Algebra and Computation

Final Examination

Due date: May 9th, 2017

Instructions

1. You may discuss with your classmates until 3rd May 2017, beyond which you are expected to work on the solutions by yourself.
2. Questions 1 and 2 are (in my opinion) harder than the rest. You may ask for a hint for those questions, if you want, at the cost of **10 points per hint** but you may only do so during 4th May – 7 May 2017. (All students who ask for the hint would be receiving the same hint.)
3. The deadline for not receiving any late-penalty is 9th May 2017. You may choose to delay your submission by **up to 5 days** but it would **cost you 8 points per day of delay**.
4. Solutions are expected as a LaTeX document. You may use this very file by obtaining the source files from megh.
5. This paper has a total of **100 points**.

That is, you may perhaps get some ideas for directions early on but you are expected to solve the problems yourself.

You cannot delay by more than 5 days as your grades have *to be submitted by 15th May 2017.*

Questions

Question 1 (20 points). *Given a group $G \leq S_n$ by a generating set S such that $|G| = p^r \cdot m$ and* $\gcd(m, p) = 1$. *Obtain an algorithm to find a generating set for a Sylow p-group $H \leq G$ in time* $\mathrm{poly}(n, |S|, m)$.

Question 2 (20 points). *You are given a group $G \leq S_n$ by a generating set S and say suppose $H \leq S_m$. To* specify *a homomorphism $\Phi : G \to H$, it suffices to give the value of $\Phi(g)$ for every $g \in S$ as it can then be extended to all of G. But of course, not every map $\tilde{\Phi} : S \to H$ extends to a homomorphism. The task is to check if the given $\tilde{\Phi}$ describes a homomorphism from G to H.*

Input*: $G = \langle S \rangle \leq S_n$ and a map $\tilde{\Phi} : S \to S_m$.*

Goal*: Check whether the map $\tilde{\Phi}$ extends to a homomorphism from G to H, in time* $\mathrm{poly}(n, m, |S|)$.

Question 3 (10 points). *You are given an $n \times n$ matrix M with each entry being a positive integer less than 2^c. Come up with a* $\mathrm{poly}(n, c)$ *time algorithm to compute* $\det(M)$.

Question 4. *Define the Möbius function $\mu : \mathbb{N} \to \{-1, 0, 1\}$ as follows:*

$$\mu(n) = \begin{cases} 0 & \text{if } p^2 \mid n \text{ for some prime } p \\ (-1)^{\#\text{ of distinct prime factors}} & \text{otherwise} \end{cases}$$

E.g. $\mu(1) = 1, \mu(2) = -1, \mu(3) = -1, \mu(4) = 0, \mu(5) = -1, \mu(6) = 1$ etc.

1. **(5 points)** *Prove that $\sum_{k|n} \mu(k) = 0$, for all $n > 1$.*
2. **(10 points)** *If $f : \mathbb{N} \to \mathbb{Z}$ and $g : \mathbb{N} \to \mathbb{Z}$ satisfying*

   $$f(n) = \sum_{d|n} g(d),$$

   then show that we can invert *the dependence via*

   $$g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right).$$

3. **(10 points)** *Recall that over $\mathbb{F}_q$, we have the equation*

   $$x^{q^n} - x = \prod_{\substack{d|n \\ p(x) \text{ monic, irred.} \\ \deg p = d}} p(x).$$

   Show that the number of monic irreducible polynomials of degree d over $\mathbb{F}_q$ is roughly $\frac{q^d}{d}$.

Question 5. *An ideal I in $\mathbb{C}[x_1, \ldots, x_n]$ is said to be* primary *if whenever $fg \in I$ we have either $f \in I$ or $g^m \in I$ for some $m > 0$.*

1. **(5 points)** *If I is primary, show that $\sqrt{I}$ is a prime ideal.*
2. **(10 points)** *Suppose I is* not *a primary ideal, and say $fg \in I$ along with $f \notin I$ and $g^n \notin I$ for any $n > 0$. Show that there is some $N > 0$ such that*

   $$I = (I + \langle f \rangle) \bigcap \left(I + \left\langle g^N \right\rangle\right).$$

3. **(10 points)** *Show that every ideal can be written as a finite intersection of primary ideals.*