Solutions to Final Exam

Math 401

1. (20 points) Lagrange's theorem states that if H is a subgroup of a finite group G then $|H|$ divides $|G|$. You might imagine that for every number k dividing $|G|$ there is necessarily a subgroup of order k, but this is not true, as we will now see.

Let G be the group of rotations of the tetrahedron or, if you prefer, the alternating group $A_4 \subset S_4$. We have seen that these are isomorphic, and that $|G| = 12$.

(a) How many elements does G have of order 1? 2? 3? 4? 6? 12? (Hint: your answers should add up to 12.)

Solution: It has one element of order 1: the identity. It has three elements of order 2: for each pair of opposite edges, the the 180°-rotation about the line joining their midpoints. It has eight elements of order 3: for each of the four vertices there are two the 120°-rotations, one clockwise and one counterclockwise. This accounts for all 12 elements, so there are no elements of order 4, 6, or 12.

If you prefer to work with A_4, the three elements of order 2 are

$$(1\ 2)(3\ 4) \qquad (1\ 3)(2\ 4) \qquad (1\ 4)(2\ 3)$$

and the eight elements of order 3 are

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

(b) Show that G has subgroups of order 2 and 3.

Solution: Take the cyclic subgroup generated by any element of order 2 or 3.

(c) Show that G has a subgroup of order 4. (Hint: It appeared in the last homework.)

Solution: Take the subgroup consisting of the identity and the three elements of order 2. This appeared on the last homework as the stabilizer of a pair of opposite edges.

(d) Show that G has no subgroup of order 6. (Hint: Quote the result of the next problem. How many elements of order 3 does G have?)

Solution: By problem 2, a subgroup of order 6 would contain every element of order 3; but there are eight of these, which is too many.

2. (10 points) Let G be a group of order $2n$ and H a subgroup of order n, that is, a subgroup of index 2. Show that any element $g \in G$ of order 3 must be contained in H. (Hint: Consider the cosets H, gH, and g^2H. Can they all be disjoint from one another?)

Solution: The cosets H, gH, and g^2H each n elements, so they cannot all be disjoint from one another; otherwise G would have at least $3n$ elements. If $H \cap gH \neq \emptyset$ then $H = gH$, so $g \in H$. If $H \cap g^2H \neq \emptyset$ then $H = g^2H$, so $g^2 \in H$, but $g^2 = g^{-1}$ and H is a subgroup, so $g \in H$. If $gH \cap g^2H \neq \emptyset$ then $gH = g^2H$, so $H = gH$, so again $g \in H$.

3. (20 points) Let p be a prime number.

(a) Fill in the blank: $GL_2(\mathbb{Z}_p)$ is the group of 2×2 matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $a, b, c, d \in \mathbb{Z}_p$, such that ________.

Solution: $ad - bc \neq 0$.

(b) Let $GL_2(\mathbb{Z}_p)$ act on the set of column vectors $\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right)$, where $x, y \in \mathbb{Z}_p$, by left multiplication. How many elements are in this set? How many are in the orbit of $\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$? Are there any other orbits?

Solution: There are p^2 elements in the set. The orbit of $\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$ is everything other than $\left(\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right)$: if $x \neq 0$ then $\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right) = \left(\begin{smallmatrix} x & 0 \\ y & x^{-1} \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$, and if $y \neq 0$ then $\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right) = \left(\begin{smallmatrix} x & y^{-1} \\ y & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$. There are $p^2 - 1$ elements in this orbit. The other orbit consists of the single element $\left(\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right)$.

(c) Find the stabilizer of $\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$. What is its order?

Solution: Suppose that $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$. Then $a = 1$ and $c = 0$, so the requirement $ad - bc \neq 0$ becomes $d \neq 0$. Thus the stabilizer is the subgroup of matrices of the form $\left(\begin{smallmatrix} 1 & b \\ 0 & d \end{smallmatrix}\right)$, where b is arbitrary and $d \neq 0$. There are p choices for b and $p - 1$ choices for d, so this subgroup has order $p(p - 1)$.

(d) What is the order of $GL_2(\mathbb{Z}_p)$?

Solution: The order of the group is the order of the stabilizer of $\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$ times the order of its orbit: $p(p-1)(p^2-1)$ (This agrees with the homework problem in which we saw that $GL_2(\mathbb{Z}_2) \cong S_6$.)

