

Algebra Final – Solutions

Math 122 – Harvard University – Fall 2002

1. (10 points) Prove that D_4 is isomorphic to the semidirect product of the Klein 4 group and $\mathbb{Z}/2$.

Proof. Let $D_4 = \langle r, f : r^4 = f^2 = 1, rf = fr^{-1} \rangle$. Let $G = \langle f, r^2 \rangle$ and $H = \langle rf \rangle$. It is easy to see G is isomorphic to the Klein 4 group and H is isomorphic to $\mathbb{Z}/2$. Also G is normal in D_4 , because $fr^2f = r^{-2} = r^2 \in G$ and $rf r^{-1} = r^2 f \in G$. But $rf \notin G$, so $(1, rf)$ is a list of coset representatives for D_4/G . Thus $D_4 = HG$, and therefore $D_4 = G \rtimes H$. ■

2. (10 points)

- (a) Give an example of a matrix A in $SO_2(\mathbb{R})$ such that $A^2 = -I$.
(b) Give an example of $A \neq 0$ in $M_2(\mathbb{R})$ such that $e^A = I$.

(a) $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

(b) $A = 2\pi \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ does the trick. Since its eigenvalues are distinct, this matrix is diagonalizable over \mathbb{C} ; that is, we can find $B \in GL_2(\mathbb{C})$ such that $BAB^{-1} = \begin{pmatrix} e^{2\pi i} & 0 \\ 0 & e^{-2\pi i} \end{pmatrix}$. Then $Be^AB^{-1} = \begin{pmatrix} e^{2\pi i} & 0 \\ 0 & e^{-2\pi i} \end{pmatrix} = I$ and therefore $e^A = I$.

3. (10 points) Let $A \in M_n(\mathbb{R})$ be a symmetric, positive-definite matrix. Prove that the largest entries in A occur along the diagonal; in other words, that $\max_{i \neq j} A_{ij} < \max_k A_{kk}$.

Proof. Let $\langle v, w \rangle$ be the inner product defined by A . Suppose A_{ij} is the largest off-diagonal entry of A . Then we have

$$0 < \langle e_i - e_j, e_i - e_j \rangle = A_{ii} + A_{jj} - 2A_{ij},$$

and thus one of the diagonal entries A_{ii} or A_{jj} must be strictly larger than A_{ij} . ■

4. (10 points) Let $R \subset \mathbb{Q}$ be the set of all rationals of the form p/q where $q \not\equiv 0 \pmod{5}$.

- (a) Prove that R is a subring of \mathbb{Q} .
(b) Find all of the ideals in R . Which ones are maximal? Which ones are prime?

(a) Let $x = p/q$ and $y = r/s$ be elements of R , expressed so that 5 does not divide q or s . Since 5 is prime, it cannot divide qs either. Thus $x + y = (ps + rq)/(qs)$ and $xy = (pr)/(qs)$ belong to R . Clearly $1 \in R$, so R is a ring.

(b) The ideals of R are all principal; they have the form $I = (5^n)$ or $I = (0)$. The only maximal ideal is $I = (5)$. The prime ideals are $I = (0)$ and $I = (5)$.

5. (10 points) Let G be a simple group of order 60.

(a) Find the number of 3- and 5-Sylow subgroups of G .

(b) Show A_5 has a subgroup of order 12.

(c) Show if G has a subgroup of order 12, then $G \cong A_5$.

(d) Show G is, in fact, isomorphic to A_5 .

(a) Let s_n be the number of n -Sylow subgroups. Then $s_3 = 10$ and $s_5 = 6$.

Indeed, by the Sylow theorems, $s_5 = 1 \pmod{5}$ and $s_5 | 12$; thus $s_5 = 1$ or 6. But if $s_5 = 1$ then there is a normal 5-Sylow subgroup, contradicting the simplicity of G . Similarly, $s_3 = 1 \pmod{3}$ and $s_3 | 20$, so $s_3 = 1, 4$ or 10. The case $s_3 = 1$ is ruled out as above; and if $s_3 = 4$ the action of G by conjugation of the set of 3-Sylow subgroups would give a nontrivial map $G \rightarrow S_4$, again contradicting normality because $|S_4| = 24 < |G|$.

(b) $A_4 \subset A_5$ has order 12.

