Solutions of exercise sheet 8

1. In this exercise, we will give a characterization for solvable groups using commutator subgroups. See last semester's (Algebra I, HS 2014) Exercise Sheet 3, Exercise 6, for the definition and some properties of the commutator subgroup.

1. Let G be a group and $G_1 \trianglelefteq G$ a normal subgroup such that G/G_1 is abelian. Show that
$$[G, G] \subseteq G_1.$$
2. Deduce that G is solvable if and only if there exists $m \geq 1$ such that $G^{(m)} = \{1\}$, where the $G^{(m)}$ are subgroups defined inductively via
$$G^{(0)} = G$$
$$G^{(i+1)} = [G^{(i)}, G^{(i)}].$$

Solution: Recall that for a monic polynomial $f \in \mathbb{Z}[X]$ we know that f is irreducible in $\mathbb{Z}[X]$ if and only if it is irreducible in $\mathbb{Q}[X]$

1. By Point 4 of the Exercise referred to in the problem, the commutator $[G, G]$ lies in the kernel of the projection map $G \longrightarrow G/G_1$, because G/G_1 is abelian by hypothesis. This kernel is clearly G_1, so that $[G, G] \subseteq G_1$.
2. By Point 1 and 3 of the Exercise referred to in the problem, the $G^{(i)}$ form a subnormal series with abelian quotients, so that if $G^{(m)}$ is trivial for some $m \geq 1$, then G is solvable.

   Conversely, suppose that G is solvable with a subnormal sequence with abelian quotients
$$\{1\} = G_m \trianglelefteq G_{m-1} \trianglelefteq \cdots \trianglelefteq G_1 \trianglelefteq G_0 = G.$$
   We can prove that $G^{(m)} = \{1\}$ by checking with an induction on $k \geq 0$ that $G^{(k)} \subseteq G_k$. This property is trivial for $k = 0$ and it is the previous point for $k = 1$. Moreover, whenver $G^{(k)} \subseteq G_k$, one gets
$$G^{(k+1)} = [G^{(k)}, G^{(k)}] \subseteq [G_k, G_k] \subseteq G_{k+1},$$
   where the first inclusion is immediate from the definition of commutator and the second is immediate from the first point.

2.
1. Show that S_3 and S_4 are solvable groups.
2. Show that the group A_5 is generated by the two permutations $(1\ 2)(3\ 4)$ and $(1\ 3\ 5)$.

Please turn over!

3. Show that $[S_5, S_5] = A_5$ and deduce that the group S_5 is not solvable.

Solution:

1. It is clear that $\{1\} \subseteq A_3 \subseteq S_3$ is a subnormal sequence with abelian quotients, so that S_3 is solvable.
   For S_4, notice that
   $$V = \{\mathrm{id}, (1\ 2)(3\ 4), (1\ 4)(2\ 3), (1\ 3)(2\ 4)\} \trianglelefteq A_4.$$
   It is indeed easy to check that it is a subgroup with the same group structure of $C_2 \times C_2$, and normality is immediate from the fact that it is the union of the permutations of cycle type $1+1+1+1$ and $2+2$ in S_4, so that one has $V_4 \trianglelefteq S_4$ and in particular $V_4 \trianglelefteq A_4$. Then $|A_4/V_4| = 12/4 = 3$, so that A_4/V_4 is cyclic and hence abelian. Then we can embed a C_2 in V_4 as $C_2 = \{\mathrm{id}, (1\ 2)(3\ 4)\}$. In conclusion, the following is a subnormal sequence with abelian quotients:
   $$\{1\} \trianglelefteq C_2 \trianglelefteq V_4 \trianglelefteq A_4 \trianglelefteq S_4,$$
   so that S_4 is solvable.
2. We have that $|S_5| = 5! = 120$, so that $|A_5| = 60$. Let $H = \langle (1\ 2)(3\ 4), (1\ 3\ 5)\rangle$. Clearly $H \leq A_5$ because it is generated by even permutations. Let us first notice that H contains an element of order 5:
   $$H \ni (1\ 2)(3\ 4)(1\ 3\ 5) = (1\ 4\ 3\ 5\ 2).$$
   This means that $|H|$ is divisible by 2 (the order of $(1\ 2)(3\ 4)$), 3 (the order of $(1\ 3\ 5)$) and 5, so that $|H|$ is divisible by 30. Suppose by contraddiction that $|H| = 30$. Then $[A_5 : H] \in$ so that H would be a normal subgroup of A_5, which is simple, contraddiction. Hence $H = A_5$.
3. Clearly $[S_5, S_5]$ because commutators are even permutation by construction. For the other inclusion, by the previous point it is enough to prove that $(1\ 2)(3\ 4)$ and $(1\ 3\ 5)$ lie in $[S_5, S_5]$. This is quite immediate using conjugation in S_5 (more precisely, the fact that conjugation classes consist of elements with the same cycle type):
   - $(1\ 2)$ is conjugated to $(3\ 4)$, so that for some $g \in S_5$ we have $g(1\ 2)g^{-1} = (3\ 4)$, so that
     $$[(1\ 2), g] = (1\ 2)g(1\ 2)g^{-1} = (1\ 2)(3\ 4) \in [S_5, S_5].$$
   - $(1\ 3)$ is conjugated to $(3\ 5)$, so that for some $g \in S_5$ we have $g(1\ 3)g^{-1} = (3\ 5)$, so that
     $$[(1\ 3), g] = (1\ 3)g(1\ 3)g^{-1} = (1\ 3)(3\ 5) = (1\ 3\ 5) \in [S_5, S_5].$$

