MATH 315 Final

Instructor: Dr. Thomas Bitoun
Name: Yifeng Pan
UCID: 30063828

Winter 2020

1

1.1 Let C_{15} be a cyclic group of order 15. How many subgroups does C_{15} have? List all of them.

Let g be a generator of C_{15}.

The order of every subgroup of C_{15} has to divide 15.

The divisors of 15 are $\{1, 3, 5, 15\}$. So the subgroups of C_{15} can be generated using g^1, g^3, g^5, g^{15}.

The subgroups are:

$$\begin{aligned} C_{15} &= \left\{g^0 = g^{15}, g^1, g^2, \ldots, g^{14}\right\}, \\ C_5 &= \left\{g^0 = g^{3^5}, g^3, g^{3^2}, g^{3^3}, g^{3^4}\right\}, \\ C_3 &= \left\{g^0 = g^{5^3}, g^5, g^{5^2}\right\}, \\ C_1 &= \left\{g^0\right\} \end{aligned}$$

1.2 Give an example of a simple group of order 60. (You do not need to justify your answer for part (ii).)

A_5 is the archetypical simple group, where every simple group of order 60 is isomorphic to A_5.

2 Let p be a prime number.

2.1 Determine the group of group automorphisms of $(\mathbb{Z}/p\mathbb{Z}, +)$.

Let A be the group of group automorphisms of $(\mathbb{Z}/p\mathbb{Z}, +)$.

Let g be a generator of $(\mathbb{Z}/p\mathbb{Z}, +)$.

Since automorphisms are ismorphic homomorphisms, an automorphism of $(\mathbb{Z}/p\mathbb{Z}, +)$ must map g to a generator.

Since p is prime, $(\mathbb{Z}/p\mathbb{Z})$ has $p - 1$ unique generators. Therefore $|A| = p - 1$, and the elements of A would be the unique automorphisms defined by

$$\phi_1(g) = g, \phi_2(g) = g^2, \phi_3(g) = g^3, \ldots, \phi_{p-1}(g) = g^{p-1}$$

where $g^n = \sum_{i=1}^{n} g$.

2.2 Determine the group of ring automorphisms of $\mathbb{Z}/p\mathbb{Z}$, for the ring $\mathbb{Z}/p\mathbb{Z}$ with the usual addition and multiplication of integers modulo p.

Let A be the group of ring automorphisms of $\mathbb{Z}/p\mathbb{Z}$.

Similarly to part (i), we consider the generators of $\mathbb{Z}/p\mathbb{Z}$.

Since every generator of $(\mathbb{Z}/p\mathbb{Z}, \times)$ is a generator of $(\mathbb{Z}/p\mathbb{Z}, +)$, we only have to consider the case for $(\mathbb{Z}/p\mathbb{Z}, \times)$.

Let $\{g_1, g_2, \ldots\}$ be the generators/primative roots of $(\mathbb{Z}/p\mathbb{Z}, \times)$.

Let n be the number of primative roots of $(\mathbb{Z}/p\mathbb{Z}, \times)$.

Then $|A| = n$, and the elements of A would be the unique automorphisms defined by

$$\phi_1(g_1) = g_1, \phi_2(g_1) = g_2, \phi_3(g_1) = g_3, \ldots, \phi_n(g_1) = g_n$$

2.3 Determine the group of automorphisms of the symmetric group S_3 of permutations of the set $\{1, 2, 3\}$.

An automorphism of S_3 would map some permutation of $\{1, 2, 3\}$ to some permutation.

Therefore the group of group automorphisms of S_3 is S_3 itself.

3

3.1 Define the class equation of a finite group G.

Definition 1: (Used in (3.2))
Define an equivalence relation of G such that $a \sim b \iff \exists g \in G, gag^{-1} = b$.

The class equation is the summation of the sizes of the equivalence classes of the above relation.

Definition 2: (Used in (3.3))
Define a group action of G on itself such that $(g, x) \to gxg^{-1}$.

Denote an orbit of this action $C(x)$ as an conjugacy class. Denote an stabilizer subgroup of this action $Z(x)$ as an centralizer.

The class equation is $|G| = \sum |C(x)|$.

3.2 What is the class equation of an abelian group of order 10? Justify your answer.

Using the equivalence relation from above.

