1. *Prove that G cannot be simple if*

a) $|G| = 45,\ 56,\ 80,\ 36$;

b) $|G| = p^a m$, *where p is a prime and $p > m > 1$, $a > 0$;*

c) $|G| = pq,\ p^2q$ *or* p^2q^2, *where p, q are prime numbers.*

Solution: a) If $|G| = 45 = 3^2 \cdot 5$ then $|Syl_5(G)| \equiv 1 \pmod 5$ and $|Syl_5(G)| \mid 9$, but of $1, 3$ and 9 only 1 satisfies the congruence, so $|Syl_5(G)| = 1$, implying that the Sylow 5-subgroup is normal.

If $|G| = 56 = 2^3 \cdot 7$, then $|Syl_7(G)| \equiv 1 \pmod 7$ and $|Syl_7(G)| \mid 8$ gives that $|Syl_7(G)| = 1$ or 8. If it is 1 then the Sylow 7-subgroup is normal. If it is 8 then, since the Sylow 7-subgroups have prime order, they are all disjoint and each contains 6 elements of order 7, there are altogether $8 \cdot 6 = 48$ elements of order 7 in G, so there remains a set S of $56 - 48 = 8$ elements for the rest. This implies that all the Sylow 2-subgroups are in S but they are of order 8, so S is the only Sylow 2-subgroup, hence $S \lhd G$.

If $|G| = 80$ then $|Syl_5(G)| \equiv 1 \pmod 5$ and $|Syl_5(G)| \mid 16$, and of the divisors $1, 2, 4, 8, 16$ only 1 and 16 is congruent to 1 modulo 5. If $|Syl_5(G)| = 1$ then the Sylow 5-subgroup is normal, if $|Syl_5(G)| = 16$, then similarly to the case of the group of order 56, we can count the elements of order 5: there are $16 \cdot 4 = 64$ such elements, so all the Sylow 2-subgroups are in the remaining set of cardinality $80 - 64 = 16$, and there is enough space there only for one Sylow 2-subgroup, so in this case the Sylow 2-subgroup is normal.

If $|G| = 36$ then we can deduce that there can be 1 or 4 Sylow 3-subgroups. If $|Syl_3(G)| = 1$ then the Sylow 3-subgroup is normal. Suppose now that $|Syl_3(G)| = 4$. We cannot apply now the previous argument for counting elements because the Sylow 3-subgroups may not be disjoint, so they may not cover so many elements. However we can find a group action of G whose kernel is a proper, nontrivial normal subgroup. Let us take the group action $\psi : G \to S_\Omega$, where $\Omega = Syl_3(G)$, and $\psi(g)$ acts on Ω by conjugation. Then by the third Sylow theorem we know that $\operatorname{Im}\psi$ acts transitively on Ω, so $\operatorname{Im}\psi \neq 1$, thus $\operatorname{Ker}\psi \neq G$. On the other hand, $\operatorname{Ker}\psi \neq 1$, either, since otherwise $\operatorname{Im}\psi \cong G/\operatorname{Ker}\psi = G$ would be a 36-element subgroup of the 24-element symmetric group $S_\Omega = S_4$. So we found a proper, nontrivial normal subgroup.

b) $|Syl_p(G)| \equiv 1 \pmod p$ implies that either $|Syl_p(G)| = 1$, in which case the Sylow p-subgroup is normal, or $|Syl_p(G)| \geq p + 1 > m$, which contradicts to $|Syl_p(G)| \mid m$.

c) We may assume in all three cases that $p \neq q$, otherwise G is a p-group of order greater than p, so its center contains an element of order p, which then generates a proper normal subgroup.

A group of order pq satisfies condition b) for p or q (whichever is greater), so the group is not simple.

The same holds when $|G| = p^2q$ and $p > q$. Suppose now that $|G| = p^2q$ and $p < q$. Then $|Syl_q(G)| \mid p^2$, so $|Syl_q(G)| = 1$, p or p^2. But $1 < p < q$, so $|Syl_q(G)| \equiv 1 \pmod q$ can only hold if it is 1 or p^2. In the first case the Sylow q-subgroup is normal. In the second we can count the elements of order q, similarly to the cases 56 or 80, and get that there are only $p^2q - p^2(q-1) = p^2$ elements whose order is not q, so there can be only be one Sylow p-subgroup.