4. (15 points)

(a) Let R be a commutative ring and $I, J \subset R$ be ideals. Define

$$IJ = \left\{ \, i_1 j_1 + \cdots + i_n j_n \;\middle|\; i_k \in I, j_k \in J \right\}.$$

Show that IJ is an ideal.

Solution: Clearly IJ is closed under addition, so we need to show that it is closed under multiplication by an arbitrary element $r \in R$. Let $i_1 j_1 + \cdots + i_n j_n \in IJ$ be given. For each k we have $ri_k \in I$ because I is an ideal. Thus

$$r(i_1 j_1 + \cdots i_n j_n) = (ri_1) j_1 + \cdots + (ri_n) j_n$$

is in IJ.

(b) Show that if $I = (a)$ and $J = (b)$ then $IJ = (ab)$.

Solution: Clearly $ab \in IJ$, so $(ab) \subset IJ$. Conversely, suppose that $i_1 j_1 + \cdots + i_n j_n \in IJ$. For each k we can write $i_k = ar_k$ and $j_k = bs_k$ for some $r_k, s_k \in R$. Thus

$$i_1 j_1 + \cdots + i_n j_n = ab(r_1 s_1 + \cdots + r_n s_n),$$

which is in (ab).

(c) Show that if $I = (a, b)$ and $J = (c, d)$ then $IJ = (ac, ad, bc, bd)$.

Solution: Clearly ac, ad, bc, and bd are in IJ, so $(ac, ad, bc, bd) \subset IJ$. Conversely, suppose that $i_1 j_1 + \cdots + i_n j_n \in IJ$. For each k we can write $i_k = ar_k + bs_k$ and $j_k = ct_k + du_k$ for some $r_k, s_k, t_k, u_k \in R$. Thus

$$\begin{aligned} i_1 j_1 + \cdots + i_n j_n = {} & ac(r_1 t_1 + \cdots + r_n t_n) + ad(r_1 u_1 + \cdots + r_n u_n) \\ & + bc(s_1 t_1 + \cdots + s_n t_n) + bd(s_1 u_1 + \cdots + s_n u_n), \end{aligned}$$

which is in (ac, ad, bc, bd).

Some recollections: Recall that in an integral domain R,

- An element a is called *irreducible* if $a = bc$ implies that b is a unit or c is a unit.
- An element a is called *prime* if $a \mid bc$ implies that $a \mid b$ or $a \mid c$.

- An ideal I is called *prime* if $bc \in I$ implies $b \in I$ or $c \in I$.

It is a good exercise, although we will not do it right now, to show that an element a is prime if and only if the principal ideal (a) is a prime ideal, and that if a is prime then it is irreducible. In a principal ideal domain like $\mathbb{Z}$ or $F[x]$ or $\mathbb{Z}[i]$, the converse holds as well: if a is irreducible then it is prime. But this does not hold in general, as we will see in the next problem.

5. (35 points)

(a) Show that there are no $x, y \in \mathbb{Z}$ such that $x^2+5y^2 = 2$. (Hint: Make an elementary argument, not a fancy argument.) Then write "Similarly, there are no $x, y \in \mathbb{Z}$ such that $x^2 + 5y^2 = 3$."

Solution: Since x^2 and $5y^2$ are both non-negative, $x^2+5y^2 = 2$ would imply that $x^2 \leq 2$ and $5y^2 \leq 2$. Since x and y are integers, the first implies that $x = 0$ or ± 1, and the second implies that $y = 0$. But in that case we have $x^2 + 5y^2 = 0$ or 1, not 2. Similarly, there are no $x, y \in \mathbb{Z}$ such that $x^2 + 5y^2 = 3$.

(b) Let $R = \mathbb{Z}[\sqrt{-5}] = \{x + y\sqrt{-5} : x, y \in \mathbb{Z}\}$. This is a subring of $\mathbb{C}$, hence is an integral domain. Observe that if $z \in R$ then $|z|^2$ is a non-negative integer. Then show that z is a unit in R if and only if $|z|^2 = 1$. (Hint: $|zw|^2 = |z|^2|w|^2$.)

Solution: We have $|x + y\sqrt{-5}|^2 = x^2 + 5y^2$, which is clearly non-negative and an integer. Suppose that z is a unit in R, so there is a $w \in R$ such that $zw = 1$. Then $|z|^2|w|^2 = 1$, but since $|z|^2$ and $|w|^2$ are non-negative integers this implies that $|z|^2 = 1$ and $|w|^2 = 1$. Conversely, if $z \in R$ satisfies $|z|^2 = 1$ then $z\bar{z} = 1$, and we note that $\bar{z} \in R$. (In fact, if $x^2 + 5y^2 = 1$ then $x = \pm 1$ and $y = 0$, so ± 1 are the only units in R.)

