MATHEMATICS Chalmers University of Technology
Examination in algebra MMG500 and MVE 150, 2013-06-07
No books, written notes or any other aids are allowed.
Telephone: 0703-088304

1a) Let $m \geq 2$ and $n \geq 2$ be integers. Show that a finite group of order $mn$ has at least three subgroups. 3p

b) Prove that an infinite group has infinitely many subgroups. 2p

2. Let $a,b,c$ be positive integers such that $c$ divides $ab$.

a) Show that $c$ divides $b$ if $\text{GCD}(a, c)=1$. 3p

b) More generally, show that $c$ divides $bd$ for $d=\text{GCD}(a, c)$. 2p

3. Let $\theta: G \to H$ be a homomorphism of groups and $g \in G$. Show that $o(\theta(g))$ is a factor of $o(g)$. 3p

4. An ideal $P \neq R$ of a commutative ring $R$ is said to be a prime ideal if for all $a,b \in R$, we have that $ab \in P$ implies that $a \in P$ or $b \in P$. Prove that, if $n$ is a positive integer, then $(n):=\{mn : m \in \mathbf{Z}\}$ is a prime ideal of $\mathbf{Z}$ if and only if $n$ is a prime. 3p

5. Let $G$ be a multiplicative group and $H$ be a subset of $G$. Show that $H$ is a subgroup of $G$ if and only if the following conditions hold. 4p

a) $H$ is non-empty

b) if $a \in H$ and $b \in H$, then $ab \in H$.

c) if $a \in H$, then $a^{-1} \in H$.

6. Let $\theta: R \to S$ be a ring homomorphism.

a) Show that the kernel of $\theta$ is an ideal of $R$. 3p

b) More generally, show that the inverse image $\theta^{-1}(J)$ of an ideal $J$ of $S$ is an ideal of $R$. 2p

(You should here verify all conditions for a subset to be an ideal without referring to any other theorem.)

*The theorems of Durbin's book may be used to solve exercises 1–4, but all claims that are made must be motivated.*

# Solutions to examination in algebra MMG500 and MVE 150

2013-06-07

1a) If $G$ is a finite group of order$\geq 2$, then there is an element $g \neq e$ in $G$, which by the subgroup criterion generates a subgroup $H = \langle g \rangle \neq \{e\}$ of $G$ If $|H| < |G|$, then $H$ is a subgroup different from $\{e\}$ and $G$. If $|H| = |G|$, then $G = \langle g \rangle$ is cyclic. By a theorem in Durbin's book, we have then that $H = \langle g^m \rangle$ is a cyclic subgroup of order $|G|/m$ for factors $m$ of $|G|$. This subgroup is thus different from $\{e\}$ and $G$ if $|G| = mn$ with $m \geq 2$ and $n \geq 2$.

1b) Suppose first that $G$ contains an element $g$ of infinite order. There are then infinitely many cyclic subgroups $\langle g^n \rangle$ of $G$, indexed by $n \in \mathbf{N}$. If instead all elements of $G$ are of finite order, then $G$ will be the union of the finite cyclic subgroups $\langle g \rangle$, $g \in G$. As $|G|$ is infinite, $G$ must thus have infinitely many finite different cyclic subgroups.

2a) Let $a,b,c$ be positive integers with GCD$(a, c)=1$. By Euclid's algorithm we may find integers $x,y$ with $ax+cy=1$. If $c$ divides $ab$, then it will also divide $b(ax+cy)=b$.

b) If GCD$(a, c)=d$, then $ax+cy=d$ for some $x,y \in \mathbf{Z}$. Hence $c|ab \Rightarrow c|\, b(ax+cy)=bd$.

3) Let $n=o(g)$. Then $\theta(g)^n = \theta(g^n) = \theta(e) = e$. Hence $m := o(\theta(g))$ divides $n$ be a theorem in Durbin's book. Indeed, if $n = mq+r$ with $0 \leq r < m$, then $e = \theta(g)^n = \theta(g)^{mq}\theta(g)^r = (\theta(g)^m)^q\theta(g)^r = e^q\theta(g)^r = \theta(g)^r$ implies that $r=0$ as $m$ is the smallest positive integer with $\theta(g)^m = e$.

4) If $(n)$ is a prime ideal, then $n \geq 2$ as $(n) \neq \mathbf{Z}$. Also, if $n = ab$ for $a,b \in \mathbf{N}$, then $a \in (n)$ or $b \in (n)$. We have thus that $n|a$ or $n|b$. But if $n|a$, then $a \leq ab = n \leq a$ and if $n|b$, then $b \leq ab = n \leq b$. Hence $n=a$ or $n=b$ for any factorization $n = ab$, which means that $n$ is prime.

Conversely, if $n$ is a prime, then $n \geq 2$ and $(n) \neq \mathbf{Z}$. If $ab \in (n)$, then $n|\, ab$. By Euclid's lemma we have thus for a prime $n$ that $n|\, a$ or $n|\, b$. Hence $a \in (n)$ or $b \in (n)$, which means that $(n)$ is a prime ideal.

5) See Durbin's book

6a) See Durbin's book.

b) Let $\Theta$: $R \to S/J$ be the ring homomorphism which sends $r \in R$ to $\theta(r)+J \in S/J$. Then $\theta^{-1}(J)$ is the kernel of $\Theta$ and hence an ideal of $R$ by a).