Math 3GR3 Tutorial Problems

Mike Cummings

Fall 2023

Tutorial 1

Question 1. Recall that an equivalence relation is a relation on a nonempty set that is reflexive, symmetric, and transitive. Explain why the following relations are not equivalence relations.

(a) $x \sim y$ in $\mathbb{R}$ if $x \neq y$

(b) $x \sim y$ in $\mathbb{C}$ if $x \leq y$

(c) Let $\mathrm{Mat}_n(\mathbb{Q})$ denote $n \times n$ matrices with entries in $\mathbb{Q}$. Define $A \sim B$ in $\mathrm{Mat}_n(\mathbb{Q})$ if $\det(AB) < 0$.

Question 2 (Judson Chapter 1, Exercise 29. The projective real line)**.** Define a relation on $\mathbb{R}^2 \setminus \{(0,0)\}$ by letting $(x_1, y_1) \sim (x_2, y_2)$ if there exists a nonzero real number λ such that $(x_1, y_1) = (\lambda x_2, \lambda y_2)$.

(a) Prove that $\sim$ defines an equivalence relation on $\mathbb{R}^2 \setminus \{(0,0)\}$.

(b) What are the corresponding equivalence classes?

Question 3 (Lakins Exercise 6.2.1(c))**.** Compute $\gcd(7776, 16650)$ and find integers x, y such that $7776x + 16650y = \gcd(a, b)$.

Question 4 (Judson 2.4.16)**.** Let a and b be nonzero integers. If there exist integers r and s such that $ar + bs = 1$, show that a and b are relatively prime.

Question 5 (Judson 2.4.24)**.** If $d = \gcd(a, b)$ and $m = \mathrm{lcm}(a, b)$, prove that $dm = |ab|$.

Question 6. Let p be a prime number.

(a) (Lakins Exercise 6.3.6) If i is an integer satisfying $0 < i < p$, show that $\binom{p}{i} \equiv 0 \mod p$. That is, show that p divides $\binom{p}{i}$.

(b) Give an example to show that (a) fails if p is not prime.

(c) (Freshman's dream) Let a and b be integers. Using (a), show that $(a + b)^p \equiv a^p + b^p \mod p$. [Hint: binomial theorem.]

Tutorial 2

Question 7. Course webpage: https://math.mcmaster.ca/~matt/3gr3/index.html.

- Use the Sage cell on the course webpage
- Open online version of the course textbook
- Enter the following commands:

```
a = 11
b = 77115025
gcd(a, b)
>> run cell

# Q: what does the following output give us?
xgcd(a, b)
```

For fun:

```
for g in graphs(4):

    if not g.is_connected():
        continue

    g.show()
    print('\n')
```

Question 8. Which of the following Cayley tables form a group?

(a) [Judson Exercise 3.5.2(a)]

$\circ$	a	b	c	d
a	a	c	d	a
b	b	b	c	d
c	c	d	a	b
d	d	a	b	c

(b)

	e	w	x	y	z
e	e	w	x	y	z
w	w	e	y	z	x
x	x	z	e	w	y
y	y	x	z	e	w
z	z	y	w	x	e

Question 9. Compute the Cayley tables of the following additive groups:

(a) $\mathbb{Z}_4$,

(b) $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Question 10 (Judson Exercise 3.5.7)**.** Let $S = \mathbb{R} \setminus \{-1\}$ and define a binary operation on S by $a * b = a + b + ab$. Prove that $(S, *)$ is an abelian group.

Question 11 (Judson Exercise 3.5.32)**.** Let G be a group with a finite and even number of elements. Show that there exists some *nonidentity* $a \in G$ such that $a^2 = e$.

Tutorial 3

Question 12 (Judson 3.5.17)**.** Give an example of three different groups with 8 elements. Why are the groups different?

Aside: Much of abstract algebra in the 20th century was devoted to the "classification problem", determining exactly how many unique groups with n elements there are, for each n. In the case of finite *simple* groups, this was solved in ∼2004, culminating the work of around 100 authors spanning half a century.

The takeaway is this: questions like the previous question are very difficult in general. Later in the course, we will learn what it means for a group to be simple, and the notion of *isomorphic* groups, that is, when are two groups "the same".

