MATH 207: Problem Set 6

Jesse Farmer

10 November 2003

1. *Let F be a field and $A \in M_2(F)$. Show that A has a inverse if and only if $det(A) \neq 0$*

   By question 2, A is invertible if and only if $det(A)$ is invertible in F. But since F is a field the only element that is not invertible is 0. Therefore A is invertible if and only if $det(A) \neq 0$;

2. *Let R be a commutative ring with one and $A \in M_2(R)$. When does A have an inverse?*

   Claim: A is invertible if and only if $det(A)$ is invertible in R.

   Lemma: For any matrices $A, B \in M_2(R)$, $det(AB) = det(A)det(B)$

   Let $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ and $B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$

$$\begin{aligned} det(AB) &= det(\begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix}) \\ &= a_{12}a_{21}b_{12}b_{21} - a_{11}a_{22}b_{12}b_{21} - a_{12}a_{21}b_{11}b_{22} + a_{11}a_{22}b_{11}b_{22} \\ &= (a_{11}a_{22} - a_{12}a_{21})(b_{11}b_{22} - b_{12}b_{21}) \\ &= det(A)det(B) \end{aligned}$$

   Assume A is invertible, then there exists a $B \in M_2(R)$ such that $AB = I_2$. But this means $det(AB) = det(I_2) = 1$. Since the determinent is distributive, $1 = det(AB) = det(A)det(B) \Rightarrow det(B) = det(A)^{-1}$. That is, $det(A)$ is invertible.

   Assume $det(A)$ is invertible and let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

   We see that $det(A) = ad - bc$, and $A \cdot \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \frac{1}{ad-bc} \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$. That is, A is invertible.

   Therefore A is invertible if and only if $det(A)$ is invertible in R.

3. *What are the zero divisors of $M_2(R)$?*

   Claim: A is a zero divisor if and only if A is not invertible.

   Assume A is is both invertible and a zero divisor. Then there exists a $0 \neq B \in M_2(R)$ such that $AB = 0$. $0 = A^{-1}0 = A^{-1}(AB) = (A^{-1}A)B = I_2B = B$, but by hypothesis $B \neq 0$.

   The proof of the converse escapes me.

4. *Let $(R,+,\cdot,<)$ be an ordered integral domain. Show that R has a subring which is order isomorphic to $\mathbb{Z}$.*

   Let $R \supset S^+ = \{1, 1+1, 1+1+1, \dots\}$. This set must be infinite, since, if it were not, it would not be ordered (as e but every subset of an ordered set is necessarily ordered. Assume for contradiction that S^+ is not well-ordered; that is, there is some non-empty subset which does not have a leave element. Every subset is bounded below by 1, so 1 is not in this subset. Likewise, if n is not in this subset then $n+1$ cannot be in this subset since that would then be the least element. This subset must be empty, a contradiction of our assumption that this was a non-empty subset. Therefore S^+ is well ordered.

   If we take $-1 \cdot S^+ = S^-$, then this is the set of additive inverses of the elements in S^+. Letting $S = S^+ \bigcup \{0\} \bigcup S^-$, we see that we now have additive inverses and Therefore, by Problem 13 on Homework 3, this is order isomorphic to $\mathbb{Z}$.

5. *Show that $\mathbb{Q}$ does not satisfy the least upper bound property.*

   Let $S = \{p \in \mathbb{Q} | p^2 < 2\}$. We know that $p^2 = 2 \Rightarrow p \notin \mathbb{Q}$. So we want to show that this number is the upper bound. Let $\alpha = \sup S \in \mathbb{Q}$.

   - Assume $\alpha^2 > 2$
     $\alpha^2 > 2 \Leftrightarrow \alpha^2 + 2\alpha > 2 + 2\alpha \Leftrightarrow \alpha > \frac{2\alpha+2}{\alpha+2}$
     $$\begin{aligned} (\tfrac{2\alpha+2}{\alpha+2})^2 > 2 \quad &\Leftrightarrow \quad 4\alpha^2 + 8\alpha + 4 > 2\alpha^2 + 8\alpha + 8 \\ &\Leftrightarrow \quad 4\alpha^2 > 2\alpha^2 + 4 \\ &\Leftrightarrow \quad 2\alpha^2 > 4 \\ &\Leftrightarrow \quad \alpha^2 > 2 \end{aligned}$$
     So $\frac{2\alpha+2}{\alpha+2}$ is an upper bound but less than α, contradicting the assumption that $\alpha = \sup S$.
   - Assume $\alpha^2 < 2$
     $\alpha^2 < 2 \Leftrightarrow \alpha^2 + 2\alpha < 2 + 2\alpha \Leftrightarrow \alpha < \frac{2\alpha+2}{\alpha+2}$
     $$\begin{aligned} (\tfrac{2\alpha+2}{\alpha+2})^2 < 2 \quad &\Leftrightarrow \quad 4\alpha^2 + 8\alpha + 4 < 2\alpha^2 + 8\alpha + 8 \\ &\Leftrightarrow \quad 4\alpha^2 < 2\alpha^2 + 4 \\ &\Leftrightarrow \quad 2\alpha^2 < 4 \\ &\Leftrightarrow \quad \alpha^2 < 2 \end{aligned}$$
     So $\frac{2\alpha+2}{\alpha+2} \in S$ but greater than α, contradicting the assumption that $\alpha = \sup S$.

