Math 4320 — Final Exam

2:00pm–4:30pm, Friday 18th May 2012

Symmetry, as wide or as narrow as you may define its meaning, is one idea by which man through the ages has tried to comprehend and create order, beauty and perfection. Hermann Weyl, *Symmetry*, 1980.

This exam contains eight questions. Choose ONLY FOUR to answer — if you attempt more than four questions, you must indicate which four you would like to be graded. Calculators, cell phones, music players and other electronic devices are not permitted. Notes and books may not be used.

Write your name on all exam booklets. Do not hand in any scratch paper. Unless otherwise indicated, all answers should be justified.

1. (a) State and prove Lagrange's Theorem on subgroups of finite groups.

   (b) Suppose a is an element of a group G. Show that $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ is a subgroup of G.

   (c) Recall that the order n of an element a in a finite group G is the least integer $n \geq 1$ such that $a^n = 1$. Show that $|\langle a \rangle| = n$ and explain why n divides $|G|$.

   13 + 6 +6 = 25 pts

Answer.

(a) Page 156 of Rotman's *A First Course in Abstract Algebra with Applications*, Third Edition.

(b) Page 150.

(c) Proposition 2.74 on page 151 and Corollary 2.85 on page 157.

2. (a) When a group G acts on set X, what are meant by the *orbit* $\mathcal{O}(x)$ and the *stabilizer* G_x of $x \in X$? What formula gives $|G|$ in terms of $|\mathcal{O}(x)|$ and $|G_x|$ when G is finite?

   (b) Show that when a group G acts on set X, the orbits partition X.

   (c) Explain how the Class Equation for a finite group G:

   $$|G| \ = \ |Z(G)| + \sum_i [G : C_G(x_i)]$$

   where in the sum one x_i is selected from each conjugacy class of size at least 2, follows from parts (a) and (b). [*Recall that $Z(G)$ denotes the* center *of G—that is, the elements that commute with all elements of the group—and that $C_G(x_i)$ denotes the centralizer of x_i—that is, all elements of G that commute with x_i.*]

   (3+3+3) + 8 + 8 = 25 pts

Answer.

(a) $\mathcal{O}(x) = \{gx \mid g \in G\}$ and $G_x = \{g \in G \mid gx = x\}$. The formula is $|G| = |\mathcal{O}(x)| \cdot |G_x|$.

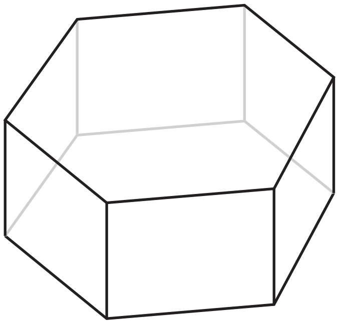
(b) Page 199.

(c) Pages 200–201.

3. (a) Burnside's Lemma gives what formula for the number of orbits of a finite group G acting on a finite set X?

(b) How many ways are there to color the eight faces of a regular hexagonal prism (see below) up to rotational symmetry using the colors red and blue?

5 + 20 = 25 pts



Answer.

(a) $\displaystyle\frac{1}{|G|}\sum_{g\in G} F(g)$, where $F(g) = |\{x \in X \mid gx = x\}|$.

(b) We consider the group of rotational symmetries of the regular hexagonal prism (namely, D_{12}) acting on the set of all possible colorings of the faces of a fixed regular hexagonal prism using the colours red and blue. The number of orbits is the number of different colorings up to rotational symmetry.

The identity fixes all 2^8 colorings. The three π rotations about axes through midpoints of opposite rectangular faces fix 2^5 colorings. The three π rotations about axes through midpoints of opposite vertical edges fix 2^4 colorings. As for the vertical axis through the middle of the prism, the $\pi/3$ and $-\pi/3$ rotations fix 2^3 colorings, the $2\pi/3$ and $-2\pi/3$ fix 2^4 colorings, and the π rotation fixes 2^5 colorings.

