

# Review Problems for Final Exam

The following review problems are for you to look at as you study for the final exam. Since this worksheet is concerned with REVIEW, there is more group theory represented here than ring theory. However, this is NOT reflective of the emphasis of the two topics on the final exam. The solutions to these problems will be posted on Tuesday, April 20. The final exam is Friday, April 23.

## 1 Examples

The problems in this section are designed to help you ensure that you have a basic familiarity with important examples of groups, rings, fields and division rings.

1. List the subgroups, subrings and ideals of  $\mathbb{Z}$ ,  $\mathbb{Z}/n$  and  $\mathbb{Z}/p$ . Find the automorphisms of  $\mathbb{Z}$ .

The subgroups of  $\mathbb{Z}$  are the sets  $n\mathbb{Z} = \{nk | k \in \mathbb{Z}\}$ . These are also the ideals of  $\mathbb{Z}$ . The only subrings of  $\mathbb{Z}$  are 0 and  $\mathbb{Z}$ . The only subgroups and ideals of  $\mathbb{Z}/n$  are generated by  $m \in \mathbb{Z}/n$  with  $m|n$ . So,  $\mathbb{Z}/p$  has no nontrivial subgroups or ideals (or subrings).

Suppose that  $f : \mathbb{Z} \rightarrow \mathbb{Z}$  is an automorphism. That is, a group isomorphism. Then  $f(1)$  completely determines  $f$  since  $f(k) = f(1 + \dots + 1) = f(1) + \dots + f(1) = kf(1)$ . So we only need to figure out what  $f(1)$  is. Let  $f(1) = a$ . Then the image of  $f$  is  $a\mathbb{Z}$ . This is only onto if  $a = \pm 1$ . That is, there are two automorphisms of  $\mathbb{Z}$ .

If we require that  $f$  is a RING homomorphism (i.e.  $f$  preserves addition, multiplication and  $f(1) = 1$ ), then there is only ONE automorphism.

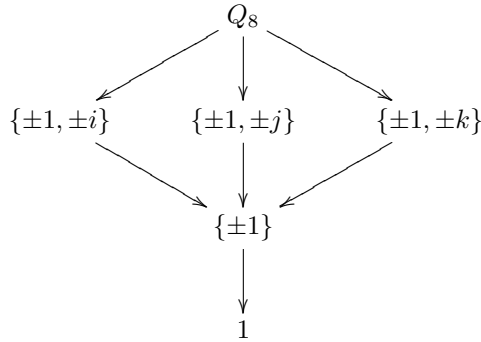
2. Let  $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$  denote the group of quaternions.

- (a) Find the order of each element.

The order of  $\pm i, \pm j, \pm k$  is 4, the order of  $-1$  is 2. The order of 1 is 1 (in any group).

- (b) Find all of the subgroups of  $Q_8$  and draw the subgroup lattice.

There are 8 elements, so it is only possible to have subgroups of order 1, 2, 4, 8. The subgroups of order 1 and 8 are trivial. The only subgroup of order 2 is  $\{1, -1\}$ . The subgroups of order 4 are  $\{1, i, -1, -i\}$  and similarly for  $j$  and  $k$ . Here is the lattice:



- (c) Show that the subgroup  $H = \{1, -1\}$  is a normal subgroup and make a table describing the partition of  $Q_8$  into cosets.

Note that  $H$  is the center of  $Q_8$ . It is easy to show that  $\pm 1$  commutes with every element in  $Q_8$ . Now, choose any other element. That element is one of  $\pm i, \pm j, \pm k$ . None of these elements commutes with the others since  $ij = -ji$ ,  $jk = -kj$  and  $ik = -ki$ . Since  $H = Z(Q_8)$ , it must be normal since the center is always a normal subgroup. You could also prove that directly.

The cosets are  $H, Hi, Hj, Hk$ .

- (d) The quotient group  $Q_8/H$  is isomorphic to either  $\mathbb{Z}/4$  or  $\mathbb{Z}/2 \times \mathbb{Z}/2$ . Which is it?

Check out the order of each element. For example,  $(Hi)^2 = H(-1) = H$ . Every element has order 2. So it must NOT be isomorphic to  $\mathbb{Z}/4$  (which has an element of order 4). The isomorphism is given by:  $\phi(H) = (0, 0)$ ,  $\phi(Hi) = (1, 0)$ ,  $\phi(Hj) = (0, 1)$  and  $\phi(Hk) = (1, 1)$  (there are other possible isomorphisms).