   Hence the supremum must satisfy $\alpha^2 = 2$, but no rational number does this. Therefore we have a bounded set of rationals, S, whose supremum is not in $\mathbb{Q}$. That is, $\mathbb{Q}$ does not satisfy the least upper bound property.

6. *Show that there is a bijection from the normal subgroups of $\frac{G}{N}$ and the normal subgroups of G containing N if $N \trianglelefteq G$.*

   We know that the function defined by $N \mapsto \varphi^{-1}(N)$ is a bijection between subgroups of $\frac{G}{N}$ and subgroups of G containing N, so all that is left to show is that, given some $H \leq G$ and $\bar{H} = \frac{N}{N} \leq \frac{G}{N}$, this map preserves normality.

   Define $f : \frac{G}{N} \to \frac{G}{H}$ by $f(xN) = xH$. Since the subgroups are normal, we see that this is a well-defined homomorphism whose kernel is $\frac{H}{N}$ and whose image is $\frac{G}{H}$. By the first isomorphism theorem we see that $\frac{G/N}{G/N}$ is isomorphic to $\frac{G}{H}$.

   I believe this implies our statement about normality, but I'm not sure how.

7. *Let G be a finite group and H be a subgroup of G with index k. Show that there exists a set of elements $x_1, x_2, \ldots, x_k$ in G which can serve as complete coset representatives for both left and right cosets of H.*

8. *Find all possible areas of lattice squares in $\mathbb{R}^2$.* Every lattice square in $\mathbb{R}^2$ is generated by constructing a line between the origin and an arbitrary point (a,b) where $a,b \in \mathbb{Z}$. The area of this square is a^2+b^2, so an integer is the area of a lattice square if and only if it is the sum of two squares. Thus, we must discover which integers are the sum of two squares.

   Claim: A positive integer n can be represented as the sum of two squares if and only if its prime factorization contains no odd powers of primes congruent to 3 modulo 4.

9. *Find all positive integers which can be the length of the hypotenuse of a right triangle with legs of integer length.*

10. *Define a polyhedron in $\mathbb{R}^n$.*

    It is a union of s-simplices for with $s \leq r$, that is closed under intersection, and such that the only time that one of simplices is contained in another is as a face. An n-simplex is the convex hull of (n+1) points in some Euclidian space.

11. *Find a Cauchy sequence in $\mathbb{Q}$ which does not converge in $\mathbb{Q}$.*

    Define
    $$a_n = \begin{cases} 1 & n=1 \\ \frac{2a_{n-1}+2}{a_{n-1}+2} & n>1 \end{cases}$$

    By the previous problem using this sequence, we see that $1 > a_2 > a_3 > \ldots > a_n > \ldots > \sqrt{2}$, so this set is clearly bounded in $\mathbb{Q}$. Moreover, this sequence is clearly Cauchy since it is strictly decreasing and bounded. Assume it converges in $\mathbb{Q}$, then $\lim_{n\to\infty} a_n = L$ and $\lim_{n\to\infty} a_{n+1} = L$, but $a_{n+1} = \frac{2a_n+2}{a_n+2}$. Thus $\frac{2L+2}{L+2} = L \Rightarrow L^2+2L = 2L+2 \Rightarrow L = \sqrt{2}$. But then $L \notin \mathbb{Q}$. So (a_n) is Cauchy but does not converge in $\mathbb{Q}$.

12. *Show that if $(a_n), (b_n)$ are Cauchy sequences then (a_n+b_n) is a Cauchy sequence.*

    We have $\forall r > 0 \exists N_1 \in \mathbb{N} \ni m,n > N_1 \Rightarrow |a_n - a_m| < \frac{r}{2}$ and $\forall r > 0 \exists N_2 \in \mathbb{N} \ni m,n > N_2 \Rightarrow |b_n - b_m| < \frac{r}{2}$

    Let $N = max(N_1, N_2)$, then $\forall r > 0, |(a_n+b_n)-(a_m+b_m)| \leq |a_n-a_m|+|b_n-b_m| < \frac{r}{2}+\frac{r}{2} = r$

    Therefore if (a_n) and (b_n) are Cauchy sequences then so is (a_n+b_n).