(c) Calculate $|z|^2$ for the following z:

$$2 \qquad 3 \qquad 1+\sqrt{-5} \qquad 1-\sqrt{-5}.$$

Show that these are irreducible in R. (Hint: Consider the possible factorizations of $|z|^2$.)

Solution: We have

$$|2|^2 = 4 \qquad |3|^2 = 9 \qquad \left|1+\sqrt{-5}\right|^2 = \left|1-\sqrt{-5}\right|^2 = 6.$$

To see that 2 is irreducible, suppose that $zw = 2$; then $|z|^2|w|^2 = 4$, so either $|z|^2 = 1$ and $|w|^2 = 4$, in which case z is a unit, or $|z|^2 = 2$ and $|w|^2 = 2$, which is impossible by part (a), or $|z|^2 = 4$ and $|w|^2 = 1$, in which case w is a unit. Similarly, $|3|^2 = 9$ can factor as $9 \cdot 1$ or $3 \cdot 3$ or $1 \cdot 9$, and $\left|1 \pm \sqrt{-5}\right|^2 = 6$ can factor as $6 \cdot 1$ or $3 \cdot 2$ or $2 \cdot 3$ or $1 \cdot 6$, but there is no $z \in R$ with $|z|^2 = 2$ or 3.

(d) Show 2 is not prime in R. (Hint: $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6$.)

Solution: Taking the hint, we see that $(1+\sqrt{-5})(1-\sqrt{-5})$ is $2 \cdot 3$, but neither $1+\sqrt{-5}$ nor $1-\sqrt{-5}$ is a multiple of 2. (Nor are they multiples of 3, so 3 is not prime. And $1 \pm \sqrt{-5}$ are not prime because they divide $6 = 2 \cdot 3$ but not 2 or 3; to see this, note that $\left|1 \pm \sqrt{-5}\right|^2 = 6$ does not divide $|2|^2 = 4$ or $|3|^2 = 9$.)

(e) Consider the ideals

$$I_1 = (2,\, 1 + \sqrt{-5}) \qquad J_1 = (3,\, 1 + \sqrt{-5})$$
$$I_2 = (2,\, 1 - \sqrt{-5}) \qquad J_2 = (3,\, 1 - \sqrt{-5}).$$

Show that $I_1 = I_2$. (Hint: Show that $1+\sqrt{-5} \in I_2$ and $1-\sqrt{-5} \in I_1$.)

Solution: Taking the hint, we have

$$1 + \sqrt{-5} = 2 - (1 - \sqrt{-5}) \in I_2$$

and

$$1 - \sqrt{-5} = 2 - (1 + \sqrt{-5}) \in I_1,$$

so $I_1 \subset I_2$ and $I_2 \subset I_1$, so $I_1 = I_2$.

(f) Show that

$$I_1 I_2 = (2) \qquad J_1 J_2 = (3)$$
$$I_1 J_1 = (1 + \sqrt{-5}) \qquad I_2 J_2 = (1 - \sqrt{-5}).$$

(Hint: Problem 4(c) is applicable. For $I_1 I_2 = (2)$, first observe that $I_1 I_2 \subset (2)$, then show that $2 \in I_1 I_2$. The others are similar.)

Solution: By problem 4(c) we have

$$I_1 I_2 = (4,\, 2 - 2\sqrt{-5},\, 2 + 2\sqrt{-5},\, 6).$$

The generators of $I_1 I_2$ are all multiples of 2, so $I_1 I_2 \subset (2)$. On the other hand, $2 = 6 - 4$ which is in $I_1 I_2$, so $(2) \subset I_1 I_2$. Next,

$$J_1 J_2 = (9,\, 3 - 3\sqrt{-5},\, 3 + 3\sqrt{-5},\, 6).$$

All the generators are multiples of 3, and $3 = 9 - 6$ which is in J_1J_2. Next,

$$I_1J_1 = (6,\, 2 + 2\sqrt{-5},\, 3 + 3\sqrt{-5},\, (1 + \sqrt{-5})^2).$$

All the generators are multiples of $1 + \sqrt{-5}$, and

$$1 + \sqrt{-5} = (3 + 3\sqrt{-5}) - (2 + 2\sqrt{-5})$$

which is in I_1J_1. Last,

$$I_2J_2 = (6,\, 2 - 2\sqrt{-5},\, 3 - 3\sqrt{-5},\, (1 - \sqrt{-5})^2).$$

All the generators are multiples of $1 - \sqrt{-5}$, and

$$1 - \sqrt{-5} = (3 - 3\sqrt{-5}) - (2 - 2\sqrt{-5})$$

which is in I_2J_2.

