1a) Compute the product $\pi=(1 \ 2)(2 \ 3)(3 \ 4)$ in $S_4$.  

b) Describe the permutations in the cyclic subgroup generated by $\pi$. 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.

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

4. Let $p$ be a prime.
   a) Show that the equation $x^p - 1 = 0$ has no other root than 1 in $\mathbb{Z}_p$.
   b) Can the equation $x^p - a = 0$ have more than one root in $\mathbb{Z}_p$ for other elements $a \neq 1$ in $\mathbb{Z}_p$?

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

All claims that are made must be motivated. The exams will be corrected within four weeks.
1a. \( \pi = (12)(23)(34) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \\ 1 & 3 & 4 & 2 \\ 2 & 3 & 4 & 1 \end{pmatrix} = (1234) \)

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

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

2. If \(k \in \mathbb{N}\), then \(h(g)^k h^{-1} = (hg)^k h h^{-1}\) by the associative law. As \(hh^{-1} = e\), we thus get \(h(g)^k h^{-1} = (hg)^k\). 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 \(k \in \mathbb{N}\) 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 \((\text{mod } 10)\) of \(k \in \mathbb{Z}\). Then, \([2], [4], [5], [6]\) and \([8]\) are zero divisors in \(\mathbb{Z}_{10}\) 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 \(\mathbb{Z}_{10}\).

Further, no element \([k]\) in \(\mathbb{Z}_{10}\) 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 \(\mathbb{Z}_{10}\).

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

5. See Durbin’s book

6. See Durbin’s book