MATHEMATICS
University of Gothenburg and Chalmers University of Technology
Examination in algebra : MMG 500 and MVE 150, 2017-06-08.
No books, written notes or any other aids are allowed.
Telephone. 031-772 35 25

1a) Compute the product π=(1 2)(2 3)(3 4) in S_4. 4p

b) Describe the permutations in the cyclic subgroup generated by π.

The permutations should be written in cycle form.

2 Let g,h be two elements in a finite group. Show that gh and hg have the same order. 4p

3.Determine the zero divisors and invertible elements in $\mathbf{Z}_{10}$. 4p

4 Let p be a prime. 5p

a) Show that the equation $x^p - 1 = 0$ has no other root than 1 in $\mathbf{Z}_p$.

b) Can the equation $x^p - a = 0$ have more than one root in $\mathbf{Z}_p$ for other elements $a \neq 1$ in $\mathbf{Z}_p$?

5. Let $* : G \times G \to G$ be an associative binary operation on a set G. 4p

a) Show that $(G, *)$ has at most one neutral element.

b) Show that each element of G has at most one inverse with respect to $*$.

6. Show that any finite integral domain is a field. 4p

All claims that are made must be motivated. The exams will be corrected within four weeks.

Brief solutions to examination in algebra 2017-06-08

(MMG 500-MVE 150)

1a). $\pi = (12)(2\ 3)(3\ 4) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \\ 1 & 3 & 4 & 2 \\ 2 & 3 & 4 & 1 \end{pmatrix} = (1234)$

1b) $(1234)^2 = (13)(24)$, $(1234)^3 = (1432)$ and $(1234)^4 = id$.

The group generated by π will thus have $\{id, (1234), (13)(24), (1432)\}$ as underlying set.

2 If $k \in N$, then $h(gh)^k h^{-1} = (hg)^k hh^{-1}$ by the associative law. As $hh^{-1} = e$, we thus get $h(gh)^k h^{-1} = (hg)^k$. In particular, if $(gh)^k = e$, then $(hg)^k = heh^{-1} = e$. Conversely, by symmetry $(hg)^k = e \Rightarrow (gh)^k = e$. The list of exponents of all $k \in N$ with $(gh)^k = e$ will therefore coincide with the list of all exponents with $(hg)^k = e$. So gh and hg have the same order.

3. Let $[k]$ be the congruence class (mod 10) of $k \in \mathbf{Z}$. Then, [2], [4], [5], [6] and [8] are zero divisors in $\mathbf{Z}_{10}$ as $[2][5] = [4][5] = [6][5] = [8][5] = [0]$, while [1], [3], [7], [9] are invertible as $[1]^2 = [1]$, $[3][7] = [1]$ and $[9]^2 = [1]$. So any element $[k] \neq [0]$ is either a zero divisor or invertible in $\mathbf{Z}_{10}$.
Further, no element $[k]$ in $\mathbf{Z}_{10}$ can be both a zero divisor and invertible, Indeed, if $[j][k] = [0]$ and $[k][l] = [1]$, then $[j] = [j][1] = [j]([k][l]) = ([j][k])[l] = [0][l] = [0]$.
There are thus no further zero divisors or invertible elements in $\mathbf{Z}_{10}$.

4 The elements $\neq 0$ in $\mathbf{Z}_p$ form a multiplicative group with $p-1$ elements as $\mathbf{Z}_p$ is a field. By a corollary of Lagrange's theorem we have thus that $x^{p-1} = 1$ for all $x \neq 0$. in $\mathbf{Z}_p$. Hence $x^p = x$ for all $x \in \mathbf{Z}_p$. The equation $x^p - a = 0$ is thus equivalent to the equation $x - a = 0$. This means that for each $a \in \mathbf{Z}_p$, the equation $x^p - a = 0$ has exactly one solution in $\mathbf{Z}_p$, namely $x = a$.

5. See Durbin's book
6. See Durbin's book