Solutions to Final Exam

Math 401

1. Recall that a group G is called *cyclic* if there is an element $g \in G$ such that every element of G is a power of g:

$$G = \{1, g^{\pm 1}, g^{\pm 2}, g^{\pm 3}, \dots\}.$$

(a) Show that if G is cyclic and H is a subgroup of G then H is cyclic. Hint: Let k be the least positive integer such that $g^k \in H$. If g^l is any other element of H then $k \mid l$; otherwise by long division we can write $l = qk + r$ for some $0 < r < k$, so...

Solution: Following the hint, let k be the least positive integer such that $g^k \in H$. If g^l is any other element of H then $k \mid l$; otherwise by long division we can write $l = qk + r$ for some $0 < r < k$, but then $g^r = g^l \cdot (g^k)^{-q}$ is in H, contradicting the minimality of k. Thus every element of H is a power of g^k, so H is cyclic.

(b) Consider a Rubik's cube. You might hope there is some clever sequence of moves such that if you take any mixed-up cube and make this sequence of moves over and over, you will eventually get to the "solved" position, no matter where you started. Show that this is not the case by observing that the symmetry group G of the Rubik's cube contains a copy of $\mathbb{Z}_4 \times \mathbb{Z}_4$, given by rotating the top and the bottom, and this is not a cyclic group.*

Solution: Suppose on the contrary that there were such a sequence of moves $g = g_1 g_2 \cdots g_k \in G$. Then we could get from the "solved" position to any mixed-up position by some power g^{-m}, so G would be cyclic. But the (injective) map $\mathbb{Z}_4 \times \mathbb{Z}_4 \to G$ which sends (a, b) to "rotate the top through a quarter-turns and the bottom through b quarter-turns" is a homomorphism, since rotating the top commutes with rotating the bottom. Thus G has a subgroup that is not cyclic − indeed, if $\mathbb{Z}_4 \times \mathbb{Z}_4$ were cyclic then it would have an element of order 16, but in fact all its elements have order dividing 4. Thus G is not cyclic.

You can also see that G is not cyclic by observing that it is not abelian: rotating the top does not commute with rotating the left side, for example; but this is harder to see without a cube in hand.

The Rubik's cube group is actually very far from being cyclic: its order is $2^{27} 3^{14} 5^3 7^2 11 \approx 4.3 \times 10^{19}$, but the largest cyclic subgroup has order 1260.

*There is an algorithm for solving the Rubik's cube, but it is not as simple as "make this sequence of moves over and over."

2. Let S_n denote the symmetric group on n letters.

(a) Show that an m-cycle $(a_1\, a_2\, \cdots\, a_m)$ is an even permutation if and only if m is odd. Hint: The point is just to remember how to factor σ as a product of transpositions.

Solution: We have

$$(a_1\ a_2\ \cdots\ a_m) = (a_1\ a_m) \cdots (a_1\ a_3)(a_1\ a_2),$$

as we saw in class, or alternatively,

$$(a_1\ a_2\ \cdots\ a_m) = (a_1\ a_2)(a_2\ a_3) \cdots (a_{m-1}\ a_m).$$

Either way this is a product of $m-1$ transpositions, and $m-1$ is even if and only if m is odd.

(b) Let $A_n \subset S_n$ be the subgroup of even permutations; then the order of A_n is half that of S_n. Why?

Solution: Fix a transposition τ. I claim that there are only two cosets of A_n in S_n: the even permutations A_n and the odd permutations τA_n. Indeed, suppose that σ is odd; then we can write $\sigma = \tau \cdot \tau\sigma$, and $\tau\sigma$ is even, so $\sigma \in \tau A_n$.

(c) List the 12 elements of A_4, in cycle notation.