Question 13 (Judson 3.5.47)**.** Prove or disprove: If H and K are subgroups of a group G, then $HK := \{hk \mid h \in H \text{ and } k \in K\}$ is a subgroup of G. What if G is abelian?

Question 14 (Judson 3.5.52)**.** Prove or disprove: Every proper subgroup of a nonabelian group is also nonabelian.

Question 15 (Judson 4.5.26)**.** Prove that $\mathbb{Z}_p$ has no nontrivial subgroups if p is prime.

Question 16 (Judson 4.5.30)**.** Suppose that G is a group and let $a, b \in G$. Prove that if $|a| = m$ and $|b| = n$, with $\gcd(m, n) = 1$, then $\langle a \rangle \cap \langle b \rangle = \{e\}$.

Question 17 (Judson 4.5.34)**.** Let G be an abelian group of order pq where $\gcd(p, q) = 1$. If G contains elements a and b of order p and q respectively, then show that G is cyclic.

Tutorial 4

Question 18. Recall that subgroups of a cyclic group are cyclic.

True or false? Fix an integer $n > 1$. Since $\mathbb{Z}$ is cyclic, so is $U(n)$.

Question 19. Let p be prime and r a positive integer. What are the generators of $\mathbb{Z}_{p^r}$? How many are there?

Question 20. Compute A^{1223} for the permutation $A \in S_9$ given by

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 1 & 4 & 5 & 4 & 7 & 8 & 9 & 6 \end{pmatrix}.$$

Question 21 (Judson 3.5.35)**.** Find all the subgroups of the symmetry group of an equilateral triangle.

Question 22. Let H be a subgroup of a group G and fix some $g \in G$. Show that gHg^{-1} is also a subgroup of G.

$$gHg^{-1} = \{ghg^{-1} \mid h \in H\}.$$

Question 23. Fix a subgroup $H = \{id, \rho_1, \rho_2\}$ of the group of symmetries of the equilateral triangle. Compute $\mu_1 H \mu_1^{-1} = \mu_1 H \mu_1$.

Question 24. Let G be an abelian group of order pq with elements a and b of orders p and q, respectively. If $\gcd(p, q) = 1$, then show that G is cyclic.

Tutorial 5

This was the review session for test 1. We didn't end up going through any of the prepared problems, but they are listed here anyway.

Question 25 (Judson 5.4.9). Does A_8 contain an element of order 26?

Question 26 (Judson 5.4.33). Suppose a permutation α satisfies $\alpha\beta = \beta\alpha$ for all $\beta \in S_n$. Show that α must be the identity.

Question 27 (Judson 5.4.34). If α is even, show that α^{-1} is too. Does the corresponding result hold if α is odd?

Question 28 (Judson 5.4.37). Let r and s be a rotation and reflection in D_n. Show that $srs = r^{-1}$ and that $r^k s = sr^{-k}$.

Question 29 (Judson 5.4.5). Find each of the following sets. Are any of these sets subgroups of S_4?

(a) $A = \{\sigma \in S_4 \mid \sigma(1) = 3\}$
(b) $B = \{\sigma \in S_4 \mid \sigma(2) = 2\}$
(c) $C = \{\sigma \in S_4 \mid \sigma(1) = 3 \text{ and } \sigma(2) = 2\}$

Tutorial 6

Question 30 (Judson 6.5.5). Describe the left and right cosets of

(a) $\langle 3 \rangle$ in $U(8)$,

(b) D_4 in S_4,

(c) A_n in S_n for all n.

Question 31 (Judson 6.5.17). Suppose that $[G : H] = 2$. If a and b are not in H, show that $ab \in H$.

Question 32 (Judson 6.5.16). If $|G| = 2n$, prove that the number of elements of order 2 is odd. Use this result to show that G must contain a subgroup of order 2.

Question 33 (Judson 5.4.5). Write out the elements of the following subset of S_4 (e.g., in permutation notation). Is it a subgroup of S_4?

$$S = \{\sigma \in S_4 \mid \sigma(1) = (3)\}.$$

Tutorial 7

Question 34. Partition the group G of symmetries of a triangle by left cosets of $H = \{e, \mu_1\}$. Recall that the Cayley table for G is as follows.