If $|G| = p^2q^2$, then we may assume that $p > q$. Then $|Syl_p(G)| \mid q^2$ implies that $|Syl_p(G)| = 1, q$ or q^2 but $q \not\equiv 1 \pmod{p}$, so it is either 1 or q^2. If it is 1 then we are done. If it is q^2 then $q^2 \equiv 1 \pmod{p} \Rightarrow p \mid q^2 - 1 = (q-1)(q+1)$ but $q - 1 < p$, so $q < p \mid q + 1$, which implies $p = q + 1$, and this can only happen when $q = 2$ and $p = 3$, so $|G| = 36$. In this case, we already proved in part a) that G is not simple.

2. *Prove that A_5 is the smallest non-abelian simple group.*

Solution: Of the possible orders $1, 2, 3, \ldots, 59$, we can exclude 1 and the prime numbers because those groups are abelian, the higher prime powers because p-groups have nontrivial centers, so they have normal subgroups of order p, and all numbers of the form listed in problem 6.b),c). The only remaining orders are: 24, 30, 40, 45, 48, 56. The orders 45 and 56 were handled in 6.a).

If $|G| = 40$ then $|Syl_5(G)| \equiv 1 \pmod{5}$ and $|Syl_5(G)| \mid 8$ gives $|Syl_5(G)| = 1$, so G is not simple. If $|G| = 24$ or $|G| = 48$ then either the Sylow 2-subgroup is normal, or $|Syl_2(G)| = 3$. But in the latter case we have a transitive group action on $Syl_2(G)$, whose kernel cannot be trivial because both 24 and 48 are greater than $|S_3| = 6$. Since the kernel cannot be the whole G, either, by the transitivity of the group action, it is a proper, nontrivial normal subgroup.

Finally, if $|G| = 30$ then $|Syl_5(G)|$ is either 1 or 6, and in the first case the Sylow 5-subgroup is normal. Assume now that $|Syl_5(G)| = 6$. Then we can again use the method of counting the elements of order 5: there are $6 \cdot 4 = 24$ such elements, so all the remaining Sylow subgroups are in a 6-element subset S of G. However, if the Sylow 3-subgroup is not normal, then we have at least 4 Sylow 3-subgroups (since their number is congruent to 1 modulo 3), and they are all disjoint 3-element subgroups, so there should be at least $4 \cdot 2 = 8$ elements of order 3 in S, which is impossible.

Remark: It can also be proved that A_5 is the only simple group of order 60 up to isomorphism.

3. *a) What can be the number of Sylow 3-, 5- or 7-subgroups in a group G of order 105?*
b) Prove that one of the Sylow subgroups of G must be normal.
c) Prove that the Sylow 7-subgroup is always normal in G.

Solution: a) Let the number of Sylow 3-, 5- and 7-subgroups be n_3, n_5 and n_7. Then

$n_3 \mid 35$ and $n_3 \equiv 1 \pmod{3} \Rightarrow n_3 = 1$ or 7,
$n_5 \mid 21$ and $n_5 \equiv 1 \pmod{5} \Rightarrow n_5 = 1$ or 21,
$n_7 \mid 15$ and $n_7 \equiv 1 \pmod{7} \Rightarrow n_7 = 1$ or 15.

b) If $n_7 \neq 1$ then $n_7 = 15$, so the number of elements of order 7 is $15 \cdot 6 = 90$, and a subset S of $105 - 90 = 15$ elements contains all the other Sylow 5- and 3-subgroups. But if $n_5 \neq 1$ then $n_5 = 21$, and then S contains $21 \cdot 4 = 84$ elements of order 5, which is impossible. So either the Sylow 7-subgroup or the Sylow 5-subgroup is normal.

c) We have seen that either $n_7 = 1$ or $n_5 = 1$. In the latter case, let $Syl_5(G) = \{ N \}$. Consider the group G/N of order 21. Here the Sylow 7-subgroup must be normal, so there is a normal subgroup $M/N \lhd G/N$ or order 7, thus $M \lhd G$ and $|M| = 35$. But it can be easily seen that in a group of order 35 both the Sylow 5-subgroup and the Sylow 7-subgroup are normal, so for $P \in Syl_7(M)$, $P \lhd M$. Clearly, P is also a Sylow 7-subgroup of G. On the other hand, for every $g \in G$, $P^g \leq M^g = M$ is also a Sylow 7-subgroup of M, and $|Syl_7(M)| = 1$, so $P^g = P$. This proves that $P \lhd G$.