Solution: By part (a) we can skip the 2-cycles and the 4-cycles, which leaves the identity, the 3-cycles, and the products of two 2-cycles:

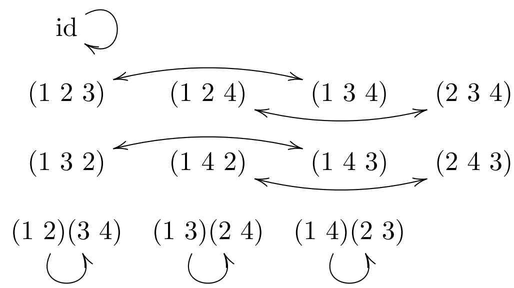
$$\begin{array}{cccc}
\mathrm{id} & & & \\
(1\ 2\ 3) & (1\ 2\ 4) & (1\ 3\ 4) & (2\ 3\ 4) \\
(1\ 3\ 2) & (1\ 4\ 2) & (1\ 4\ 3) & (2\ 4\ 3) \\
(1\ 2)(3\ 4) & (1\ 3)(2\ 4) & (1\ 4)(2\ 3) &
\end{array}$$

(d) Let A_4 act on itself by conjugation. How many orbits are there? How many elements are in each orbit? Hint: To save time, it is enough to see how $(1\ 2)(3\ 4)$, $(1\ 3)(2\ 4)$, and $(1\ 4)(2\ 3)$ act on the 3-cycles, and how $(1\ 2\ 3)$ acts on the products of 2-cycles; then note that conjugation preserves cycle type, and there is no orbit of order eight (why?), so the orbits can't get any bigger than what you've already found at this point.

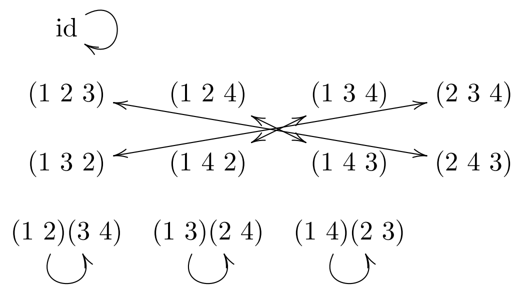
Solution: Conjugating by $(1\ 2)(3\ 4)$ acts as follows:

$$\begin{tikzcd}
\mathrm{id} \arrow[loop right] & & & \\
(1\ 2\ 3) \arrow[dr, leftrightarrow] & (1\ 2\ 4) \arrow[dl, leftrightarrow] & (1\ 3\ 4) \arrow[dr, leftrightarrow] & (2\ 3\ 4) \arrow[dl, leftrightarrow] \\
(1\ 3\ 2) & (1\ 4\ 2) & (1\ 4\ 3) & (2\ 4\ 3) \\
(1\ 2)(3\ 4) \arrow[loop below] & (1\ 3)(2\ 4) \arrow[loop below] & (1\ 4)(2\ 3) \arrow[loop below] &
\end{tikzcd}$$

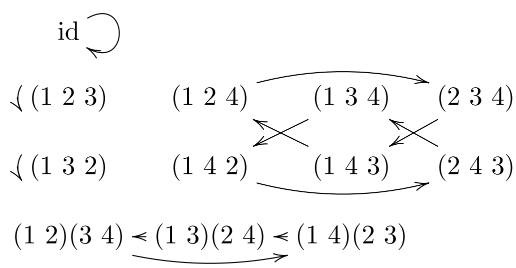
Conjugating by (1 3)(2 4) acts as follows:



Conjugating by (1 4)(2 3) acts as follows:



Conjugating by (1 2 3) acts as follows:



Thus there are at most four orbits:

$$
\begin{gathered}
\{\ \mathrm{id}\ \} \\
\{\ (1\ 2\ 3),\ (1\ 3\ 4),\ (1\ 4\ 2),\ (2\ 4\ 3)\ \} \\
\{\ (1\ 2\ 4),\ (2\ 3\ 4),\ (1\ 3\ 2),\ (1\ 4\ 3)\ \} \\
\{\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\ \}.
\end{gathered}
$$

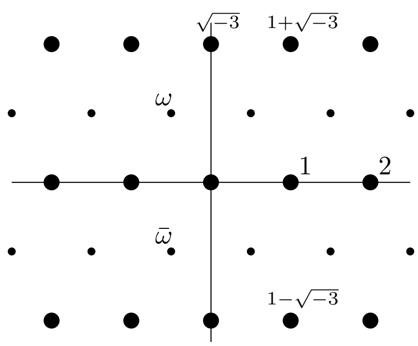
Now we might worry that one of the other seven 3-cycles will connect up two or more of these orbits to make a bigger one. But conjugation preserves cycle type, that is, it cannot turn a 3-cycle into a product of two 2-cycles, so the worst that could happen is that the two middle orbits (of four 3-cycles each) might become one. But by the orbit-stabilizer theorem, the order of an orbit divides the order of the group, and 8 does not divide 12, so these two orbits will not become one big one.