3. Find all subgroups of  $D_n$ . Find the order of each element. Can  $D_n$  be isomorphic to  $\mathbb{Z}/2n$ ? If  $n$  is odd, find all homomorphisms from  $D_n$  to  $\mathbb{Z}/2n$ .

It is easier to first address the order of each element. Let  $D_n = \langle a, b \mid a^n = 1, b^2 = 1, aba = b \rangle$ . Then the order of  $a^k$  is equal to  $n/\gcd(n, k)$  if  $k \mid n$ , and equal to  $n$  otherwise. The order of  $b$  is 2. The order of  $a^k b$  is two since  $a^k b a^k b = b b = 1$ .

The order of  $D_n$  is  $2n$ . Start with  $n = p$ , prime... in that case, the only subgroups are of order 1, 2,  $p$  and  $2p$ . The subgroups of order 1 and  $2p$  are trivial. The subgroups of order 2 are the cyclic subgroups generated by  $a^k b$  for  $0 \leq k < n$ . The subgroup of order  $p$  is the one generated by  $a$ . Note that there are no other subgroups... if  $a^k b$  and  $a^j b$  are in  $H$  with  $k > j$ , then  $a^k b a^j b = a^{k-j} b^2 = a^{k-j}$  is in  $H$ . Since  $p$  is prime, the cyclic subgroup generated by  $a^{k-j}$  is all of  $\langle a \rangle$ , so  $\langle a \rangle \subset H$ . But that means  $|H| > p$ , so  $H = D_n$ .

When  $n$  is not prime the story is much more complicated. One must identify all of the cyclic subgroups of  $\langle a \rangle$  as well as those subgroups we have noted above. For example, when  $n = 4$ , we have cyclic subgroups  $\langle a \rangle$  (of order 4) and  $\langle a^2 \rangle, \langle b \rangle, \langle a^k b \rangle$  (of order 2). In addition, there is a subgroup  $H = \{1, a^2, b, a^2 b\}$  which is isomorphic to the Klein group.

S'pose that  $\phi : D_n \rightarrow \mathbb{Z}/2n$ . Further s'pose that  $\phi(a) \neq 0 \neq \phi(b)$ . Then  $\phi(b) = \phi(aba) = \phi(a) + \phi(b) + \phi(a)$ . That is,  $2\phi(a) = 0$ , proving that the order of  $\phi(a)$  is either 1 or 2. But the order of  $\phi(a)$  divides the order of  $a$ . Since  $n$  is odd,  $|\phi(a)| = 2$  does not divide  $|a| = n$ . So we conclude that  $\phi(a) = 0$  (the unique element of order 1).

Then the two remaining choices are  $\phi(b) = 0$  (the trivial homomorphism) or  $\phi(b) = n$  (use order of  $b$  is 2 in  $D_n$  and order of  $n$  is 2 in  $\mathbb{Z}/2n$ ), both of which work. This proves that  $D_n$  can not be isomorphic to  $\mathbb{Z}/2n$ , even though they have the same order.

There are, of course, many other ways to prove this.

4. Let  $H$  be the subgroup of  $D_6$  generated by  $a^2$ , where  $a$  is the element of order 6 in  $D_6$ . Show that  $H$  is a normal subgroup of  $D_6$ . Find all homomorphisms from  $D_6/H$  to  $\mathbb{Z}/4$ .

It is sufficient to show that  $aHa^{-1} \subset H$  and  $bHb^{-1} \subset H$ , since  $D_6$  is generated by these (recall the HW question using this reduction) (and for those of you worried about the details... this is enough since  $a^{-1} = a^{n-1}$  and  $b^{-1} = b$ ). Now,  $a$  commutes with elements in  $H$ , so  $aHa^{-1} = H$ . Let  $ba^{2k}b \in bHb^{-1}$ . Then  $a^{2k}b = ba^{-2k}$ , so  $ba^{2k}b = bba^{-2k} = a^{-2k} \in H$ . By the normal subgroup test,  $H$  is normal in  $D_6$ .