   This proves that $[S_5, S_5] = A_5$. Since A_5 is simple, $[A_5, A_5]$ is either trivial or equal to A_5. If we prove that it is non-trivial, then we can conclude that A_5 and S_5 are not solvable because of Exercise 1.

See next page!

3. Let K be a field and consider the group

$$B_2 = \left\{ \begin{pmatrix} a & x \\ 0 & b \end{pmatrix} \middle| a, b \in K^\times, x \in K \right\} \leq \mathrm{GL}_2(K).$$

Show that B_2 is solvable.

Can you find a generalization to the subgroup B_n of upper-triangular matrices in $\mathrm{GL}_n(K)$, for $n \geq 2$?

Solution: For $n \geq 1$, we consider the invertible upper-triangular matrices

$$B_n = \{(a_{ij})_{1 \leq i,j \leq n} : a_{ij} = 0 \text{ for } j < i, a_{ii} \in K^\times\} \leq \mathrm{GL}_n(K).$$

We claim that B_n is solvable (and consider n fixed). It is easy to check that the map

$$\begin{aligned} \pi_0 : B_n &\longrightarrow (K^\times)^n \\ (\lambda_{ij})_{i,j} &\mapsto (\lambda_{ii}) \end{aligned}$$

is a surjective group homomorphism. Let $M_0 = \ker(\pi_0)$. Then $B_n/M_0 \cong (K^\times)^n$ is abelian. Notice that M_0 consists of the upper-triangular matrices with 1 in all entries of the diagonal. We know find a normal subsequence of M_0 by considering matrices with more and more zeroes. Define, for $k = 0, 1, \ldots, n-1$,

$$N_k = \{(a_{ij})_{i,j} \in M_0 | a_{ij} = 0 \text{ for } 1 \leq j - i \leq k\}.$$

Those are easily seen to be subgroups of M_0 satisfying $N_k \leq N_{k-1}$ for all k. Moreover, $N_0 = M_0$ and $N_{n-1} = \{1\}$. Indeed, N_k is the subgroup of matrices with 1 in the principal diagonal, and zeroes in the first k upper partial diagonals. We want to prove that N_k is a normal subgroup of N_{k-1} with abelian quotient for each $k = 1, \ldots, n$ in order to conclude. This is easily done by observing that for $k = 1, \ldots, n$ the maps

$$\begin{aligned} p_k : N_{k-1} &\longrightarrow K^{n-k} \\ (\lambda_{ij})_{i,j} &\mapsto (\lambda_{i,j+k}) \end{aligned}$$

are surjective group homomorphisms. Indeed, those maps just copy out the first upper partial diagonal which is not required to be vanishing, so that $N_k = \ker(p_k)$ for each k, implying normality and commutativity of the quotient (which is just isomorphic to a power of K).

In conclusion, we have a subnormal sequence with abelian quotients

$$\{1\} = N_{n-1} \trianglelefteq N_{n-2} \trianglelefteq \cdots \trianglelefteq N_1 \trianglelefteq N_0 = M_0 \trianglelefteq B_n.$$

4. *(Gauss's Lemma)* Let R be a UFD and $K = \mathrm{Frac}(R)$. We say that the elements $a_1, \ldots, a_n \in R$ are *coprime* if whenever $u | a_i$ for each i, then $u \in R^\times$. We call a non-zero polynomial $p \in R[X]$ *primitive* if its coefficients are coprime. Prove the following statements:

Please turn over!

1. Each irreducible element in R (i.e., a non-zero non-unit in R which cannot be written as product of two non-units) is prime in R (i.e., whenever it divides a product bc, then it divides b or c).
2. If $a, b \in R$ are coprime and $b|ac$ for some $c \in R$, then $b|c$.
3. Any element $\lambda \in K$ can be written as a quotient $\lambda = a/b$, with $a, b \in R$ coprime elements.
4. The product of two primitive polynomials $p, q \in R[X]$ is a primitive polynomial. [*Hint:* For d an irreducible element, notice that there is an isomorphism of rings $R[X]/dR[X] \cong (R/dR)[X]$, and deduce that $R[X]/dR[X]$ is an integral domain.]
5. If $f \in R[X]$ can be factored as $f = gh$ with $g, h \in K[X]$, then there exist $g', h' \in R[X]$ such that $f = g'h'$ and $g = \lambda g'$ for some $\lambda \in K$. [*Hint:* Prove that one can write $g = \gamma \cdot G$ for some $\gamma \in K$ and $G \in R[X]$ primitive polynomial. You main need to use the three previous points.]
6. A polynomial $f \in R[X]$ is irreducible in $R[X]$ if and only if it is primitive and it is irreducible in $K[X]$.

