Prof. Dr. Marcus Greferath
Dept. of Mathematics and Systems Analysis
School of Sciences
Aalto University
Spring 2019

MS-E1997: Abstract Algebra II

Problem Set I

Problem 1: Let G be a group and M be a subset of G.

(a) Show that $\{x_1^{n_1} \dots x_k^{n_k} \mid n_i \in \mathbb{Z},\ k \in \mathbb{N} \text{ and } x_i \in M\}$ is a subgroup of G.

(b) Show that this subgroup coincides with $\langle M \rangle := \bigcap \{U \leq G \mid M \subseteq U\}$.

Work: **(a)** We first observe that, regardless of the set M being empty or not, the set $X := \{x_1^{n_1} \dots x_k^{n_k} \mid n_i \in \mathbb{Z},\ k \in \mathbb{N} \text{ and } x_i \in M\}$ is non-empty because it contains (at least) the empty product which evaluates to 1. Furthermore this set is closed under multiplication because the result of a multiplication is just a concatenation of the strings that we see in X. For the existence of inverses observe that $(x_1^{n_1} \dots x_k^{n_k})^{-1} = x_k^{-n_k} \dots x_1^{-n_1}$ and, as this is again of the form of the elements in X we see that X is closed under inversion. All in all we have proven X to be a subgroup of G.

For **(b)** we use that X is certainly a subgroup that contains M. Hence, it is one of the subgroups occuring in the definition of $\langle M \rangle$, and this shows that $X \geq \langle M \rangle$. On the other hand, every subgroup of G that contains M must also contain all products of powers of elements in M, and thus X. Since $\langle M \rangle$ contains M we therefore see that $\langle M \rangle \geq X$, which concludes the proof of equality.

Problem 2: Let A_1, A_2, B_1, B_2 be normal subgroups of a group G with $B_1 \leq A_1$ and $B_2 \leq A_2$ and finally $A_1 \cap A_2 = \{e\}$. Then $B_1 B_2$ is normal subgroup in $A_1 A_2$ and there holds

$$(A_1 A_2)/(B_1 B_2) \cong (A_1/B_1) \oplus (A_2/B_2).$$

Work: We consider the mapping

$$\varphi : A_1 \oplus A_2 \longrightarrow A_1/B_1 \oplus A_2/B_2, \quad a_1 a_2 \mapsto (a_1 B_1, a_2 B_2).$$

For each $g \in A_1 A_2$ there are unique $a_1 \in A_1$ and $a_2 \in A_2$ such that $g = a_1 a_2$. Therefore this mapping is well-defined. Moreover, as A_1 and A_2 are normal with trivial intersection, we have $a_1 a_2 = a_2 a_1$ for all $a_1 \in A_1$ and $a_2 \in A_2$, and for this reason we will find that φ is a homomorphism. Indeed, if $g = a_1 a_2$ and $h = a_1' a_2'$ then

$$\begin{aligned}
\varphi(gh) &= \varphi(a_1 a_2 a_1' a_2') \;=\; \varphi(a_1 a_1' a_2 a_2') \\
&= (a_1 a_1' B_1, a_2 a_2' B_2) \;=\; (a_1 B_1, a_2 B_2) \cdot (a_1' B_1, a_2' B_2) \\
&= \varphi(g)\varphi(h)
\end{aligned}$$

The homomorphism φ is even onto because for arbitrary (a_1B_1, a_2B_2) we find the preimage a_1a_2 under φ. For the kernel we see that

$$\ker\varphi \;=\; \{a_1a_2 \in A_1 \oplus A_2 \mid a_1B_1 = B_1 \text{ and } a_2B_2 = B_2\} \;=\; B_1 \oplus B_2,$$

and by this observation we obtain our claim by application of the homomorphism theorem.

Problem 3: If G is a free Abelian group of ranks r and s, then $r = s$. Prove this in the following way: Let $\varphi : \mathbb{Z}^r \longrightarrow \mathbb{Z}^s$ be an isomorphism, and let α and β be the natural embeddings of $\mathbb{Z}^r$ (resp. $\mathbb{Z}^s$) into the respective direct sums of copies of $\mathbb{Q}$.