Note that  $H = \{1, a^2, a^4\}$ . So  $|D_6/H| = 12/3 = 4$ . In fact,  $D_6/H = \{H, Ha, Hb, Hab\}$  which is isomorphic to  $D_2 = K_4$ . In particular, every element has order 2 and the group is abelian. The only homomorphisms are the trivial homomorphism, and

$$f_1(H) = 0, f_1(aH) = 2, f_1(bH) = 2, f_1(abH) = 0$$

and

$$f_2(H) = 0, f_2(aH) = 2, f_2(bH) = 0, f_2(abH) = 2$$

and

$$f_3(H) = 0, f_3(aH) = 0, f_3(bH) = 2, f_3(abH) = 2.$$

5. Let  $\mathbb{H}$  be the ring of quaternions. Find all ideals in  $\mathbb{H}$ . Prove that every element in  $\mathbb{H}$  is a unit.

Well..... to prove that every element is a unit notice that  $(a + bi + cj + dk)(a - bi - cj - dk)$  is a real number. Use this to construct inverses (as we did in class, or in the book). Now, any ideal containing a unit ends up being the whole tamale. So, the only ideals are 0 (no units) and  $\mathbb{H}$  (the whole tamale).

That is,  $\mathbb{H}$  is a simple ring.

6. Find all units in  $\mathbb{Z}/3 \times \mathbb{Z}/4$ . Find all the zero divisors.

Units:  $(1, 1), (1, 3), (2, 1), (2, 3)$ . Zero-divisors:  $(0, 1), (0, 2), (0, 3), (1, 0), (1, 2), (2, 0), (2, 2)$ .

$(0, 0)$  is neither a unit nor a zero divisor. We listed all of the other elements. That is, except for  $(0, 0)$ , every element in this ring is either a unit OR a zero divisor. What other rings have this property?

7. Let  $R$  be a commutative ring and let  $R[x]$  be the ring of polynomials. Let  $r \in R$  and define a map  $ev_r : R[x] \rightarrow R$  by  $ev_r(p(x)) = p(r)$ . For which value(s) of  $r$  is  $ev_r$  a ring homomorphism? A generalized ring homomorphism?

It is always a generalized ring homomorphism. We have:

- $ev_r(f(x) + g(x)) = f(r) + g(r) = ev_r(f(x)) + ev_r(g(x));$
- $ev_r(f(x)g(x)) = f(r)g(r) = ev_r(f(x))ev_r(g(x));$
- $ev_r(1(x)) = 1(r) = 1.$

8. How many elements are there in  $(\mathbb{Z}/3)[x]$ ?

In  $(\mathbb{Z}/3)[x]/\langle x^2 \rangle$ ?

In  $(\mathbb{Z}/3)[x]/\langle x^2 + 1 \rangle$ ? (remove this one)

Show that  $p(x) = x^4 + x$  and  $q(x) = x^2 + x$  determine the same function in  $(\mathbb{Z}/3)[x]$ .

There are infinitely many elements in  $\mathbb{Z}/3[x]$  (for example,  $x^n$  for each  $n$ ). There are 9 elements of  $\mathbb{Z}/3[x]/x^2$ . Any polynomial in  $\mathbb{Z}/3[x]/x^2$  is of the form  $a + bx$ . There are three choices for what  $a$  can be and three choices for what  $b$  can be. There are also only 9 elements of  $\mathbb{Z}/3[x]/x^2 + 1$ ... but we didn't really talk enough about polynomial rings for you to know this (I'll remove this from the review sheet). For the last part, just check that  $p(0) = q(0)$ ,  $p(1) = q(1)$  and  $p(2) = q(2)$ .

## 2 Problem solving

The following problems are designed to help you practice important problem solving skills. Most problems that you are asked to solve are either direct applications of important Theorems or other concepts, or else a test of your ability to synthesize new definitions and apply them to what you already know.

1. Define a binary relation on  $\mathbb{R}^3$  by

$$(a, b, c) \cdot (a', b', c') = (a + a', b + b', c + c' + ab').$$

Let  $H$  denote  $\mathbb{R}^3$  equipped with this binary relation. This is a group, called the **Heisenberg group**.

- (a) Find the identity in  $H$  and find the inverse of  $(a, b, c)$ .

The identity element is  $(0, 0, 0)$ . The inverse is  $(-a, -b, -c + ab)$ .

- (b) Is  $A = \{(a, b, c) \in H \mid b = 0, c = 0\}$  a subgroup of  $H$ ?