3. Let R be a ring and S a subring. Show that if I is an ideal of R then $J = I \cap S$ is an ideal of S. Show that if I is a prime ideal of R then J is a prime ideal of S.

Solution: First we argue that J is an ideal. Let $j \in J$ and $s \in S$ be given. Then $j \in S$, so $sj \in S$ because S is a subring. And $s \in R$ and $j \in I$, so $sj \in I$ because I is an ideal. Thus $sj \in I \cap S = J$; so J is an ideal of S.

Next we suppose that I is prime – that is, for all $a, b \in R$ we have $ab \in I \Rightarrow a \in I$ or $b \in I$ – and we argue that J is prime. Let $c, d \in S$ be given, and suppose that $cd \in J$; then $cd \in I$, so $c \in I$ or $d \in I$, and still $c, d \in S$, so $c \in I \cap S = J$ or $d \in I \cap S = J$. Thus J is a prime ideal of S.

4. Let $S = \mathbb{Z}[\sqrt{-3}]$, and let $R = \mathbb{Z}[\omega]$, where $\omega = e^{2\pi i/3} = \frac{-1+\sqrt{-3}}{2}$ is a cube root of unity. Observe that $\sqrt{-3} = 2\omega + 1$, so S is a subring of R, and that both are subrings of $\mathbb{C}$ and thus in particular integral domains. Here is a picture of R, with the subring S shown in heavier dots:



(a) Observe that if $z = a + b\sqrt{-3} \in S$ then $|z|^2 = a^2 + 3b^2$, which is a non-negative integer for all $a, b \in \mathbb{Z}$. Conclude that z is a unit in S if and only if $|z| = 1$. List the units in S. Hint: There are two.

Solution: It is clear that $a^2 + 3b^2$ is a non-negative integer.

If z is a unit then there is a $w \in R$ such that $zw = 1$, so $|z|^2|w|^2 = 1$, and since $|z|^2$ and $|w|^2$ are both non-negative integers this implies that $|z|^2 = 1$. Conversely, if $|z|^2 = 1$ then $z\bar{z} = 1$, so $\bar{z} = a - b\sqrt{-3} \in S$ is an inverse for z, so z is a unit.

From the picture we see that the only elements $z \in R$ with $|z| = 1$ are ± 1.

(b) Observe that if $z = a + b\omega \in R$ then $|z|^2 = a^2 - ab + b^2$, which is a non-negative integer for all $a, b \in \mathbb{Z}$: non-negative because it's $|z|^2$, and an integer because it's $a^2 - ab + b^2$. Conclude that z is a unit in R if and only if $|z| = 1$. List the units in R. Hint: There are six.

Solution: If $z = a + b\omega$ then

$$|z|^2 = z\bar{z} = (a + b\omega)(a + b\bar{\omega}) = a^2 + ab(\omega + \bar{\omega}) + b^2\omega\bar{\omega} = a^2 - ab + b^2$$

as claimed. Or if you prefer, $z = (a - \frac{b}{2}) + \frac{b\sqrt{-3}}{2}$, so

$$|z|^2 = (a - \tfrac{b}{2})^2 + \tfrac{3b^2}{4} = a^2 - ab + b^2.$$

Thus $|z|^2$ is a non-negative integer by the argument in the statement of the problem.

The argument that z is a unit if and only if $|z|^2 = 1$ is the same as in part (a), except that it is less obvious that $\bar{z} \in S$ for $z = a + b\omega \in S$. But we can see this from the picture – it is symmetric under reflecting top-to-bottom – or we can write $\bar{\omega} = -1 - \omega$, so $\bar{z} = (a - b) - b\omega$ which is indeed in S.

From the picture we find six points on the unit circle: ± 1 and $\frac{\pm 1 \pm \sqrt{-3}}{2}$.

(c) Show that 2 is irreducible in S. Hint: Argue that there is no $z \in S$ with $|z|^2 = 2$. Thus if $2 = zw$ then...

Solution: There are no $a, b \in \mathbb{Z}$ with $a^2 + 3b^2 = 2$: indeed, if $b \neq 0$ then $a^2 + 3b^2 \geq 3$, so we must have $b = 0$, but then $a^2 = 2$ which is impossible. Thus there is no $z \in S$ with $|z|^2 = 2$.

