Department of Mathematics
University of Illinois at Urbana-Champaign

MATH 417 – SPRING 2017 – SECTION B1
FINAL EXAM

MAY 5, 2017

SOLUTIONS

1. (50 points) Consider the symmetric group in 4 elements S_4 and let $H \subset S_4$ be the subgroup:

$$H = \{I, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}.$$

(a) Show that H is a normal subgroup of S_4;
(b) What is the order of the quotient group S_4/H? Justify.
(c) Is the group S_4/H abelian? What about A_4/H? Justify.

SOLUTION:
(a) For any $\pi \in S_4$ we have

$$\pi(i,j)(k,l)\pi^{-1} = (\pi(i), \pi(j))(\pi(k), \pi(l)).$$

Hence, if $\sigma \in H$ then $\pi\sigma\pi^{-1} \in H$, and we conclude that H is normal in A_4.

(b) By Lagrange's theorem:

$$|S_4/H| = |S_4|/|H| = 4!/4 = 6.$$

(c) The group S_4/H is not abelian, since we have:

$$(1,2)H \cdot (2,3)H = (1,2)(2,3)H = (3,1,2)H,$$
$$(2,3)H \cdot (1,2)H = (2,3)(1,2)H = (1,3,2)H,$$

and these two elements are distinct since:

$$(3,1,2) \cdot (1,3,2)^{-1} = (3,1,2) \cdot (2,3,1) = (1,3,2) \notin H.$$

On the other hand, $|A_4/H| = 4!/8 = 3$, and any group of order 3 is isomorphic to $\mathbb{Z}_3$, hence is abelian.

2. (50 points) Give one example of a ring $(A, +, \cdot)$ in each of the following classes (justify your answer):
(a) A is a field;
(b) A is a division ring but is not a field;
(c) A is an integral domain, but it is not a division ring;
(d) A satisfies the cancellation law, but it is not an integral domain;
(e) A does not satisfy the cancellation law.

SOLUTION:
(a) $A = \mathbb{R}$ (real numbers);

(b) $A = \mathbb{H}$ (quaternions);

(c) $A = \mathbb{Z}$ (integers);

(d) $A = 2\mathbb{Z}$ (even integers);

(e) $A = M_2(\mathbb{R})$ (real 2×2 matrices).

3. (50 points) Let $(A, +, \cdot)$ be an ordered ring with identity 1. Define the absolute value of an element $a \in A$ as usual by:

$$|a| = \max\{a, -a\}.$$

Show that for $a, b \in A$ the following statements are equivalent:

(a) $|a| \leq |b|$;

(b) $-|b| \leq a \leq |b|$;

(c) $a^2 \leq b^2$.

SOLUTION:

(a) $\Longrightarrow$ (b)

$$\begin{aligned} |a| \leq |b| &\implies a \leq |b| \text{ and } -a \leq |b| \\ &\implies a \leq |b| \text{ and } a \geq -|b| \\ &\implies -|b| \leq a \leq |b| \end{aligned}$$

(b) $\Longrightarrow$ (c) Since $|b|^2 = b^2$, we have:

$$-|b| \leq a \leq |b| \implies a^2 \leq |b|^2 = b^2$$

(c) $\Longrightarrow$ (a) Since $a^2 = |a|^2$ and $|a| \geq 0$, we conclude that:

$$\begin{aligned} a^2 \leq b^2 &\implies |a|^2 \leq |b|^2 \\ &\implies |a| \leq |b|. \end{aligned}$$

4. (50 points) Let $F_n = 2^{2^n} + 1$ be the n-esimal Fermat number.

(a) Prove by induction that $F_{n+1} - 2 = \prod_{i=0}^{n} F_i$, for all $n \geq 0$;

(b) Show that if $n \neq m$ then $\gcd(F_n, F_m) = 1$;

(c) Show that the previous result implies the existence of an infinite number of primes.

SOLUTION:

(a) When $n = 0$ the formula gives $F_1 - 2 = F_0$. Since $F_0 = 3$ and $F_1 = 5$, this is obviously true. Now assume that we know that $F_n - 2 = \prod_{i=0}^{n-1} F_i$. Then:

$$\begin{aligned} F_{n+1} - 2 &= 2^{2^{n+1}} - 1 \\ &= (2^{2^n})^2 - 1 \\ &= (2^{2^n} - 1)(2^{2^n} + 1) \\ &= (F_n - 2)F_n \\ &= \left(\prod_{i=0}^{n-1} F_i\right) F_n = \prod_{i=0}^{n} F_i. \end{aligned}$$

(b) Assume, say, that $m > n$. Then by (a), we have that $F_m - 2 = \prod_{i=0}^{m-1} F_i$. If d is a divisor of both F_m and F_n, then we conclude that d must divide 2. However, the Fermat numbers are all odd, so we must have $d = 1$. We conclude that $\gcd(F_n, F_m) = 1$.

(c) If they were a finite number of primes, then at least one of them would have to divide more than one (actually, infinite!) Fermat number, since there are an infinite number of such numbers. But this contradicts them being pairwise coprimes.

5. (50 points) Consider the following two linear system of equations in $\mathbb{Z}_5$:

$$\begin{cases} 3x + 4y \equiv a \\ -x + 2y \equiv b \end{cases} \qquad \begin{cases} 3x + 4y \equiv a \\ x + 2y \equiv b \end{cases}$$

(a) Which of these systems has solutions for all $a, b \in \mathbb{Z}$? Why?

(b) Solve the system that has solutions, in terms of a and b.

SOLUTION:

(a) The matrices of these linear systems have determinants, respectively:

$$\det \begin{pmatrix} 3 & 4 \\ -1 & 2 \end{pmatrix} = 10 \equiv 0 \pmod 5$$

$$\det \begin{pmatrix} 3 & 4 \\ 1 & 2 \end{pmatrix} = 2 \not\equiv 0 \pmod 5$$

Hence, only the second matrix is invertible in $\mathbb{Z}_5$, in which case the system has solutions for all $a, b \in \mathbb{Z}$. We can find its solutions by computing the inverse matrix:

$$\begin{aligned} A^{-1} &= (\det A)^{-1} \mathrm{adj} A \\ &= 2^{-1} \begin{pmatrix} 2 & -4 \\ -1 & 3 \end{pmatrix} \\ &= 3 \begin{pmatrix} 2 & -4 \\ -1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix} \end{aligned}$$

Therefore the solutions of the system are:

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a + 3b \\ 2a + 4b \end{pmatrix}$$

6. (50 points) Consider the ring $A = \mathbb{R}[x]/\langle x^2 + 2x\rangle$. Determine if the element $a = x + 1 + \langle x^2 + 2x\rangle$ is invertible in A and if yes, find its inverse.

SOLUTION:

Elements of the quotient ring A take the form $rx + s + \langle x^2 + 2x\rangle$. In order to find the inverse, we need to find $r, s \in \mathbb{R}$ such that:

$$\big(x + 1 + \langle x^2 + 2x\rangle\big)\big(rx + s + \langle x^2 + 2x\rangle\big) = 1 + \langle x^2 + 2x\rangle.$$

$$\iff (x + 1)(rx + s) + \langle x^2 + 2x\rangle = 1 + \langle x^2 + 2x\rangle$$

$$\iff (rx^2 + (r + s)x + s) + \langle x^2 + 2x\rangle = 1 + \langle x^2 + 2x\rangle$$

Hence, if we let $r = s = 1$, we obtain a solution, and we conclude that the inverse of a is a itself.