0$, shows that the center of $\mathbb{Z}_7 \rtimes_\phi \mathbb{Z}_3$, for non-trivial ϕ, is trivial.

* * *

Next, we generalize. What here depended on specific values $m = 7$ and $n = 3$? We used the fact that m was prime, and we required a solution to $t^n \equiv 1 \pmod m$. In order for the map ϕ to be non-trivial, we required a non-trivial solution, i.e. $t \not\equiv 1 \pmod m$. This is what I have in the past heard referred to as a **metacyclic group** parameterized by m, n, and t. I call these two conditions on t a *constructibility criterion*.

What about the center of $\mathbb{Z}_m \rtimes_\phi \mathbb{Z}_n$ for prime m? The same two judicious choices give us

$$t^b = 1$$

and

$$a(1 - t^d) = 0.$$

The second of these forces $a = 0$ if m is prime, as long as t is not 1, which is true for the non-abelian case of interest. The first does not always force $b = 0$.

For example, with $n = 4$ and $t = 2$, the constructibility criterion is for there to be a non-trivial solution t for

$$t^4 \equiv 1 \pmod 7 \quad \text{and} \quad t \not\equiv 1 \pmod 7.$$

This is satisfied by $t = 6$. Then $t^b = 1$ has solutions $b = 0$ and $b = 2$, so the center is non-trivial:

$$Z(\mathbb{Z}_7 \rtimes_\phi \mathbb{Z}_3) = \{(0, 0), (0, 2)\}.$$

8 Classification of small groups

A common question is: classify all groups of order 20. Often, we are given an order of the form p^2q for primes p and q. If you read through various algebra texts, e.g. [**DF**], you will see various tricks employed. Here, though, is a (not necessarily exhaustive!) list of the kinds of things you can try.

(0) The zeroth step is to know something about your destination:

- Write down all the abelian groups, using, say, elementary-divisor decomposition.

  - Also write down any non-abelian groups that come to mind. For example, for every even order there is a dihedral group of that order. So for order 20, we know there is $\mathcal{D}_{10}$. Likewise, if 4 divides the order of the group, then there is the product of a dihedral with a cyclic-two — e.g. for order 20, there is $\mathcal{D}_5 \times \mathcal{C}_2$.

  Listing some known groups will give you a lower bound on the number of non-abelian groups, helping you to check your work in subsequent steps.

(1) Use the Sylow theorems. E.g. for order p^2q we have:

$$\begin{array}{rcll} n_p & \equiv & 1 & \mod p, \\ n_q & \equiv & 1 & \mod q, \\ n_p & \mid & q, & \\ n_q & \mid & p^2. & \end{array}$$

(2) If you can conclude that both $n_p = 1$ and $n_q = 1$, then let P be the p-Sylow subgroup and let Q be the q-Sylow subgroup. Then $G = P \times Q$. Often, this will reduce to the abelian cases: groups of order p or p^2 are abelian. However, there are non-abelian groups of order p^3.

(3) For the case that, say, $n_p = 1$ but $n_q \neq 1$, then $G = P \rtimes Q$. Now you can list out the homomorphisms from Q into $\mathrm{Aut}(P)$. It is handy to know that:

  - $\mathrm{Aut}(\mathbb{Z}_p) \cong \mathbb{F}_p^\times \cong \mathbb{Z}_{p-1}$.
  - $\mathrm{Aut}(\mathbb{Z}_p^n) \cong \mathrm{GL}(n, \mathbb{F}_p)$. Also, from [**Rotman**],

$$\#\mathrm{GL}(n, \mathbb{F}_p) = (p^n - 1)(p^n - p)(p^n - p^2 \cdots (p^n - p^{n-1}).$$

(4) Petal diagrams. [Needs a nice picture here.] Say you have the case $p = 3$ and $n_p = 4$. Then there are four subgroups of order 3, which intersect only at the identity. This means there are at least 9 elements in the group, 8 of them of order 3 — with none of the latter possibly being in a q-Sylow subgroup. Often, you can use such an argument to show that such a case would require more elements than the order of the group. [Insert an example here.]

Do note that Rotman soft-pedals classification of groups of a given order. See, for example, [**DF**] for a more thorough treatment.

9 Wreath products

Note: This section is not qualifier material. The subject of wreath products came up while I was TA'ing 511 in 2006-2007, and I couldn't find any examples as clear as the following so I thought I'd write them down for posterity.