Yup. It contains the unit  $(0, 0, 0)$ . It is closed under the group operation since  $(a, 0, 0) + (a', 0, 0) = (a + a', 0, 0)$ . It contains inverses since the inverse of  $(a, 0, 0)$  is just  $(-a, 0, 0)$ .

- (c) Is  $K = \{(a, b, c) \in H \mid c = 0\}$  a subgroup of  $H$ ?

Nope. It's not closed.

- (d) Consider the function  $\alpha : \mathbb{R} \rightarrow H$  defined by

$$\alpha(t) = (t, t, t^2/2).$$

View  $\mathbb{R}$  as a group under addition. Is  $\alpha$  a group homomorphism?

Yup.

$$\alpha(s+t) = (s+t, s+t, (s+t)^2/2) = (s+t, s+t, s^2/2+t^2/2+st) = (s, s, s^2/2) \cdot (t, t, t^2/2) = \alpha(s) \cdot \alpha(t).$$

2. A subgroup  $N$  of  $G$  is called a characteristic subgroup if  $\phi(N) = N$  for all isomorphisms  $G \rightarrow G$  (aka automorphisms). Prove that the commutator subgroup is characteristic.

Recall that a subgroup  $H$  of a group  $G$  is contained in the commutator  $G'$  if and only if  $G/H$  is abelian and  $H$  is normal in  $G$ .

You have a theorem that tells you that  $H \leq G'$  iff  $H \triangleleft G$  and  $G/H$  is abelian. So we show that  $\phi(G')$  is normal in  $G$  (easy) and that  $G/\phi(G')$  is abelian. For any  $a \in G$ , let  $a\phi(g)a^{-1} \in a\phi(G')a^{-1}$  with  $g \in G'$ . Since  $\phi$  is onto,  $a = \phi(b)$  for some  $b \in G$ . Then  $a\phi(g)a^{-1} = \phi(bgb^{-1})$ . But  $G'$  is already normal, so  $bgb^{-1} \in G'$ . That is,  $\phi(bgb^{-1}) \in \phi(G')$ . By the normal subgroup test, and since  $a$  was arbitrary,  $\phi(G')$  is normal in  $G$ . Now, consider  $\phi(G')a\phi(G')b = \phi(G')ab$ . Then  $\phi(G')ab = \phi(G')ba$  iff

$ab(ba)^{-1} = aba^{-1}b^{-1} \in \phi(G')$ . Since  $\phi$  is onto, write  $a = \phi(x)$  and  $b = \phi(y)$ . Then  $aba^{-1}b^{-1} = \phi(x)\phi(y)\phi(x)^{-1}\phi(y)^{-1} = \phi(xy x^{-1}y^{-1}) \in \phi(G')$ . That is,  $G/\phi(G')$  is abelian.

So  $\phi(G') \subset G'$ .

Now,  $G' \subset \phi(G')$  since  $\phi$  is onto so  $aba^{-1}b^{-1} = \phi(c)\phi(d)\phi(c)^{-1}\phi(d)^{-1} = \phi(cdc^{-1}d^{-1})$ . The commutator  $G'$  is generated by these elements.

Thus,  $G' = \phi(G')$ .

3. Let  $\langle a \rangle$  be a cyclic group of order  $n$ .

- (a) State the Fundamental Theorem of Cyclic Subgroups.
- (b) How many subgroups of order  $k$  does  $\langle a \rangle$  have if  $k$  divides  $n$ ? What if  $k$  does not divide  $n$ ?

It's immediate from the theorem that there is EXACTLY one subgroup of order  $n/m = k$ . If  $k$  does not divide  $n$ , there is no subgroup of order  $k$  (by Lagrange, or the special case in the Fundamental theorem for cyclic subgroups).

- (c) If  $H \leq \langle a \rangle$ , show that  $H \triangleleft \langle a \rangle$ . Describe the group  $\langle a \rangle/H$ ? What is its order? What is the group structure?

The only subgroups of a cyclic group are again cyclic. So, the elements of  $H$  commute with the elements of  $\langle a \rangle$  and  $H$  must be normal. If  $G$  is cyclic, then so is  $G/H$  (which describes the group and tells you it's group structure). The order is given by the Lagrange theorem. If  $|\langle a \rangle| = n$  is finite, then  $|\langle a \rangle/H| = n/|H|$ . If  $\langle a \rangle$  is infinite, then it is isomorphic to  $\mathbb{Z}$ . The order of  $\mathbb{Z}/m\mathbb{Z}$  is given by  $m$  if  $H = m\mathbb{Z}$ .