Since the binary operation of an abelian group is commutative, $gag^{-1} = b \iff a = b$. Therefore the class equation is $10 = \sum_{i=1}^{10} 1$, since the group has 10 distinct elements.

3.3 Show that there is no group of class equation $10 = 1 + 1 + 1 + 1 + 1 + 5$.

Let G be a group with the class equation $10 = 1 + 1 + 1 + 1 + 1 + 5 = |C_1| + |C_2| + \ldots + |C_6|$.

Since there are 5 conjugacy clases with the size 1, these 5 elements are commutative with every element of G. Therefore the center of G contains these 5 elements.

Now, we find the size of the centralizers using the equlity: $|G| = |C(x)|\,|Z(x)|$.
We get $|Z_1| = |Z_2| = |Z_3| = |Z_4| = |Z_5| = 10, |Z_6| = 2$.

Now, since the center of G is also the intersection of all the centralizers of G, and $|Z_6| = 2$, then order of the center ≤ 2.

But the center contains 5 elements, therefore we have a contradiction, and there exists no such group G. $\square$

4

4.1 Describe the units in the direct product ring $M_2(\mathbb{R}) \times M_2(\mathbb{R})$, where $M_2(\mathbb{R})$ is the ring of 2 by 2 matrices with real coefficients.

To find the units of $R = M_2(\mathbb{R}) \times M_2(\mathbb{R})$, we need to find the elements of R that has a multiplicative inverse.

The multiplicative identity R is (I_2, I_2), where I_2 is the 2 by 2 identity matrix.

The units are therefore: $\{(A, B) | A, B \in M_2(\mathbb{R}), \det(A) \neq 0, \det(B) \neq 0\}$. $\square$

4.2 Is the direct product of groups $\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$ a cyclic group? Justify your answer.

If $\mathbb{Z}/7\mathbb{Z}$ and $\mathbb{Z}/11\mathbb{Z}$ are under multiplication, then their orders would be 6 and 10 respectively. 6 and 10 are not relatively prime, and their lowest common multiple $= 30$.

Therefore a "generator" of $\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$ can only ever cover 30 elements. But $\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$ has $6 * 10 = 60$ elements.
Therefore $\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$ is not a cyclic group under multiplication, since there is no generator for it. $\square$

If $\mathbb{Z}/7\mathbb{Z}$ and $\mathbb{Z}/11\mathbb{Z}$ are under addition, then their orders would be 7 and 11 respectively. 7 and 11 are relatively prime, and their lowest common multiple $= 7 * 11 = 77$.

Let $G = \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$ under addition. We prove $(1, 1)$ is a generator. Since the period of 1 in $\mathbb{Z}/7\mathbb{Z}$ is 7, and the period of 1 in $\mathbb{Z}/11\mathbb{Z}$ is 11, the period of $(1, 1)$ in G is their lowest common multiple 77.

But G only contains 77 elements, so $(1, 1)$ is a generator. **Therefore G under addition is a cyclic group.** $\square$

5

5.1 Show that $Q(x) := 200x^3 - 200x^2 + 200x + 100$ is an irreducible polynomial over the field $\mathbb{Q}$ of rational numbers.

Since $Q(x)$ is of degree 3, if it is reducible, it can be reduced into a polynomial of degree 2 and a polynomial of degree 1, or three polynomials of degree 1. Either way, if $Q(x)$ is reducible in $\mathbb{Q}[x]$, it has an factor in $\mathbb{Q}$.

Suppose $Q(x)$ is reducible in $\mathbb{Q}[x]$. So $\exists x = \frac{a}{b} \in \mathbb{Q}$ such that $200x^3 - 200x^2 + 200x + 100 = 0$. Furthermore, we can assume a/b is in it's irreducible fraction form. (Similarly to the common proof that $\sqrt{2}$ is irrational.)