Definition 9.1. The **wreath product** (as I have seen it most clearly defined) of two groups A and K is as follows: K maps homomorphically into $\mathcal{S}_n$ for some n. (This makes sense when K is finite. A wreath product can also be defined for infinite K.) Then

$$A \wr K = A^n \rtimes K$$

where the action of K on A^n is by permuting indices on n-tuples in A^n. This requires specifying n as well as the homomorphism from K into $\mathcal{S}_n$. When no homomorphism is given, it is taken to be the left-regular representation. (Remember that for the left regular action, n would be the order of K.)

Remark 9.2. The automorphism group of A has nothing to do with the wreath product (again, as I have seen it defined). *All* the group K does is permute the *positions* of n-tuples of A^n for some n — it does not act automorphically on the *elements* at those positions.

Example 9.3. $\triangleright$ For $\mathbb{Z} \wr \mathbb{Z}_3$, we could have $\mathbb{Z}^3 \rtimes \mathbb{Z}_3$ with $\mathbb{Z}_3$ cyclically permuting triples of integers. I will use the exponent notation for semidirect actions, as in section 6, and since $\mathbb{Z}$ is abelian, I will use additive rather than multiplicative notation:

$$((m_1, m_2, m_3), a) + ((n_1, n_2, n_3), b) \quad = \quad ((m_1, m_2, m_3) + (n_1, n_2, n_3)^a, a + b).$$

If we let $\mathbb{Z}_3$ act on $\mathbb{Z}^3$ by right-shifting, then as a particular example:

$$\begin{aligned} ((m_1, m_2, m_3), 1) + ((n_1, n_2, n_3), 2) &= ((m_1, m_2, m_3) + (n_1, n_2, n_3)^1, 1 + 2) \\ &= ((m_1, m_2, m_3) + (n_2, n_3, n_1), 0) \\ &= ((m_1 + n_2, m_2 + n_3, m_3 + n_1), 0). \end{aligned}$$

Note that the group operation on A^n (here, $\mathbb{Z}^3$) is just plain old componentwise operation, *except* that we first permute the positions of the tuples in the second operand. Hence the term *wreath*.

We could also have $\mathbb{Z}_3$ act on $\mathbb{Z}^3$ by left-shifting, or by no shift at all. Or we could have $\mathbb{Z}_3$ act on $\mathbb{Z}^6$ by left-shifting pairs of triples:

$$(m_1, m_2, m_3, m_4, m_5, m_6)^1 = (m_2, m_3, m_1, m_5, m_6, m_4).$$

Etc. etc. $\triangleleft$

Example 9.4. $\triangleright$ For $\mathbb{Z} \wr \mathcal{S}_3$, there are several possibilities. Again taking $n = 3$, one possibility is:

$$((m_1, m_2, m_3), \sigma) + ((n_1, n_2, n_3), \tau) \quad = \quad ((m_1, m_2, m_3) + (n_1, n_2, n_3)^\sigma, \sigma \circ \tau).$$

As a particular example in that construction,

$$\begin{aligned} ((m_1, m_2, m_3), (13)) + ((n_1, n_2, n_3), (123)) &= ((m_1, m_2, m_3) + (n_1, n_2, n_3)^{(13)}, (13) \circ (123)) \\ &= ((m_1, m_2, m_3) + (n_3, n_2, n_1), (12)) \\ &= ((m_1 + n_3, m_2 + n_2, m_3 + n_1), (12)). \end{aligned}$$

We could also have $\mathcal{S}_3$ act on $\mathbb{Z}^3$ by permutations, or inverse permutations; we could have $\mathcal{S}_3$ act on $\mathbb{Z}^2$ by having the odd permutations swap 2-tuples of integers and having the even permutations leave 2-tuples of integers intact; etc. $\triangleleft$

10 Rings

Let m be a squarefree integer, other than 0 or 1. Then the **quadratic integers** of $\mathbb{Q}(\sqrt{m})$, which Grove calls R_m, are

$$\begin{cases} \mathbb{Z}[\frac{1+\sqrt{m}}{2}], & m \equiv 1 \pmod 4. \\ \mathbb{Z}[\sqrt{m}], & m \equiv 2, 3 \pmod 4 \end{cases}$$

Mnemonic 10.1. Which is which? Just remember that $i = \sqrt{-1}$, -1 is 3 mod 4, the integers of $\mathbb{Q}(i)$ are $\mathbb{Z}[i]$, and "two three four".

Mnemonic 10.2. Remember **FEPUI** [feh, pooey!]: fields $\subsetneq$ Euclidean domains $\subsetneq$ PIDs $\subsetneq$ UFDs $\subsetneq$ integral domains.