- (d) If the only subgroups of  $\langle a \rangle$  are the trivial subgroup, the whole group, and a group of order 7, what's  $n$ ?

If  $|a| = n$ , then there is a (unique) subgroup of order  $k$  for every  $k$  which divides  $n$ . This problem is asking us to find a number whose only proper divisor is 7. We find  $n = 7^2$ .

4. State the cycle decomposition theorem.

- (a) Given a cycle  $\alpha = (a b c)$  of order 3, find a way to compute  $\alpha^n$  for all  $n \in \mathbb{Z}$ .

Well,  $\alpha^3 = 1 \dots$  so  $\alpha^n = (\alpha)^3 q \alpha^r = \alpha^r$  where  $n = 3q + r$  and  $0 \leq r \leq 3$ .

- (b) Find the orders of the elements in  $A_5$ .

The even cycles have orders 1, 3, 5. There are also elements which are the product of two disjoint transpositions of order 2. We could also have an element of order 9 or 15 or 25 if we could find two disjoint 3-cycles in  $A_5$  or a disjoint 3-cycle and a disjoint 5-cycle in  $A_5$  or

disjoint 5-cycles. But we can't since  $A_5$  involves permutations on 5 elements only (in the cases I mentioned there must be overlap).

- (c) Show that  $A_5$  has no element of order 15.

The only way to get an element of order 15 is to take a (disjoint) product of a 3 cycle and a 5 cycle... but you can't have these in  $A_5$ ... see above.

- (d) Show that any normal subgroup of  $A_5$  must contain all of the elements of order 3 and order 5. (this completes a significant portion of the proof that  $A_5$  is simple)

This is the "challenge problem" portion of the review. It is ok not to be able to solve it, but it is a good exercise for thinking about symmetric groups and even permutations.

Here's a sketch of how to show that  $A_5$  contains all the three cycles: First, show that any normal subgroup must contain at least ONE 3-cycle. There are lots of cases here... but the idea is that if your normal subgroup contains ANY non-trivial element, then you can use closure and conjugation to get a three cycle. Next, show that any three cycle can be obtained from a given three cycle by conjugation. That is, given a three cycle like  $(1\ 2\ 3)$  and another three cycle like  $(a\ b\ c)$  you can find an element  $\sigma$  of  $A_5$  with

$$\sigma^{-1}(1\ 2\ 3)\sigma = (a\ b\ c).$$

There are many cases to this, I will try to find a short solution and post it later. Once you have done that, since  $\sigma^{-1}H\sigma \leq H$ , you've shown that  $H$  contains all the three cycles.

I \*think\* you can take a similar approach to the five cycles. Stay tuned.

5. State the (first) isomorphism theorem for groups, and compare it to the (first) isomorphism theorem for rings.

The first isomorphism theorem for groups states that if  $\phi : G \rightarrow H$  is a group homomorphism, then  $G/\ker\phi \cong im\phi$ . To get the one for rings, you just need a ring homomorphism.

- (a) Can you use the second and third isomorphism theorem for rings to state and prove second and third isomorphism theorems for groups?

The second isomorphism theorem says that if  $S$  is a subring of  $R$  and  $A$  is an ideal of  $R$  then  $S + A/S \cong S/A \cap S$ . For groups, just replace subring by subgroup and ideal by normal subgroup.

- (b) Suppose that  $k$  divides  $n$  and consider  $[k]_n \in \mathbb{Z}/n$ . Show that  $\mathbb{Z}/\langle [k]_n \rangle \cong \mathbb{Z}/k$ .

Use the first isomorphism theorem... use  $\phi([r]_n) = [r]_k$ . This is onto. This is a ring homomorphism. The kernel is anything divisible by  $k$  in  $\mathbb{Z}/n$ .

6. Let  $R$  be a ring with unity  $1_R$ . Prove: If  $\langle 1_R \rangle$  (the subRING generated by  $1_R$ ) has infinite order, then  $\text{char}(R) = 0$ . If  $\langle 1_R \rangle$  (the subRING generated by  $1_R$ ) has order  $n$  then  $\text{char}(R) = n$ .

Here's the finite case.... let  $r \in R$  and look at  $nr$ . Then  $nr = (n1)r = 0r = 0$  since  $n1 = 0$  follows from the order  $|\langle 1 \rangle| = n$ .