Now, we prove a and b are both even, and therefore is a reducible fraction.

$$\begin{aligned} 0 &= 200x^3 - 200x^2 + 200x + 100 \\ &= 2a^3b^{-3} - 2a^2b^{-2} + 2ab^{-1} + 1 \\ \text{(since } b \neq 0) \ &= 2a^3 - 2a^2b + 2ab^2 + b^3 \\ \rightarrow b^3 &= -2a^3 + 2a^2b - 2ab^2 \\ &= 2(-a^3 + a^2b - ab^2) \end{aligned}$$

Therefore 2 is a factor of b^3, and therefore 2 is a factor of b. Let $b = 2c$. Now,

$$\begin{aligned} 0 &= 2a^3 - 2a^2b + 2ab^2 + b^3 \\ &= 2a^3 - 4a^2c + 8ac^2 + 8c^3 \\ \rightarrow a^3 &= 2a^2c - 4ac^2 - 4c^3 \\ &= 2(a^2c - 2ac^2 - 2c^3) \end{aligned}$$

Therefore 2 is a factor of a.

Since a and b are both even, a/b is reducible (Contradiction), and there exists no such x.

Therefore $Q(x)$ is not reducible in $\mathbb{Q}[x]$. $\square$

5.2 Compute the sum of the complex roots of $Q(x)$. Justify your answer.

We find the roots of $100(2x^3 - 2x^2 + 2x + 1)$.

All polynomials of degree ≥ 2 are reducible in $\mathbb{C}[x]$.

So $2x^3 - 2x^2 + 2x + 1 = 2(x-a)(x-b)(x-c)$, where $a, b, c \in \mathbb{C}$ are the complex roots of $Q(x)$.

We have

$$\begin{aligned} -abc &= \frac{1}{2} \\ ab + bc + bc &= 1 \\ -c + -b + -a &= 1 \end{aligned}$$

The sum of the roots are therefore -1. $\square$

5.3 Let $P(x)$ be a polynomial in $\mathbb{Z}[x]$ of degree 5 such that $P(1) = 3$ and $P = (x-1)^5$ modulo 3. Show that as a polynomial in $\mathbb{Q}[x]$, $P(x)$ is irreducible.

Suppose $P(x)$ is reducible in $\mathbb{Q}[x]$.

So $\exists ab = P(x)$, such that $a, b \in \mathbb{Z}[x]$, and the degree of a and b are both ≥ 1.
(Multiply the factors in $\mathbb{Q}[x]$ by the lowest common multiple of the coefficients of their denominators to get factors in $\mathbb{Z}[x]$.)

So $3 = P(1) = a(1)b(1)$.

Suppose $a(1) = 3, b(1) = 1$. (Proof for vice versa is simular.)

We have $P = ab = (x-1)^5$ in $\mathbb{F}_3[x]$.

So $a = (x-1)^x$ and $b = (x-1)^y$ in $\mathbb{F}_3[x]$, with $x + y = 5$.

But $b(1) = 1$ in $\mathbb{Z}[x]$, so $(x-1)$ cannot be a factor of b in $\mathbb{F}_3[x]$.

So $a = (x-1)^5$. But the degree of b is by construction ≥ 1, therefore the degree of a plus the degree of $b \geq 6$. Contradiction, since $ab = P$.

Therefore there exists no such factors a, b, and $P(x)$ is irreducible in $\mathbb{Q}[x]$.

6 Let p be a prime number.

6.1 Show that there are $\frac{p(p+1)}{2}$ reducible monic quadratic polynomials over the finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Monic quadratic polynomials are of the form $x^2 + ax + b$, for some $c, d \in \mathbb{F}_p$.

There are p^2 polynomials of this form in $\mathbb{F}_p$.

Since quadratics are of degree 2, the are either irreducible, or can be reduced into two polynomials with degree 1.

Therefore the reducible polynomials are of the form $x^2 + ax + b = (x+c)(x+d) = x^2 + (c+d)x + cd$, for some $c, d \in \mathbb{F}_p$.

The number of distinct reducible polynomials are therefore the number of distinct images of $(x+c)(x+d)$ with $c, d \in \mathbb{F}_p$.

We count:

1. Choose $c \in \mathbb{F}_p$. (p choices)
2. Choose $d \in \mathbb{F}_p, d \neq c$. ($p-1$ choices)
3. The choices for (c, d) are commutative, so we counted everything twice. $(1/2)$
4. Now we add the the number of ways to choose $c, d \in \mathbb{F}_p, c = d$. ($p$ choices).

We have $\frac{p(p-1)}{2} + p = \frac{p^2-p+2p}{2} = \boldsymbol{\frac{p(p+1)}{2}}$. $\square$

6.2 Construct a field of order 49.

$F = \mathbb{F}_7/(x^2+1)$.