4. *By examining the Sylow subgroups, prove that every group of order* 15 *is cyclic.*

Solution: Let n_3 and n_5 be the number of Sylow 3- and 5-subgroups of a group G of order 15. Then
$n_3 \mid 5$ and $n_3 \equiv 1 \pmod 3 \Rightarrow n_3 = 1$ and
$n_5 \mid 3$ and $n_5 \equiv 1 \pmod 5 \Rightarrow n_5 = 1$.
So if $P \in Syl_3(G)$ and $Q \in Syl_5(G)$ then $P, Q \triangleleft G$. Furthermore, $|P|$ and $|Q|$ are coprime, so $P \cap Q = 1$, and $|PQ| = |P| \cdot |Q|/|P \cap Q| = 15$ gives that $PQ = G$, hence $G = P \times Q \cong C_3 \times C_5 \cong C_{15}$.

5. *Find a group of order* 21 *in* S_7.

Solution: First we investigate what we know about such a subgroup if it exists. Suppose $H \le S_7$ and $|H| = 21$. Furthermore, let $P \in Syl_7(H)$ and $Q \in Syl_3(H)$. It follows from the Sylow theorems, that $P \triangleleft H$ (see the solution of problem 1.c), case pq), and since $|P|$ is a prime, $P \cong C_7$. Let $P = \langle a \rangle$. Then $o(a) = 7$, so in S_7 a can only be a 7-cycle, say $a = (1234567)$. Furthermore, Q is also cyclic, and it normalizes P, that is, $Q = \langle b \rangle$, $o(b) = 3$, and $a^b \in \langle a \rangle$, implying that $a^b = a^k$ for some k. The element b cannot centralize a because then $o(ab) = 21$, and there is no such element is S_7, on the other hand, $a = a^{b^3} = ((a^b)^b)^b = a^{k^3}$, so we need a k such that $k^3 \equiv 1 \pmod 7$ but $k \not\equiv 1 \pmod 7$, and $k = 2$ satisfies this.
Now we want to find an element of order 3 that conjugates a to a^2. An element of order 3 in S_7 is either a 3-cycle or the product of two disjoint 3-cycles, in either case, it must have a fixed-point. We may try to make 1 fixed, so when finding a conjugating element, we start the cycle in a^2 with a 1: $(1234567)^b = (1357246)$, and we get $b = (235)(476)$. Since this b has order 3, we got that $H = \langle a, b \rangle = \langle a \rangle \langle b \rangle$ (note that for the latter equation we needed that $\langle b \rangle \le N_H(\langle a \rangle)$) has order 21, and this is what we wanted.

6. *Consider the pure imaginary elements of the quaternions* $\mathbb{H}$ *as vectors of* $\mathbb{R}^3$ *(where* i, j, k *are the elements of the standard basis). Show that the product of the vectors* $\mathbf{u}, \mathbf{v} \in \mathbb{R}^3$ *in* $\mathbb{H}$ *is* $-\mathbf{uv} + \mathbf{u} \times \mathbf{v}$*, where* $\mathbf{uv}$ *is the dot product and* $\mathbf{u} \times \mathbf{v}$ *is the cross product in* $\mathbb{R}^3$.

Solution: Let $u = ai+bj+ck$ and $v = a'i+b'j+c'k$. Then $uv = (ai+bj+ck)(a'i+b'j+c'k) = aa'i^2 + bb'j^2 + cc'k^2 + ab'ij + ba'ji + ac'ik + ca'ki + bc'jk + cb'kj = -aa' - bb' - cc' + ab'k - ba'k - ac'j + ca'j + bc'i - cb'i = -(aa' + bb' + cc') + ((bc' - cb')i - (ac' - ca')j + (ab' - ba')k)$, where the first summand is, indeed, $-\mathbf{uv}$, and the second is $\mathbf{u} \times \mathbf{v}$ as vector products.

7. *Let* G *be a finite group and* $R = KG$ *the group algebra of* G *over* K. *Prove that* $I = K(\sum_{g \in G} g)$ *and* $J = \{ \sum_{g \in G} \lambda_g g \mid \sum_{g \in G} \lambda_g = 0 \}$ *are both ideals in* R*, and also subspaces in the vector space* KG_K.