$\circ$	e	ρ_1	ρ_2	μ_1	μ_2	μ_3
e	e	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	e	μ_3	μ_1	μ_2
ρ_2	ρ_2	e	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	e	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	e	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	e

With this example as motivation, let us review Lemma 6.3.

Lemma 6.3. Let H be a subgroup of G and pick $g_1, g_2 \in G$. The following are equivalent.

(i) $g_1H = g_2H$

(ii) $Hg_1^{-1} = Hg_2^{-1}$

(iii) $g_1H \subset g_2H$

(iv) $g_2 \in g_1H$

(v) $g_1^{-1}g_2 \in H$

For instance, in the above example, $\mu_3H = \rho_1H$ since $\mu_3 \in \rho_1H$.

Question 35 (Judson 6.5.8)**.** Prove that $\mathbb{Q}$ is not isomorphic to $\mathbb{Z}$.

Question 36 (Judson 9.4.7)**.** Show any cyclic group G of order n is isomorphic to $\mathbb{Z}_n$.

Question 37 (Judson 9.4.2)**.** Let G be the subgroup of $\mathbf{GL}_2(\mathbb{R})$ consisting of matrices of the following form.

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

Show that $G \cong \mathbb{C}^*$.

Tutorial 8

Question 38. True or false? Justify your answers.

(a) $U(20) \cong U(24)$.
(b) Any subgroup of S_3 is normal.
(c) A_n is always normal in S_n.
(d) Every subgroup of a cyclic group is normal.
(e) Every group has at least 2 distinct normal subgroups.

Recall: Theorem 10.3. Let N be a subgroup of G. The following are equivalent:

(a) N is normal in G,
(b) $gNg^{-1} = N$,
(c) $gNg^{-1} \subseteq N$.

Question 39. Let $T = \{z \in \mathbb{C}^* \mid |z| = 1\}$ be the multiplicative subgroup of complex numbers lying on the unit circle and let $\mathbb{R}^+$ be the multiplicative group of positive real numbers. Show that $\mathbb{C}^* \cong \mathbb{R}^+ \times T$.

Question 40 (Dummit–Foote 3.1.34)**.** Consider the dihedral group D_n. Fix an integer k dividing n. Show that the cyclic subgroup $\langle r^k \rangle$ is a normal subgroup of D_n.

Question 41. Suppose N is a subgroup of G such that if $g \in G$, then $g^2 \in N$. Show that N is normal.

Question 42. Prove or disprove: if a group G has normal subgroups N and K such that $N \cong K$, then $G/N \cong G/K$.

Tutorial 9

This was the review session for test 2. No questions were prepared.

Tutorial 10

Question 43 (Modified from Judson exercise 11.4.13)**.** Consider the following statement:

$\mathbb{Q}/\mathbb{Z}$ and $\mathbb{Q}$ are isomorphic as groups.

(a) ChatGPT proved this statement as follows. Find the mistake(s).

Proof. To show that $\mathbb{Q}/\mathbb{Z} \cong \mathbb{Q}$ as groups, we need to find a group isomorphism between them. Let's define a map $\phi : \mathbb{Q}/\mathbb{Z} \to \mathbb{Q}$ as follows:

$$\phi\left(\frac{a}{b} + \mathbb{Z}\right) = \frac{a}{b},$$

where $\frac{a}{b} \in \mathbb{Q}$ is a rational number, and we identify it with its coset $\frac{a}{b} + \mathbb{Z}$ in $\mathbb{Q}/\mathbb{Z}$.

First, we need to show that ϕ is well-defined. Suppose $\frac{a}{b} + \mathbb{Z} = \frac{c}{d} + \mathbb{Z}$. This means $ad = bc$. Since b and d are coprime (having no common factors other than 1), it follows that b divides c, say $c = bk$. Now, we have $\frac{a}{b} = \frac{bk}{d}$, and since b and d are coprime, b divides k, say $k = bm$. Thus, $\frac{a}{b} = \frac{b \cdot bm}{d} = \frac{b^2 m}{d}$, which shows that $\frac{a}{b} = \frac{b^2 m}{d} + \mathbb{Z}$. So, the choice of representative does not matter, and ϕ is well-defined.