(c) If $H \subset G$ has order 12, then $S = G/H$ has order 5, and the left action of G on S gives a nontrivial homomorphism $\phi : G \rightarrow \text{Sym}(S) \cong S_5$. Since G is simple, the map is injective. Since A_5 is normal in S_5 , the group $A_5 \cap \phi(G)$ is normal in $\phi(G)$, and thus $A_5 = \phi(G)$ by simplicity again. Thus G is isomorphic to A_5 .

(d) Each 2-Sylow subgroup H in G has order 4. Using the Sylow theorems as above, we find $s_2 = 5$ or 15. If $s_2 = 5$ then the action of G by conjugation on the set S of 2-Sylow subgroups gives a nontrivial homomorphism $\phi : G \rightarrow S_5$, from which we conclude that $G \cong A_5$ reasoning as above.

Suppose on the other hand that $s_2 = 15$. If these 15 subgroups meet in pairs only at the identity, then G has 45 elements of even order, which does not leave room for the elements of orders 3 and 5 found in (a). Thus we have must 2 different Sylow 2-subgroups, say H_1 and H_2 , containing a common element $x \in G$ of order 2.

Consider the centralizer $Z(x)$. This subgroup contains H_1 and H_2 so its order is > 4 and divisible by 4. Moreover $n = |Z(x)|$ divides 60; thus $n = 12, 20$ or 60. The case $n = 20$ would give a nontrivial map $G \rightarrow S_3$ and the case $n = 60$ would give a nontrivial element in the center of G , both contradicting simplicity. Thus $n = 12$ and by (c), $G \cong A_5$.

Note: It is tempting to argue that $s_2 = 15$ is impossible because G has too few elements of order 2 — only 15 — to accommodate 15 distinct subgroups of order 4. But this simple counting argument doesn't work, because the subgroups can overlap. For example, $(\mathbb{Z}/2)^4$ has only 15 elements of order 2, but it contains 15 different subgroups of order 8!

(50 points) Mark each assertion True (T) or False (F).

1. F. Given any pair of polynomials $f, g \in \mathbb{C}[x, y]$, there exists a pair of complex numbers (z, w) such that $f(z, w) = g(z, w) = 0$. (What if $f = 1$, the constant polynomial?)
2. F. The only unitary matrices $A \in M_2(\mathbb{C})$ with all their eigenvalues real are $A = \pm I$. (The matrix $A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ is also unitary.)
3. F. The center of the group $O_3(\mathbb{R})$ is trivial. (The element $-I$ is in the center.)
4. F. There is a point p on the cube whose orbit under the symmetries of the cube satisfies $|G \cdot p| = 4$. (The orders of stabilizers of points on the cube are 1, 2, 3 and 4, so the orbits have sizes 24, 12, 8 and 6.)
5. F. The group $SL_2(\mathbb{F}_7)$ has order 168. (The order is $(p^2 - 1)(p^2 - p)/(p - 1) = 336$.)
6. T. The group A_8 contains an element of order 15. (The permutation $(123)(45678)$ is even and of order 15.)
7. F. The vector space of all continuous functions $f : [0, 1] \rightarrow \mathbb{R}$ has a countable basis. (Consider the uncountably many functions $f_a(x) = |x - a|$, $a \in [0, 1]$. These functions are linearly independent: the graph of any finite linear combination of them has a sharp bend at one or more points, so it cannot be zero.)
8. F. The rings $(\mathbb{Z}/10)[x]$ and $\mathbb{Z}[x, y]/(10y)$ are isomorphic. (Here $(10y)$ denotes the principal ideal in $\mathbb{Z}[x, y]$ generated by $10y$.) (The ideal $(10y)$ does not contain the integer 10. Thus the sum of 1 with itself 10 times gives zero in the first ring but not the second, so they cannot be isomorphic.)
9. F. Every prime ideal in \mathbb{Z} is also a maximal ideal. ($I = (0)$ is prime but not maximal.)
10. F. Let $n > 0$ be a positive integer. If there exists a finite field F and a homomorphism $\phi : \mathbb{Z}/n \rightarrow F$, then n must be prime. (Consider the natural reduction map, $\mathbb{Z}/6 \rightarrow \mathbb{Z}/2 \cong F$.)