Abstract Algebra in Theoretical Computer Science

Assignment 1

Lecturer: Gil Cohen

Problem 1 - Composing groups from existing ones

1. Let G be a group. Let $(H_i)_{i\in I}$ be subgroups of G, where the index set $I \neq \emptyset$ is allowed to be infinite. Prove that $\cap_{i\in I} H_i$ is a subgroup of G.

2. Assuming further that all H_i are normal subgroups of G. Prove that $\cap_{i\in I} H_i$ is a normal subgroup of G.

Given subgroups H, K of a group G, we define

$$HK = \bigcap_{H\cup K\subseteq L<G} L$$

3. Prove that $HK < G$.

4. Prove that if at least one of H, K is normal in G then HK can be written explicitly (i.e., without resorting to an abstract-intersection-type description) as $HK = \{hk \mid h \in H, k \in K\}$.

5. Let $G = (\mathbb{Z}, +)$, $H = (n\mathbb{Z}, +)$, and $K = (m\mathbb{Z}, +)$ for integers n, m. What are $H \cap K$ and $H + K$? (Note that $H + K$ is the above HK but with the suitable additive notation).

Problem 2 - Forbidden subgroups

Prove that if G is a group of order pq for primes $p > q$ then G has at most one subgroup of order p.

Problem 3 - Playing with a small group

Prove that, up to isomorphism, there is a unique group of order 15.

Problem 4 - Subgroups of finite groups

Let G be a finite group. Prove that $\emptyset \neq H \subseteq G$ is a subgroup of G if and only if for every $h_1, h_2 \in H$, $h_1h_2 \in H$ (recall that, without the finiteness condition, one needs to verify that $h_1h_2^{-1} \in H$).

Problem 5 - Classifying groups of order prime squared

In this problem we are going to classify all groups of order p^2 for a prime p. Let G be a group of order p^2.

1. Prove that for every $g \in G \setminus \{e\}$, $\langle g \rangle \triangleleft G$.
2. Prove that G is abelian. I'll give you a hint because it is fairly tricky. Say you want to prove that $hg = gh$ for arbitrary h, g. Note that $hgh^{-1} = g^i$ for some $i \in \{0, 1, \ldots, p-1\}$. Now observe that
$$g^{i^2} = (hgh^{-1})^i = hg^ih^{-1} = h^2gh^{-2}.$$
Continue from here while keeping in mind Fermat's little theorem.
3. Conclude that G is isomorphic to either $\mathbb{Z}_{p^2}$ or to $\mathbb{Z}_p \times \mathbb{Z}_p$.

Problem 6 - Simple groups

A group is said to be *simple* if it has no non-trivial normal subgroups. In a sense, if G is not simple and thus has a non-trivial normal subgroup N, one can "decompose" G to N and G/N. If G is finite, both N and G/N are smaller than G and so for a finite G this process can be repeated to obtain a "decomposition" of G into a finite number of simple groups, very much like factoring an integer to its prime factors. Thus, classifying finite simple groups is a very important problem.

In a momentous effort, the complete classification of all finite simple groups was obtained in 2004. It turns out that most of the finite simple groups belong to one of four families of groups. However, there are 26 groups that do not seem to belong to these families. These intriguing 26 groups are called the *sporadic groups*, the biggest of which is called the *monster group* M. It has order

$$|M| = 808,017,424,794,512,875,886,459,904,961,710,757,005,754,368,000,000,000.$$

So I do not want to hear complaints about Problem 3 :) Search "life, death, and the monster - numberphile" on youtube to hear a 10 minute talk about this by the great John Conway who discovered the monster group.

In this problem we will do a little bit of digging into finite simple groups.

1. Classify all abelian simple groups.

Next we are going to find a non-abelian simple group. Let G be the group of permutations over $\{1, 2, 3, 4, 5\}$ that is generated by σ, τ, where

$$\begin{array}{ll} \sigma(1) = 2 & \tau(1) = 3 \\ \sigma(2) = 1 & \tau(2) = 2 \\ \sigma(3) = 4 & \tau(3) = 5 \\ \sigma(4) = 3 & \tau(4) = 4 \\ \sigma(5) = 5 & \tau(5) = 1 \end{array}$$

2. Prove that G is non-abelian.

3. Find $|G|$.

4. Prove that G is simple (this may require some effort).

Problem 7 - The second homomorphism theorem

In this problem you are asked to prove a theorem known as *the second homomorphism theorem*. It is the content of the fourth item. Let G be a group, $H < G$, $N \triangleleft G$. Prove the following:

1. $HN < G$

2. $H \cap N \triangleleft H$

3. $N \triangleleft HN$

4. $H \Big/ (H \cap N) \simeq (HN) / N$

5. What does the above item implies when applied to $G = (\mathbb{Z}, +)$ with two subgroups $N = (n\mathbb{Z}, +)$ and $H = (m\mathbb{Z}, +)$?

Problem 8 - The correspondence theorem

In this problem you are asked to prove an important theorem known as *the correspondence theorem.* Let G, G' be groups and $\phi\colon G \to G'$ an epimorphism with $\text{Ker}\phi = K$. Let $H' < G'$ and define $H = \phi^{-1}(H')$. Prove that

1. $K \subseteq H < G$

2. $H/K \simeq H'$

3. If $H' \triangleleft G'$ then $H \triangleleft G$.

Let G be a group and $N \triangleleft G$. Observe that if we apply the above to the natural homomorphism $\phi\colon G \to G/N$ (that maps g to gN) we obtain a one-to-one correspondence between the subgroups of the quotient group G/N and the subgroups of G that contains N. Moreover, this correspondence preserves normality. Try to see what this means for $G = (\mathbb{Z}, +)$ and $N = 6\mathbb{Z}$.