Next, we need to show that ϕ is a group homomorphism. Let $\frac{a}{b} + \mathbb{Z}$ and $\frac{c}{d} + \mathbb{Z}$ be two elements in $\mathbb{Q}/\mathbb{Z}$. Then,

$$\begin{aligned}
\phi\left(\left(\frac{a}{b} + \mathbb{Z}\right) + \left(\frac{c}{d} + \mathbb{Z}\right)\right) &= \phi\left(\frac{a}{b} + \frac{c}{d} + \mathbb{Z}\right) \\
&= \phi\left(\frac{ad + bc}{bd} + \mathbb{Z}\right) \\
&= \frac{ad + bc}{bd} \\
&= \frac{a}{b} + \frac{c}{d} \\
&= \phi\left(\frac{a}{b} + \mathbb{Z}\right) + \phi\left(\frac{c}{d} + \mathbb{Z}\right).
\end{aligned}$$

This shows that ϕ preserves the group operation.

Now, let's show that ϕ is injective. Suppose $\phi\left(\frac{a}{b}+\mathbb{Z}\right) = \phi\left(\frac{c}{d}+\mathbb{Z}\right)$. This implies $\frac{a}{b} = \frac{c}{d}$, which, in turn, means $ad = bc$. Since b and d are coprime, this forces $a = c$ and $b = d$, so $\frac{a}{b}+\mathbb{Z} = \frac{c}{d}+\mathbb{Z}$. Thus, ϕ is injective.

Finally, let's show that ϕ is surjective. For any $\frac{a}{b} \in \mathbb{Q}$, we have $\phi\left(\frac{a}{b}+\mathbb{Z}\right) = \frac{a}{b}$, so ϕ is surjective.

Since ϕ is a well-defined, injective, and surjective group homomorphism, it is an isomorphism, and we can conclude that $\mathbb{Q}/\mathbb{Z} \cong \mathbb{Q}$ as groups. $\square$

(b) Determine whether the statement is true or false. If it is true, fix ChatGPT's proof to show that they are isomorphic. If it is false, give a proof that they are not isomorphic.

Question 44. Recall that $\mathbb{R}^*$ is a multiplicative group and $\mathbb{R}$ is an additive group. Show that $\mathbb{R}^*/\{\pm 1\} \cong \mathbb{R}$.

Question 45 (Judson 16.6.34)**.** Let p be a prime integer. Prove that the **ring of integers localized at** p, given by

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} \,\middle|\, \gcd(b,p) = 1 \right\},$$

is a ring, and moreover, that it is an integral domain. Determine the characteristic of $\mathbb{Z}_{(p)}$.

Tutorial 11

Question 46. Give an example of...

(a) a noncommutative ring;
(b) a ring without (multiplicative) identity (AKA a rng);
(c) a ring with identity that is not a division ring;
(d) a commutative ring with identity that is not an integral domain;
(e) an integral domain that is not a field.

Question 47. Show that $\mathbb{R}[x]/\langle x^2+1\rangle \cong \mathbb{C}$. *[Hint: recall from linear algebra that if z is a root of a polynomial in $\mathbb{R}[x]$, then so is $\overline{z}$.]*

Question 48 (Judson 16.6.26)**.** Let R be an integral domain. If the only ideals of R are $\{0\}$ and R itself, then show that R is a field.

Question 49. A **principal ideal domain (PID)** is an integral domain D for which every ideal $I \subseteq D$ can be generated by a single element, e.g., there exists some $a \in D$ such that $I = \langle a\rangle$. Show that the integers $\mathbb{Z}$ form a PID.

Think about how you might adapt your argument to show that $\mathbb{R}[x]$ is a PID.

Question 50 (Judson 16.6.27)**.** Let R be a commutative ring. An element a of R is called **nilpotent** if $a^n = 0$ for some positive integer n. Show that the set of all nilpotent elements is an ideal of R.