(a) Show that for every $x \in \mathbb{Q}^n$ there exists $z \in \mathbb{Z}$ such that $zx \in \mathbb{Z}^n$.

(b) Define $\overline{\varphi} : \mathbb{Q}^r \longrightarrow \mathbb{Q}^s$ by $x \mapsto \frac{1}{z}\varphi(zx)$ where z is the number that you found in **(a)**. Show that this mapping is well-defined.

(c) Show that $\overline{\varphi}$ is additive and (hence) $\mathbb{Z}$-linear; then show that $\overline{\varphi}$ is $\mathbb{Q}$-linear.

(d) Show that $\overline{\varphi}$ is one-to-one, and draw your final conclusion by symmetry.

<u>Proof:</u> **(a)** This claim is immediate because the entries in x have a common denominator, and using z to be this denominator we have $x = \frac{1}{z}zx$ where $zx \in \mathbb{Z}^n$.
(b) We have to show first that this definition does not depend on the choice of z. For $z, z' \in \mathbb{Z}$ we compute

$$\begin{aligned}\frac{1}{z}\varphi(zx) - \frac{1}{z'}\varphi(z'x) \;&=\; \frac{1}{zz'}(z'\varphi(zx) - z\varphi(z'x)) \\ &=\; \frac{1}{zz'}(\varphi(z'zx) - \varphi(zz'x)) \;=\; 0,\end{aligned}$$

and this shows that $\overline{\varphi}$ is well-defined.
(c) For $x, y \in \mathbb{Q}^r$ there exists $z \in \mathbb{Z}$ such that $zx \in \mathbb{Z}^r$ and $zy \in \mathbb{Z}^r$, and certainly $z(x+y) \in \mathbb{Z}$. For this reason we find

$$\overline{\varphi}(x+y) \;=\; \frac{1}{z}\varphi(z(x+y)) \;=\; \frac{1}{z}\varphi(zx) + \frac{1}{z}\varphi(zy) \;=\; \overline{\varphi}(x) + \overline{\varphi}(y),$$

which shows that $\overline{\varphi}$ is additive and (hence) $\mathbb{Z}$-linear. For the $\mathbb{Q}$-linearity we consider $x \in \mathbb{Q}^r$ and $q \in \mathbb{Q}$. Then there exists $a, b \in \mathbb{Z}$ with $aq \in \mathbb{Z}$ and $bx \in \mathbb{Z}^r$. We then compute

$$\begin{aligned}\overline{\varphi}(qx) \;&=\; \frac{1}{ab}\varphi(aqbx) \;=\; \frac{1}{ab}aq\varphi(bx) \\ &=\; q\frac{1}{b}\varphi(bx) \;=\; q\overline{\varphi}(bx),\end{aligned}$$

and hence we have $\mathbb{Q}$-linearity.
(d) If $x, y \in \mathbb{Q}^r$ with $\overline{\varphi}(x) = \overline{\varphi}(y)$ then we find $z \in \mathbb{Z}$ with $zx \in \mathbb{Z}^r$ and $zy \in \mathbb{Z}^r$. Like in the **(a)** part we compute

$$0 \;=\; \overline{\varphi}(x) - \overline{\varphi}(y) \;=\; \frac{1}{z}\varphi(zx) - \frac{1}{z}\varphi(zy) \;=\; \frac{1}{z}\varphi(z(x-y))$$

which shows that $\varphi(z(x-y)) = 0$ and by injectivity of φ also $z(x-y) = 0$. From this, however we find $x - y = 0$ and this shows the claim. For surjectivity let $y \in \mathbb{Q}^s$ be given. Then there exists $z \in \mathbb{Z}$ with $zy \in \mathbb{Z}^s$ and we consider the element $x := \frac{1}{z}\varphi^{-1}(zy) \in \mathbb{Q}^r$. For this element we certainly have

$$\overline{\varphi}(x) \;=\; \frac{1}{z}\overline{\varphi}\varphi^{-1}(zy) \;=\; \frac{1}{z}\varphi\varphi^{-1}(zy) \;=\; \frac{1}{z}zy \;=\; y,$$

and this finishes our work.

Problem 4: Determine all Abelian groups of order 9000.

You are encouraged to collaborate in preparing solutions, however, please submit individual write-ups.