MATHEMATICS Univ. of Gothenburg and Chalmers University of Technology
Examination in algebra : MMG500 and MVE 150, 2014-03-14.
No books, written notes or any other aids are allowed.
Telephone : 0703-088304

1 Let G be a group and $g \in G$. The centraliser $C(g)$ of g in G is the set of all $h \in G$ such that $gh=hg$.

a) Prove that $C(g)$ is a subgroup of G. 3p

b) Determine the centraliser of $g=(1\ 2)$ in S_3. 2p

(Hint: If you use a) you get less calculations.)

2. Let G be a group and θ: $G \to G$ be the map where $\theta(g)=g^2$ for all $g \in G$. Suppose that θ is a homomorphism. Show that G is abelian. 3p

3. A ring R is called Boolean if $r^2=r$ for all $r \in R$. Prove or disprove that any Boolean integral domain with unity is isomorphic to $\mathbf{Z}_2$ as a ring. (Hint: Use the hypothesis!) 3p

4. Let p be a prime and I be the principal ideal in $\mathbf{Q}[x]$ generated by $f(x)= ((x+1)^p -1)/x \in \mathbf{Z}[x]$.

a) Show that the quotient ring $F= \mathbf{Q}[x]/I$ is a field. 3p

b) Determine the inverse of $(x+1)+ I$ in F and write it in the form $g(x)+I$ for a polynomial $g(x) \in \mathbf{Q}[x]$ of degree at most p-2. 2p

5. Formulate and prove the fundamental theorem of arithmetic. 5p

(The proof should be complete and not based on unproved lemmas.)

6. Formulate and prove the fundamental homomorphism theorem for groups. 4p

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) **2014-03-14**

1a) We apply the subgroup criterion. First, $C(g)\neq\varnothing$ as $ge=eg \Rightarrow e\in C(g)$.
Next, if $a,b\in C(g)$, then $ab\in C(g)$ as $g(ab)=(ga)b=(ag)b=a(gb)=a(bg)=(ab)g$.
Finally, $a^{-1}g^{-1}=(ga)^{-1}=(ag)^{-1}=g^{-1}a^{-1}$ for $a\in C(g)$. Hence $ga^{-1}=ga^{-1}g^{-1}g=gg^{-1}a^{-1}g=a^{-1}g$ such that $a^{-1}\in C(g)$ for $a\in C(g)$.

b) Clearly $H=\{e,g\}\subseteq C(g)$ as $ge=eg$ and $gg=gg$. Hence as $g^2=(1\ 2)^2=id=e$, H is a subgroup of $C(g)$. Further, $(1\ 3)\notin C(g)$ as $(1\ 2)(1\ 3)=(1\ 3\ 2)\neq(1\ 3)(1\ 2)=(1\ 2\ 3)$.
So $C(g)\neq S_3$ and $o(C(g))<6$. By Lagrange's theorem $o(H)|\ o(C(g))$ and $o(C(g))|\ o(S_3)=6$.
Therefore, $o(C(g))=2$ and $C(g)=H=\{id, (1\ 2)\}$.

2. Let $g,h\in G$. Then $\theta(gh)=\theta(g)\theta(h) \Rightarrow (gh)(gh)=g^2h^2 \Rightarrow [(gh)g]h=[g^2h]h \Rightarrow (gh)g=g^2h \Rightarrow g(hg)=g(gh) \Rightarrow hg=gh$ by associativity and the cancellation law. Hence $gh=hg$ for any $g,h\in G$, as desired.

3. Let $r\in R$ and 1 be the unity of R. Then, $r(1-r)=r-r^2=0$ and $r=0$ or $1-r=0$ as there no zero divisors in R. We have thus that $R=\{0,1\}$. As 0 is neutral in the group $(R,+)$ we have also that $0+0=0$, $0+1=1+0=1$. Further, $1+1=0$ as $1+1\neq1+0=1$ by the cancellation law. Finally, $0\times0=0$ in any ring and $0\times1=1\times0=0$ $1\times1=1$ as 1 is a unity. Therefore, $R\approx\mathbf{Z}_2$ as rings as they the two rings have the same Cayley tables for + and ×.

4a) It suffices to show that $f(x)$ is irreducible in $\mathbf{Q}[x]$ since $F=\mathbf{Q}[x]/(f(x))$ is then a field by a theorem in Durbin's book. From the binomial theorem we conclude that

$$f(x)=x^{p-1}+\binom{p}{1}x^{p-2}+\binom{p}{2}x^{p-3}+\ldots+\binom{p}{p-2}x+\binom{p}{p-1}$$

where all coefficients apart from the leading one are divisible by p. As the constant coefficient p is not divisible by p^2 we have thus by Eisenstein's criterion that $f(x)$ is irreducible in $\mathbf{Q}[x]$.

4b) Let $I=(f(x))$. Then $(x+1)^p+I=1+I$ as $(x+1)^p-1=xf(x)\in I$. Hence $((x+1)+I)((x+1)^{p-1}+I)=1+I$ such that $(x+1)^{p-1}+I$ is a mutliplicative inverse to $(x+1)+I$ in $F=\mathbf{Q}[x]/I$. If instead, we represent $(x+1)^{p-1}+I$ by $(x+1)^{p-1}-f(x)$, then we get that

$$-\binom{p}{1}x^{p-2}-\binom{p}{2}x^{p-3}-\ldots-\binom{p}{p-2}x-\binom{p}{p-1}+I$$

is a multiplicative inverse to $(x+1)+I$ in F.

5. See p.70 in Durbin's book.

6. See p.114 in Durbin's book.