Now if $2 = z \cdot w$ then we have $4 = |z|^2|w|^2$, so either $|z|^2 = 1$ and $|w|^2 = 4$, so z is a unit, or $|z|^2 = |w|^2 = 2$, which we just saw is impossible, or $|z|^2 = 4$ and $|w|^2 = 1$, so w is a unit. Thus 2 is irreducible in S.

(d) Observe that $4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$. Conclude that 2 is not prime in S.

Solution: We have $2 \mid 4 = (1 + \sqrt{-3})(1 - \sqrt{-3})$, but clearly $1 \pm \sqrt{-3}$ are not of the form $2(a + b\sqrt{-3})$, that is, $2 \nmid 1 \pm \sqrt{-3}$.

(e) I was going to ask you to show that 2 is prime (and hence irreducible) in R, but this turns out to be a pain.

Solution: On the one hand you can make a high-tech argument: ω is a root of $x^2 + x + 1 \in \mathbb{Z}[x]$, so $R \cong \mathbb{Z}[x]/(x^2 + x + 1)$, so $R/(2) \cong \mathbb{Z}_2[x]/(x^2 + x + 1)$, and $x^2 + x + 1$ is irreducible in $\mathbb{Z}_2[x]$, so this is a field. But arguing that $R \cong \mathbb{Z}[x]/(x^2 + x + 1)$ requires some care because $\mathbb{Z}$ is not a field; and you have to remember the day in lecture when we showed that the kernel of a map to a field is a prime ideal, and apply this to $R \to R/(2)$.

On the other hand you can make a low-tech argument, fiddling with coefficients for a long time to show that if $2 \nmid z$ and $2 \nmid w$ then $2 \nmid zw$.

On the third hand you could show that there are no $z \in R$ with $|z|^2 = 2$, so 2 is irreducible in R, and then prove that R has a division algorithm, so irreducible implies prime.

(f) Show that the ideals generated by 2 and $1 - \sqrt{-3}$ in R are the same, but that the ideals they generate in S are different. Hint: Recall from homework that $(a) = (b)$ if and only if there is a unit u such that $a = ub$.

Warning: Consider writing $(2)_R$ and $(2)_S$ rather than just (2) to avoid confusion.

Solution: We know that $-\omega = \frac{1-\sqrt{-3}}{2}$ is a unit in R, so we have $1-\sqrt{-3} = -2\omega$, so $(1-\sqrt{-3})_R = (2)_R$ by the homework problem recalled in the hint. In S however, $1-\sqrt{-3}$ is not a multiple of 2, because its coefficients are odd, so $1-\sqrt{-3} \notin (2)_S$ and thus $(1-\sqrt{-3})_S \neq (2)_S$.

(g) Let $I = (2)_R \subset R$ and $J = I \cap S$. Show that $J = (2, 1-\sqrt{-3})_S$, and that this is not a principal ideal. Hint: It is clear that $2 \in I \cap S$ and $1-\sqrt{-3} \in I \cap S$; for the reverse containment, note that a general element of I is of the form $2(a+b\omega)$, and multiply that out.

Solution: Clearly $2 \in J$, and we just saw that $1-\sqrt{-3} \in I$, so it is in $J = I \cap S$ as well. For the reverse containment, a general element of I is of the form

$$2a + 2b\omega = 2a + b(-1+\sqrt{-3}) = a \cdot 2 - b \cdot (1-\sqrt{-3})$$

for $a, b \in \mathbb{Z}$, and this is in $(2, 1-\sqrt{-3})_S$.

Suppose we could write $J = (z)_S$ for some $z \in S$. We have $2 \in J$, so $z = 2s$ for some $s \in S$; but 2 is irreducible in S, so its only factorizations are $2 \cdot 1$ and $(-2) \cdot (-1)$, so $z = \pm 1$ or ± 2. We have $1-\sqrt{-3} \in J$, so $1-\sqrt{-3} = zs'$ for some $s' \in S$, which rules out $z = \pm 2$. But we also have $z \in I = (2)_R$, so $z = 2r$ for some $r \in R$, which rules out $z = \pm 1$. Thus J is not principal.