So, by Burnside's Lemma, the number of different colorings up to rotational symmetry is

$$\begin{aligned} &\frac{1}{12}\left(2^8 + 3\cdot 2^5 + 3\cdot 2^4 + 2\cdot 2^3 + 2\cdot 2^4 + 2^5\right) \\ &= \frac{2^4}{12}\left(2^4 + 3\cdot 2 + 3 + 1 + 2 + 2\right) \;=\; \frac{4}{3}\cdot 30 \;=\; 40. \end{aligned}$$

4. (a) State and prove the First Isomorphism Theorem for groups.

(b) Show that the index of $\mathrm{SL}_2(\mathbb{F}_q)$ in $\mathrm{GL}_2(\mathbb{F}_q)$ is $q-1$, where q is a prime power and $\mathbb{F}_q$ denotes the finite field with q elements. [*You may assume that the determinant map* $\det : \mathrm{GL}_2(\mathbb{F}_q) \to \mathbb{F}_q \smallsetminus \{0\}$ *is a group homomorphism.*]

18 + 7 = 25 pts

Answer.

(a) Page 180.

(b) The determinant map $\mathrm{GL}_2(\mathbb{F}_q) \to \mathbb{F}_q \smallsetminus \{0\}$ is surjective since for every $a \in \mathbb{F}_q \smallsetminus \{0\}$ we have $\det \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} = a$. And its kernel is $\mathrm{SL}_2(\mathbb{F}_q)$ since $\mathrm{SL}_2(\mathbb{F}_q)$ is the group of all 2×2 matrices with coefficients in $\mathbb{F}_q$ and determinant 1. So the First Isomorphism Theorem tells us that

$$\mathrm{GL}_2(\mathbb{F}_q)/\mathrm{SL}_2(\mathbb{F}_q) \;\cong\; \mathbb{F}_q \smallsetminus \{0\}\,.$$

So the index of $\mathrm{SL}_2(\mathbb{F}_q)$ in $\mathrm{GL}_2(\mathbb{F}_q)$ is

$$|\mathrm{GL}_2(\mathbb{F}_q)/\mathrm{SL}_2(\mathbb{F}_q)| \;=\; |\mathbb{F}_q \smallsetminus \{0\}| \;=\; q-1.$$

5. (a) What is meant by an *ideal* in a commutative ring R?

(b) When is an ideal *prinipal*? What does it mean to say that an integral domain R is a *principal ideal* domain (PID)?

(c) Give, with justification, an example of a non–zero commutative ring that is a PID.

(d) Give, with justification, an example of a commutative ring that is not a PID.

(e) Show that if $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ are ideals in a PID R, then there exists n such that $I_m = I_n$ for all $m > n$.

6 + (2+2) + 4 + 4 + 7 = 25 pts

Answer.

(a) Page 249.

(b) Every ideal is principal. That is, if $I \subseteq R$ is an ideal, then $I = (a) = \{ra \mid r \in R\}$ for some $a \in R$.

(c) $\mathbb{Z}$, $k[x]$ for k a field, any field, $\mathbb{Z}[i]$. See page 260.

(d) $\mathbb{R}[x,y]$ since the ideal (x,y) is not principal: if $(f) = (x,y)$ then $f|x$ and so f is either a non–zero constant polynomial or is rx for some $r \in \mathbb{R}$, but in the former case $(f) = \mathbb{R}[x,y]$ and in the latter case $f \nmid y$.

(e) Let $I = \bigcup_{n=1}^{\infty} I_n$. Then I is an ideal:

- $0 \in I$ since $0 \in I_n$ for all n,
- if $a, b \in I$, then $a, b \in I_n$ for some n, and so $a + b \in I_n \subseteq I$,
- if $a \in I$ and $r \in R$, then $a \in I_n$ for some n, and so $ra \in I_n \subseteq I$.

So as R is a PID, $I = (a)$ for some $a \in I$. But then $a \in I_n$ for some n, and so $I = (a) = I_n$. Therefore $I_m = I_n$ for all $m > n$.

