1) Let $R$ be an integral domain with four elements $0,1,a$ and $b$ where $1$ is the neutral element for multiplication. Prove the following statements in $R$.
   a) $1+1=0$.  
   b) $a+1=b$.  
   c) $a^2=b$.  

2) Let $R$ be the set of all rational numbers of the form $m/2^n$ for integers $m$ and $n$.
   a) Show that $R$ is a subring of $\mathbb{Q}$.  
   b) Which of the integers $2$, $4$ and $6$ are irreducible in $R$? Which of these three integers are units in $R$?

3a) Determine the number of elements of order 5 in $S_5$.  
3b) Determine the number of subgroups of order 5 in $S_5$.

4) Let $T$ be the set of subgroups of order 5 of $S_5$. If $\sigma \in S_5$, let $\pi_\sigma: T \to T$ be the bijective map which sends a subgroup $H$ of order 5 to the subgroup $\sigma H\sigma^{-1}:=\{\sigma h\sigma^{-1} : h \in H\}$ in $T$.
   a) Prove that the map $\pi: S_5 \to \text{Sym}(T)$, which sends $\sigma \in S_5$ to $\pi_\sigma \in \text{Sym}(T)$ gives an action of $S_5$ on $T$.  
   b) The above action of $S_5$ on $T$ is transitive by a theorem of Sylow. Use this to show that $\pi$ is injective.

5a) Show that each group has at most one neutral element.  
5b) Show that each element of a group has at most one inverse.  

6) Prove that congruence modulo $n$ is an equivalence relation on $\mathbb{Z}$ for each positive integer $n$.

*You may use the theorems in Durbin’s book to solve the first 4 exercises.*

*But all claims should be motivated!*
Solutions to algebra exam: MMG500 and MVE 150, 2019-03-23.

1a) On applying a corollary of Lagrange’s theorem to the underlying additive group we get that $(1+1)^2=1+1+1+1=0$. Hence $1+1=0$ as we are in an integral domain.

b) The group equation $x+1=b$ has a unique solution $x=b-1$. But $0+1=1\neq b$, $1+1=0\neq b$ and $b+1\neq b$. Hence $x\notin \{0, 1\}$, which implies that $x=a$ and $a+1=b$.

c) A finite integral domain is a field and hence $\{1, a, b\}$ a multiplicative group of prime order. We have thus by a corollary of Lagrange’s theorem that $\{1, a, b\} = \{1, a, a^2\}$. So $a^2=b$.

2a) If $k.l.m.n \in \mathbb{Z}$, then $k/2^l m/2^n = (2^{-l} k \pm m)/2^n = (k \pm 2^{l-n} m)/2^l \in \mathbb{R}$ as $2^{l-n} k \pm m \in \mathbb{Z}$ or $k \pm 2^{l-n} m \in \mathbb{Z}$. Hence $R$ is closed under addition and subtraction. $R$ is also closed under multiplication as $(k/2^l)(m/2^n) = km/2^{l+n} \in \mathbb{R}$. Hence $R$ is a subring of $\mathbb{Q}$ by the subring criterion.

b) 2 and 4 are units in $\mathbb{R}$ with inverses $1/2$ resp. $1/4$ in $\mathbb{R}$. They are thus not irreducible in $\mathbb{R}$.

6 is not a unit in $\mathbb{R}$ as $1/6 \notin \mathbb{R}$. To decide if 6 is irreducible or nor we use that all elements of $\mathbb{R}$ are of the form $m/2^n$ with $n \geq 0$. If now $3=(k/2^l)(m/2^n)$ with $l, n \geq 0$, then $2^{l+n} = kl$ in $\mathbb{N}$. Hence $k$ or $l$ is then a 2-power and $k/2^l$ or $m/2^n$ a unit. This means that 6 is irreducible in $\mathbb{R}$.

3a) An element of order 5 in $S_5$ can only have one cycle of order 5. It is therefore of the form $(1 \ a \ b \ c \ d)$ with $(a,b,c,d) = \{2,3,4,5\}$. There are $4!=24$ orderings of $\{2,3,4,5\}$ and hence 24 elements of order 5 in $S_5$.

b) The intersection of two different subgroups of order 5 is of order 1 by Lagrange’s theorem. We have thus a partition of the 24 elements of order 5 into disjoint subsets with 4 elements, where each such subset consists of the 4 non-neutral elements in a subgroup of order 5. There are thus 6=24/4 such subsets and 6 subgroups of order 5 in $S_5$.

4a) Let $\sigma, \tau \in S_5$ and $H$ be a subgroup of order 5 in $S_5$. Then,

$\pi_{\sigma} (H) = (\sigma \tau) H (\sigma \tau)^{-1} = \{(\sigma \tau) h (\sigma \tau)^{-1} : h \in H\} = \{ (\sigma \tau) h (\tau^{-1} \sigma^{-1}) : h \in H\}$,

$\pi_{\tau} (H) = \sigma (\tau H \tau^{-1}) \sigma^{-1} = \{ \sigma (\tau h \tau^{-1}) \sigma^{-1} : h \in H\} = \{(\sigma \tau) h (\tau^{-1} \sigma^{-1}) : h \in H\}$.

Hence $\pi_{\sigma} = \pi_{\tau} \pi_{\tau} \pi_{\tau}$ in $\text{Sym}(T)$ for all $\sigma, \tau \in S_5$, which means that $\pi$ is an action of $S_5$ on $T$.

b) $K=\ker \pi$ is contained in the stabilizer $N(H) = \{ \sigma \in S_5 : \sigma H \sigma^{-1} = H \}$ of any $H \in T$. If the normal subgroup $K$ contained a Sylow 5-subgroup of $S_5$, then it would contain all such subgroups as they are conjugate in $S_5$. It would thus then be of order $>24$ as it contains all elements of order 5 in $S_5$. But this is impossible as $K$ is a subgroup of $N(H)$ for any $H \in T$ and $o(N(H))=o(S_5)/\text{Card} T=20$ as $S_5$ acts transitively on $T$. The order of $K$ can therefore not be divisible by 5 as it contains no Sylow-5-subgroup. It is thus by Lagrange’s theorem of order 1,2 or 4 as a subgroup of $N(H)$. If $o(K)=2$ or 4, then there is an element $\sigma \in K$ of order 2. But all conjugates of $\sigma$ are then also in $K$ as it is normal in $S_5$. We have thus then that $(12)$ and all its 9 conjugates are in $K$ or that $(12)(34)$ and all its 14 conjugates are in $K$. But this is not possible that $o(K) \leq 4$. Hence $o(K)=1$ and $\pi$ injective.