(g) Show that I_1 is a prime ideal, as follows. Consider the map $\varphi : R \to \mathbb{Z}_2$ given by $\varphi(x + y\sqrt{-5}) = \bar{x} + \bar{y}$. Show that this is a surjective ring homomorphism and $\ker\varphi = I_1$. Then quote a homework problem saying that I_1 is a prime ideal if and only if R/I_1 is ________.

Then write "Similarly, by considering the maps $R \to \mathbb{Z}_3$ given by $x + y\sqrt{-5} \mapsto \bar{x} \pm \bar{y}$ we find that J_1 and J_2 are prime."

Solution: Clearly $\varphi(1) = 1$ and $\varphi(z + w) = \varphi(z) + \varphi(w)$. If $z = x + y\sqrt{-5}$ and $w = x' + y'\sqrt{-5}$ then

$$\begin{aligned} \varphi(zw) &= \varphi((xx' - 5yy') + (xy' + yx')\sqrt{-5}) \\ &= \bar{x}\bar{x}' - \bar{5}\bar{y}\bar{y}' + \bar{x}\bar{y}' + \bar{y}\bar{x}' \end{aligned}$$

$$\begin{aligned} \varphi(z)\varphi(w) &= (\bar{x} + \bar{y})(\bar{x}' + \bar{y}') \\ &= \bar{x}\bar{x}' + \bar{x}\bar{y}' + \bar{y}\bar{x}' + \bar{y}\bar{y}' \end{aligned}$$

and because $-5 = 1$ in $\mathbb{Z}_2$ these are equal. Thus φ is a homomorphism. We have $\varphi(0) = 0$ and $\varphi(1) = 1$, so φ is surjective. For the kernel, we have $\varphi(2) = 0$ and $\varphi(1 + \sqrt{-5}) = 0$, so $I_1 \subset \ker\varphi$; conversely, if $x + y\sqrt{-5} \in \ker\varphi$ then $\bar{x} + \bar{y} = 0$, so $x - y$ is even, say $x - y = 2n$, so

$$x + y\sqrt{-5} = (x - y) + y \cdot (1 + \sqrt{-5}) = n \cdot 2 + y \cdot (1 - \sqrt{-5}),$$

so $x + y\sqrt{-5} \in I_1$. Thus by the fundamental homomorphism theorem we have $R/I_1 \cong \mathbb{Z}_2$, which is an integral domain, so I_1 is prime.

Similarly, by considering the maps $R \to \mathbb{Z}_3$ given by $x + y\sqrt{-5} \mapsto \bar{x} \pm \bar{y}$ we find that J_1 and J_2 are prime.

(h) Show that I_1 is not principal, i.e. that there is no $z \in R$ such that $I_1 = (z)$. (Hint: If z divides 2 and $1 + \sqrt{-5}$ then $|z|^2$ divides ...) Then write "Similarly, J_1 and J_2 are not principal."

Solution: If $I_1 = (z)$ then z divides 2 and $1 + \sqrt{-5}$, so $|z|^2$ divides 4 and 6, so $|z|^2$ is either 1 or 2. But from part (a) we know that $|z|^2 = 2$ is impossible, so $|z|^2 = 1$, so z is a unit, so $(z) = R$. But from the previous part we know that $1 \notin I_1$, because $I_1 = \ker \varphi$ and $\varphi(1) \neq 0$.

Similarly, J_1 and J_2 are not principal.

Thus we have seen that while the element 2 is not prime and does not factor as a product of primes, the principal ideal (2) does factor as a product of (non-principal) prime ideals, and similarly with 3 and $1 \pm \sqrt{-5}$. Thus the distressing non-unique factorization

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

is resolved by writing

$$(6) = I_1 I_2 \cdot J_1 J_2 = I_1 J_1 \cdot I_2 J_2,$$

which is no more distressing than saying that $60 = 4 \cdot 15 = 6 \cdot 10$. So in this example at least, ideals really do behave like idealized numbers.