The last three statements are usually referred to as Gauss's Lemma.

Solution:

1. Let $d \in R$ be an irreducible element, and suppose that $d|ac$ for some $a, c \in R$. Then we can write $de = ac$. Decomposing a, c and e into irreducible and applying uniqueness (up to reordering and multiplication by units) of the decomposition we get that d necessarily divides one of the irreducible factors of ac, and such a factor is either a divisor of a or c, so that $d|a$ or $d|c$.
2. This is a slight generalization of the previous point. Under the given hypothesis we can write $be = ac$ for some $e \in R$. Decomposing a, b, c and e into irreducibles and applying uniqueness (up to reordering and multiplication by units) of the decomposition we see that each of the irreducible factors of b can be associated to a divisor of c to which it is equivalent (where d, d' are said to be equivalent if $d = ud'$ for some $d \in R^\times$), since an irreducible factor of b cannot divide a by hypothesis, so that it cannot divide a divisor of a. Writing each irreducible factor d' of c which has been associated to some irreducible factor d of c as $d' = uc$ for some $u \in R^\times$, and denoting by $v \in R^\times$ the product of all the units u obtained this way and by $t \in R$ the product of the remaining divisors of c we get $c = vbt$, so that $b|c$.
3. Each $\lambda \in K$ can be written as α/β for some $\alpha, \beta \in R$ by definition of fraction field. Decomposing β into irreducible factors, we can proceed by induction on the number $n_{\alpha,\beta}$ of irreducible factors - counted with multiplicity - appearing in this decomposition which divide α (this quantity is actually indipendent on the chosen decomposition) in order to prove that α/β is equivalent to a fraction with coprime numerator and denominator. The case $n_{\alpha,\beta} = 0$ is immediate because there we can conclude that α and β are coprime. For $n_{\alpha,\beta} > 0$, pick an irreducible factor d of β dividing α. Then by uniqueness of decomposition $\alpha = ud\alpha'$ for some $u \in R^\times$

See next page!

and $\alpha' \in R$, and α/β is equivalent to $u\alpha'/\beta'$, where $\beta' = \beta/d$. It is immediate to see that $n_{\alpha',\beta'} = n_{\alpha,\beta} - 1$, so that we can make the induction work.

4. Saying that $f \in R[X]$ is primitive is equivalent to saying that for each irreducible element of R one has that $f + dR[X] \in R[X]/dR[X]$ is non trivial. Indeed, f is primitive if and only if it is not divisible by any non-unit in R, if and only if it is not divisible by any irreducible element in R (since non-units in R are all divisible by some irreducible element in R). Following the hint, one easily check that the unique ring homomorphism

$$\gamma_d : R[X] \longrightarrow (R/dR)[X]$$

sending $X \mapsto X$ and $R \ni r \mapsto r + dR$ is surjective and has kernel $dR[X]$, so that $R[X]/dR[X] \cong (R/dR)[X]$, which is a domain because d is prime in R by Point 1, and as such generates a prime ideal in R.

The claim follows them immediately by testing primitivity of p, q and pq via the given characterization on the quotient rings $R[X]/dR[X]$.

5. Collecting all the irreducible factors in the numerators separately by those in the denominators, we can write

$$g = \frac{a}{c}\bar{g} \quad \text{and} \quad h = \frac{a'}{c'}\bar{h},$$

for some $a, a', c, c' \in R$ with a coprime with c and a' coprime with c' (Point 3), and some primitive polynomials $\bar{g}, \bar{h} \in R[X]$. Then

$$f = \frac{aa'}{cc'}\bar{g}\bar{h},$$

where $\bar{g}\bar{h}$ is primitive by Point 4. We write $\alpha/\beta = aa'/cc'$ for some coprime α and β. Since $\frac{\alpha}{\beta}t \in R$ for each coefficient t of $\bar{g}\bar{h}$, by Point 2 applied for each t we obtain that β divides each coefficient of $\bar{g}\bar{h}$, so that $\beta \in R^\times$ because $\bar{g}\bar{h}$ is primitive, and $\alpha/\beta \in R$. Then we can conclude that $f = g'h'$ for

$$g' = \frac{a'}{c'}g \quad \text{and} \quad h' = \frac{c'}{a'}h,$$

and $g', h' \in R[X]$.

6. Suppose that f is irreducible in $R[X]$. Then it needs to be primitive (since $R[X]^\times = R^\times$), and it is irreducible in $K[X]$ by the previous point.

Conversely, suppose that f is irreducible in $K[X]$ and primitive. Irreducibility of f in $K[X]$ excludes decompositions of f into non-constant factors of $R[X]$, while primitivity excludes factorizations of f with a constant factor. Hence f is irreducible in $R[X]$.