13. *Let $(R,+,\cdot)$ be a ring with one. Show that $(R^x,\cdot)$ is a group.*

    - Associativity is inhereted.
    - Each element has an inverse by definition of $(R^x,\cdot)$.
    - $1\cdot 1 = 1$, so there is an identity in R^x
    - Let $a,b \in R^x$, then a^{-1}, b^{-1} exist. $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}b = 1$. So the operation is an internal law of composition.

14. *Describe $(\mathbb{Z}_n^x,\cdot)$ for $2 \leq n \leq 16$.*

n	elements	Isomorphic group
2	1	$\{e\}$
3	1,2	$(\mathbb{Z}_2,+)$
4	1,3	$(\mathbb{Z}_2,+)$
5	1,2,3,4	$(\mathbb{Z}_4,+)$
6	1,5	$(\mathbb{Z}_2,+)$
7	1,2,3,4,5,6	$(\mathbb{Z}_6,+)$
8	1,3,5,7	$(\mathbb{Z}_2\times\mathbb{Z}_2,+)$
9	1,2,4,5,7,8	$(\mathbb{Z}_3\times\mathbb{Z}_2,+)$
10	1,3,7,9	$(\mathbb{Z}_4,+)$
11	1,2,3,4,5,6,7,8,9,10	$(\mathbb{Z}_{10},+)$
12	1,5,7,11	$(\mathbb{Z}_2\times\mathbb{Z}_2,+)$
13	1,2,3,4,5,6,7,8,9,10,11,12	$(\mathbb{Z}_{12},+)$
14	1,3,5,9,11,13	$(\mathbb{Z}_3\times\mathbb{Z}_2,+)$
15	1,2,4,7,8,11,13,14	$(\mathbb{Z}_5\times\mathbb{Z}_3,+)$
16	1,3,5,7,9,11,13,15	$(\mathbb{Z}_4\times\mathbb{Z}_4,+)$

15. *Let C be the set of all Cauchy sequences in $\mathbb{Q}$. Show that $I=\{(a_n)\in C|a_n\to 0\}$ is a maximal ideal.*

First we show that I is an ideal. Let $(a_n),(b_n)\in I$, then we have $\forall r>0\exists N_1\in\mathbb{N}\ni n>N\Rightarrow |a_n|<\frac{r}{2}$ and $\forall r>0\exists N_2\in\mathbb{N}\ni n>N_2\Rightarrow |b_n|<\frac{r}{2}$. Let $N=max(N_1,N_2)$ then $\forall r>0$ we have $|a_n+b_n|\leq |a_n|+|b_n|<\frac{r}{2}+\frac{r}{2}=r$. Therefore $(a_n),(b_n)\in I\Rightarrow (a_n+b_n)\in I$. Now, let $(b_n)\in C$. Because (b_n) is Cauchy it is eventually bounded from above by some constant, call it A. Choose N so that $|a_n|<\frac{r}{A}$. Then $|a_nb_n|<\frac{r}{A}A=r$ for $n\geq N$. I is therefore an ideal of C.

To prove that I is maximal it suffices to show that for any $(a_k)\in C$ the ideal generated by I and (a_k) is equal to C. Because $(a_k)\notin I$ there is an M such that a_k is always nonzero for $k\geq M$. Define r_k as follows (b_k is any element of C):

$$r_k=\begin{cases}\frac{b_k}{a_k} & k\geq M\\ 1 & k<M\end{cases}$$

r_k is Cauchy since,

$$|\frac{a_n}{b_n}-\frac{a_m}{b_m}|=\frac{1}{|a_na_m|}|b_na_m-a_nb_m|$$

If we choose P such that $|a_k|\geq P$ for sufficiently large k and choose K such that $|b_k|\leq K$ for sufficiently large k we have

$$|\frac{a_n}{b_n}-\frac{a_m}{b_m}|\leq\frac{K}{P^2}|a_n-a_m|$$

for sufficiently large m,n. That this is Cauchy follows immediately from our assumption that (a_k) is Cauchy. Let $i_k=b_k-r_ka_k$ and note that this is eventually zero, i.e., $(i_k)\in I$. Now $(b_k)=(r_k)(a_k)+(i_k)$, but the terms on the right-hand side belong to the ideal generated by I and (a_k). Therefore (b_k) is in this ideal, i.e., this ideal is all of C. Therefore, I is a maximal ideal.