Since $x^2 + 1$ has degree 2, if it is reducible, it can be reduced into two polynomials of degree 1, which would imply it has integer roots.

It's easy to check that $x^2 + 1 \neq 0, \forall x \in \{0, 1, 2, 3, 4, 5, 6\} = \mathbb{F}_7$. Therefore $x^2 + 1$ is irreducible in $\mathbb{F}_7$.

Since $x^2 + 1$ is irreducible in $\mathbb{F}_7$, F is a field. [1]

Since $x^2 + 1$ kills all the polynomials of above degree 2 in $\mathbb{F}_7$, all the elements of F are of the form $ax + b, a, b \in \mathbb{F}_7$.

Therefore $|F| = 7^2 = 49$. $\square$

[1] I proved this in Assignment 5, I've provided a copy of the proof on the next page.

6.3 Is there a field F of characteristic p such that F is an infinite set? Prove that F does not exist or give an example.

We know $\mathbb{Z}/2\mathbb{Z}[x]$ is an integral domain.

Define F as a field of fractions over $\mathbb{Z}/2\mathbb{Z}[x]$.

F is a field by construction.

We have to prove F is infinite with a characteristic 2.

Let $[\frac{a}{b}] \in F$, for $a, b \in \mathbb{Z}/2\mathbb{Z}[x], b \neq 0$.

$[\frac{a}{b}] + [\frac{a}{b}] = [\frac{2a}{b}] = [\frac{0}{b}]$, since $2a = 0 \in \mathbb{Z}/2\mathbb{Z}[x]$, where $[\frac{0}{b}]$ is the additive identity in F.

Therefore F has a characteristic of 2.

Now, we construct an infinite subset of F. Let $S = \left\{[\frac{x}{1}], [\frac{x^2}{1}], [\frac{x^3}{1}], [\frac{x^4}{1}], \dots\right\} \subseteq F$.

The elements of S are all distinct equivalence classes, i.e. elements of F, since $x^a 1 \neq x^b 1, \forall a, b \in \mathbb{N}, a \neq b$.

Since S is denumerable, F is not finite. □

Lemma used in (6.2)

Lemma 1. $\mathbb{F}_p[x]/(f(x))$ is a field $\iff$ $f(x)$ is irreducible in $\mathbb{F}_p[x]$.

Proof: Suppose $f(x) \in \mathbb{F}_p[x]$ is irreducible (henceforth refered to as f).

Let $[g] \in \mathbb{F}_p[x]/(f)$, where $g \in \mathbb{F}_p[x] \setminus \{0\}$. We find the inverse of $[g]$.

Since f is irreducible, $\gcd(f, g) = c$ for some constant $c \in \mathbb{F}_p$. Otherwise, c would be a non-constant factor of f.

By Bézout's Identity:
$\exists a, b \in \mathbb{F}_p[x]$, such that $af + bg = 1$. Now,

$$\begin{aligned} [af + bg] &= [1] \\ [a][f] + [b][g] &= [1] \\ [a][0] + [b][g] &= [1] \\ [b][g] &= [1] \end{aligned}$$

Therefore $[b]$ is the multiplicative inverse of $[g]$ in $\mathbb{F}_p[x]/(f)$, where $[1]$ is the multiplicative identity.

Since $\mathbb{F}_p[x]/(f)$ is a quotient ring, and since every element has an inverse, $\mathbb{F}_p[x]/(f)$ is a field.

Now for the logical inverse: Suppose f is reducible. So $\exists$ non-constants $a, b \in F_p[x]$ such that $ab = f$.

We have $[ab] = [f] \to [a][b] = [0]$.

Suppose $[a] = [0]$. So $\exists r \in \mathbb{F}_p[x]$, such that $rf = a$. Now, $ab = f \to rfb = f$, and since we know $\mathbb{F}_p[x]$ is an integral domain, $rb = 0$. But $r \neq 0, b \neq 0$ from construction ($r \neq 0$ because $a \neq 0$) ,so $\mathbb{F}_p[x]$ has non-zero zero divisors. Contradiction.

Therefore $[a] \neq [0]$. Similarly, $[b] \neq [0]$.

Since $[a] \neq [0]$ and $[b] \neq [0]$, $\mathbb{F}_p[x]/(f)$ has non-zero zero divisors, and therefore is not an integral domain, and therefore not a field. □