Solution: Let $u = \sum_{g \in G} g$. Then $I = Ku = \{ \lambda u \mid \lambda \in K \}$ is the one-dimensional subspace of R_K as a vector space, so it is nonempty, and closed under addition and subtraction. So to prove that I is an ideal, the only thing left to be shown is that it is also closed under multiplication by elements of R. For $h \in G$, $uh = \sum_{g \in G} gh = \sum_{x \in G} x = u$, since every element of G can be obtained as gh for some g ($x = (xh^{-1})h$), and each element x occurs only once in the sum ($gh = g'h \Rightarrow g = ghh^{-1} = g'hh^{-1} = g'$). Thus $(\lambda u)(\sum_{h \in G} \mu_h h) = \sum_{h \in G} \lambda \mu_h uh =$

$\sum\limits_{h\in G} \lambda\mu_h u \in I$. Similarly, $hu = u$ for every $h \in G$, so $(\sum\limits_{h\in G} \mu_h h)(\lambda u) = \sum\limits_{h\in G} \lambda\mu_h u \in I$.
J contains 0, and it is closed under scalar multiplication and addition: for $\alpha \in K$, $u = \sum\limits_{g\in G} \lambda_g g$ and $v = \sum\limits_{g\in G} \mu_g g$ in J, the sum of coefficients of αu is
$\sum\limits_{g\in G} \alpha\lambda_g = \alpha \cdot \sum\limits_{g\in G} \lambda_g = \alpha 0 = 0$, and that of $u + v$ is
$\sum\limits_{g\in G} (\lambda_g + \mu_g) = (\sum\limits_{g\in G} \lambda_g) + (\sum\limits_{g\in G} \mu_g) = 0 + 0 = 0$, so J is a subspace, consequently, it is also closed under addition and subtraction. As for multiplication by elements of R, we again only have to check the multiplication by the basis elements, the others are linear combinations of these products. For $u = \sum\limits_{g\in G} \lambda_g g \in J$ and $h \in G$, we have $uh = \sum\limits_{g\in G} \lambda_g gh$, and here, as in the case of I, gh runs over all the elements of G as g runs over G, so the sum of coefficients of uh is the same as that of u, that is, 0, thus $uh \in J$, and similarly, $hu \in J$.

8. *Prove that $\mathbb{H}$ is not isomorphic to $\mathbb{R}Q$ where Q is the quaternion group.*

Solution: We have proved that $\mathbb{H}$ is a division ring. But we can show that there are zero divisors in $\mathbb{R}Q$, so it cannot be a division ring, consequently, it cannot be isomorphic to $\mathbb{H}$. We shall write the elements of Q in boldface, to distinguish the $\mathbf{1}$ and $-\mathbf{1}$ of the group from the elements 1 and -1 of the field. Then $a = 1\cdot\mathbf{1} + 1\cdot(-\mathbf{1})$ and $b = 1\cdot\mathbf{1} + (-1)\cdot(-\mathbf{1})$ are nonzero elements in the group algebra ($\mathbf{1}$ and $-\mathbf{1}$ are linearly independent) but $ab = 1\cdot\mathbf{1}^2 + 1\cdot(-\mathbf{1})\mathbf{1} + (-1)\cdot\mathbf{1}(-\mathbf{1}) + (-1)\cdot(-\mathbf{1})^2 = (1+(-1))\cdot\mathbf{1} + (1+(-1))\cdot(-\mathbf{1}) = 0\mathbf{1} + 0(-\mathbf{1}) = 0$.

9. *What can we say about a ring R where the set $\{0, a\}$ is an ideal of R for every $a \in R$?*

Solution: First of all, $a + a$ can only be 0, so the additive group of the ring is a vector space over $\mathbb{Z}_2$. Furthermore, if $|R| \geq 3$ then for any $0 \neq a \in R$ and $a \neq b \in R$, we have $ab, ba \in \{a, 0\} \cap \{b, 0\} = \{0\}$, so $ab = ba = 0$. But there exists $b \in R \setminus \{a, 0\}$, and for this, $a + b \neq a$, so $0 = a(a + b) = aa + ab = aa$ for any $a \neq 0$ (and clearly, also for $a = 0$), so R can only be a zero ring.
In case $|R| \leq 2$, the condition does not give any restriction, since $\{0\}$ and R are always ideals of R. Besides the zero ring, this gives only $\mathbb{Z}_2$.

HW1. *Let G be a group of order* 140. *Prove that G has at least two normal Sylow subgroups. Using this, show that G has an element of order* 35.

HW2. *Prove that the nilpotent elements (that is, the elements r for which there exists a positive integer n with $r^n = 0$) of a commutative ring form an ideal.*