(See also CANSA for groups, mnemonic 4.17.) All these inclusions are proper. Standard examples ([**DF**], end of section 8.3):

- $\mathbb{Z}$ is a Euclidean domain but not a field.
- $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ (i.e. the ring of integers of $\mathbb{Q}[\sqrt{-19}]$, as $-19 \equiv 1 \pmod 4$) is a PID which is not Euclidean.
- $\mathbb{Z}[x]$ is a UFD but not a PID (consider $\langle 2 \rangle$ and $\langle x \rangle$).
- $\mathbb{Z}[\sqrt{-5}]$ (i.e. the ring of integers of $\mathbb{Q}[\sqrt{-5}]$, as $-5 \equiv 3 \pmod 4$) is an integral domain which is not a UFD. (Remember: $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$.)

11 Fields

galois groups for cubics

Eisenstien criterion Eisenstein — make the distinction between irr'ty over $\mathbb{Z}$ vs. $\mathbb{Q}$ (or, ID and its QF more generally).

calculus to find TPs etc., or cubic **discriminant** — equivalent.

galois groups for quartics?

$\mathcal{S}_p$ trick for quintics.

12 Modules and tensor products

Definition 12.1. An R-module is **free** iff it may be written as a direct sum of copies of R.

Example 12.2. $\triangleright$ An n-dimensional vector space over a field K is isomorphic to K^n, hence free. $\triangleleft$

Proposition 12.3. *Let R be a commutative ring with identity, and let M be a two-sided unital R-module. Then*

$$R \otimes_R M \cong M.$$

Mnemonic 12.4. Move all scalars over:

$$r \otimes m = (r \cdot 1) \otimes m = 1 \otimes rm.$$

This works even for $r = 0$, since $0 \cdot 1 = 0$.

Proposition 12.5 (Hom modules)**.** *Let R be a commutative ring; let M and N be R-modules. Then*

$$\mathrm{Hom}_R(M, N)$$

is an R-module, where module addition is given by

$$(\phi + \psi)(m) = \phi(m) + \psi(m)$$

and ring-module multiplication is given by

$$(r\phi)(m) = r\phi(m).$$

Remark 12.6. Try to prove that $r\phi$ is actually an R-module homomorphism. You will immediately see why R needs to be commutative. (If R is not commutative, then $\mathrm{Hom}_R(M, N)$ is merely an abelian group.)

Remark 12.7. We can instead make the abelian group $\mathrm{Hom}_R(M, M)$ into a ring, using addition as above, but with composition as multiplication.

Remark 12.8. The notation $\mathrm{Hom}_R(M, M)$ is ambiguous — is it an R-module with ring-module multiplication as above, or is it a ring with composition as its multiplication? Sometimes people write $\mathrm{End}_R(M)$ to signify the latter.

Proposition 12.9 (FOIL for hom modules)**.** *Let R be a commutative ring; let M, M_1, M_2, N, N_1, and N_2 be R-modules. Then*

$$\mathrm{Hom}_R(M_1 \oplus M_2, N) \cong \mathrm{Hom}_R(M_1, N) \oplus \mathrm{Hom}_R(M_2, N)$$

and

$$\mathrm{Hom}_R(M, N_1 \oplus N_2) \cong \mathrm{Hom}_R(M, N_1) \oplus \mathrm{Hom}_R(M, N_2).$$

Proposition 12.10 (FOIL for tensor products of direct sums)**.** *Let M, M_1, and M_2 be left R-modules; let N, N_1, and N_2 be right R-modules. Then*

$$(M_1 \oplus M_2) \otimes N \cong (M_1 \oplus N) \otimes (M_2 \oplus N) \qquad \textit{and} \qquad M \otimes (N_1 \oplus N_2) \cong (M \oplus N_1) \otimes (M \oplus N_2)$$

Corollary 12.11. *Let M and N be free modules of ranks m and n, respectively. Then $M \otimes N$ has rank mn.*

Proof.

$$R^m \otimes R^n \cong \bigoplus_{i=1}^{m} R \otimes \bigoplus_{i=1}^{n} R \cong (R \otimes R)^{mn} \cong R^{mn}.$$

□

How to show a module is **not free**: type up GD's nice solution here.

13 Problem solutions

13.1 January 2003 # 2A

Problem 1. Let G be a group, with x an element of finite order in G. Let p be a prime. Prove that there exist unique y and z in G such that (1) $x = yz$, (2) the order of y is a power of p, and (3) the order of z is relatively prime to p.

Remark. This proof is due to Tommy Occhipinti.

Proof. Since we have little else to work with other than the finite order of x, let $m = |x|$. To split up m, we could use Euclidean division to obtain $m = qp + r$, or we could factor m into $m = ap^k$ where a is relatively prime to p. The latter approach sounds more promising since it gives us the phrase "relatively prime". Since $x^{ap^k} = 1$, x^a has order p^k, and x^{p^k} has order a. But these don't give us y and z right away: the product of x^a and x^{p^k} isn't necessarily 1, and furthermore these are not the only elements of those respective orders: $(x^{ia})^{p^k} = 1$ for all integers i (where we may take ia mod m). Likewise, $(x^{jp^k})^a = 1$ for all j.

