Final Exam

Math 401

December 13, 2014

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.)

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

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

(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?)

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?)

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 ________.

(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?

(c) Find the stabilizer of $\binom{1}{0}$. What is its order?

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

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.

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

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

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 $x^2 + 5y^2 = 3$."

(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: $|zw|^2 = |z|^2|w|^2$.)

(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 $|z|^2$.)

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

(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 $1-\sqrt{-5} \in I_1$.)

(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.)

(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."

(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."

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.