6. (a) Show that the following two characterizations of what it means for a commutative ring R to be a *domain* are equivalent.

   (i) For all $a, b, c \in R$ with $c \neq 0$, if $ca = cb$, then $a = b$.

   (ii) For all $a, b \in R$, if $ab = 0$ then $a = 0$ or $b = 0$.

Recall that a commutative ring R is a *Euclidean ring* if it is a domain and there is a function $\partial : R \setminus 0 \to \mathbb{N}$ such that

- $\partial(f) \leq \partial(fg)$ for all $f, g \in R \setminus 0$, and
- for all $f, g \in R$ with $f \neq 0$, there exists $q, r \in R$ such that $g = qf + r$ and either $r = 0$ or $\partial(r) < \partial(f)$.

(b) Give an example of a *Euclidean ring*. What is ∂ for your example? [*You are not asked to prove that ∂ satisfies the above axioms.*]

(c) Show that if R is a Euclidean ring, then it is a principal ideal domain (PID).

10 + 5 + 10 = 25 pts

Answer.

(a) Page 223.

(b) Page 268.

(c) The zero–idea (0) in r is principal. Suppose $I \subseteq R$ is a non–zero ideal. Let f be an element of $R \setminus 0$ for which $\partial(f)$ is least. Suppose $g \in I$. Then $g = qf + r$ for some $q, r \in R$ with either $r = 0$ or $\partial(r) < \partial(f)$. But then $r = g - qf$ and so $r \in I$ (as I is an ideal). So $r = 0$ else $\partial(r) < \partial(f)$ would be counter to our choice of f. So $f \mid g$ and $g \in (f)$. So $I = (f)$.

7. (a) Recall that a polynomial in $\mathbb{Z}[x]$ is *primitive* when the gcd of its coefficients is 1. Show that the product of two primitive polynomials in $\mathbb{Z}[x]$ is primitive.

(b) State Eisenstein's Criterion for the irreducibility in $\mathbb{Q}[x]$ of a polynomial with integer coefficients.

(c) Show that $f(x) = x^4 + x^3 + x^2 + x + 1$ is irreducible in $\mathbb{Q}[x]$. [*Hint: consider $f(x + 1)$.*]

10 + 6 + 9 = 25 pts

Answer.

(a) Page 283.

(b) Page 288.

(c) $f(x) = \dfrac{x^5 - 1}{x - 1}$, so

$$\begin{aligned} f(x+1) &= \frac{(x+1)^5 - 1}{x} \\ &= \frac{(x^5 + 5x^4 + 10x^3 + 10x^2 + 5x + 1) - 1}{x} \\ &= x^4 + 5x^3 + 10x^2 + 10x + 5 \end{aligned}$$

which is irreducible by Eisenstein's Criterion with the prime concerned being 5. It follows that $f(x)$ is also irreducible in $\mathbb{Q}[x]$, as if $f(x) = g(x)h(x)$ with g and h of lower degree than f, then $g(x+1)h(x+1)$ would be an expression for $f(x+1)$ as a product of two polynomials of lower degree.

8. (a) Suppose k is a field and $I = (p(x))$ where $p(x)$ is a non–constant polynomial in $k[x]$. Show that if $p(x)$ is irreducible in $k[x]$, then $k[x]/I$ is a field. (*You can use facts about primes and irreducibles, provided you quote them correctly.*)

(b) By applying the First Isomorphism Theorem for rings to the homomorphism $\mathbb{R}[x] \to \mathbb{C}$ given by $f(x) \mapsto f(i)$, show that

$$\mathbb{R}[x]/(x^2 + 1) \;\cong\; \mathbb{C}.$$

(c) Show that

$$\mathbb{R}[x]/(x^2 - 2x + 2) \;\cong\; \mathbb{C}.$$

13 + 6 + 6 = 25 pts

Answer.

(a) Page 296–297, (iii) $\implies$ (i).

(b) Example 3.111 on page 296.

(c) As for part (b), but use $f(x) \mapsto f(1 + i)$.

TRR, 12 May 2012