Since

$$x^{ia}x^{jp^k} = x^{ia+jp^k} = 1,$$

we have

$$ia + jp^k \equiv 0 \pmod{m}.$$

Since a and p^k are relatively prime by hypothesis, we can use the Chinese Remainder Theorem (suggested by the phrase "mod m" above) to solve for unique i and j.

xxx to do: this shows orders *divide* a and p^k .... Also we have shown uniqueness *inside* $\langle x \rangle$; need to show uniqueness in all of G. □

13.2 January 2006

Problem 2. Show that any group of order $4n + 2$, for integer n, contains a subgroup of index 2.

Remark. The idea of the following proof is due to Dinesh Thakur and Tommy Occhipinti.

Proof. Let G be such a group. Any subgroup of index 2 is normal. When we want to find a normal subgroup, we should always think of the kernel of a homomorphism, since when you have one, you have the other. The trick is to find such a homomorphism.

A familiar map with image having order 2 is the parity map on $\mathcal{S}_n$: if we had a symmetric group and if we had an element of odd parity, we'd be done. Here, we don't have a symmetric group. Not quite!

Consider the Cayley left representation of G. (That is, we send G injectively into $\mathcal{S}_G$ where G acts on itself by left multiplication. This sounds fancy, but just think of a Cayley table (multiplication table) for a group. Recall that the rows of these tables are always permutations of G; also, in each row and each column, each element appears only once.)

Since 2 divides the order of G, by Cauchy's theorem there exists an element of order 2 in G. Call it σ. By the remark in the preceding paragraph, the image of σ has no fixed points. Since it is of order 2, it must therefore be the product of $2n + 1$ transpositions. This is an odd number, and therefore the parity of σ must be odd.

Now consider the parity map from $\mathcal{S}_G$ to $\{\pm 1\}$. Since we just showed that $\mathcal{S}_G$ has an odd permutation, the image of the parity map is $\{\pm 1\}$, not just $\{1\}$. By the first group homomorphism theorem, the kernel of the parity map must have index 2. □

13.3 A nice fact

Here is something which came up during summer 2006 qual prep. I found an old, second-hand proof of it and thought I'd type it up for future reference.

Proposition 13.1. *Let G be a group with center $Z(G)$. If $G/Z(G)$ is cyclic, G is abelian.*

Proof. Since $G/Z(G)$ is cyclic, let $\pi Z(G)$ be a generator of the quotient group. Let g_1, g_2 be arbitrary elements of G, so $g_1 Z(G), g_2 Z(G)$ are arbitrary elements of $G/Z(G)$. Since $G/Z(G)$ is cyclic, $g_1 Z(G) = \pi^i Z(G)$ and $g_2 Z(G) = \pi^j Z(G)$ for some integer i, j from which $\pi^{-i} g_1 \in Z(G)$ and $\pi^{-j} g_2 \in Z(G)$. Then for some $z_1, z_2 \in Z(G)$, $\pi^{-1} g_1 = z_1$ and $\pi^{-j} g_2 = z_2$. Then

$$\begin{aligned}
g_1 &= \pi^i z_1 \\
g_2 &= \pi^j z_2 \\
g_1 g_2 &= \pi^i z_1 \pi^j z_2 \\
&= \pi^i \pi^j z_1 z_2 \text{ since } z_1, z_2 \in Z(G) \\
&= \pi^{i+j} z_1 z_2 \\
g_2 g_1 &= \pi^j z_2 \pi^i z_1 \\
&= \pi^j \pi^i z_2 z_1 \text{ since } z_1, z_2 \in Z(G) \\
&= \pi^{i+j} z_1 z_2 \\
&= g_2 g_1
\end{aligned}$$

Since g_1, g_2 were arbitrary in G and since they commute, G is abelian.

□

References

[**DF**] D.S. Dummit and R.M. Foote. *Abstract Algebra* (2nd ed.). John Wiley and Sons, 1999.

[**FIS**] H. Friedberg, A. Insel, and L. Spence. *Linear Algebra* (3rd ed). Prentice Hall, 1997.

[**Grove**] L.C. Grove. *Algebra.* Dover, 2004.

[**Hun**] Hungerford, T.W. *Algebra.* Springer, 1997.

[**Lang**] S. Lang. *Algebra* (3rd ed.). Springer, 2002.

[**Rotman**] J.J. Rotman. *Advanced Modern Algebra* (2nd printing). Pearson Education, 2002.

Index