Exercise sheet 14

[Groups]

1. Let G and H be groups and $\varphi : G \longrightarrow H$ a group homomorphism. If $N \lhd G$ is a normal subgroup, and φ is surjective, then show that $\varphi(N) \lhd H$.

Solution:

It is enough to check that for every $h \in H$ one has $h\phi(N)h^{-1} \subseteq \phi(N)$. As ϕ is surjective, for every $h \in H$ there exists $g_h \in G$ such that $\phi(g_h) = h$. Then for each $x = \phi(n) \in \phi(N)$, where $n \in N$, we have

$$h\phi(n)h^{-1} = \phi(g_h)\phi(n)\phi(g_h)^{-1} = \phi(g_h n g_h^{-1}),$$

where the last equality comes from the fact that ϕ is a group homomorphism. Then since $N \lhd G$ and $n \in N$, we have that $g_h n g_h^{-1} \in N$, implying that $h\phi(n)h^{-1} = \phi(g_h n g_h^{-1}) \in \phi(N)$. We can then conclude that $h\phi(N)h^{-1} \subseteq \phi(N)$ for each $h \in H$, and $\phi(N) \lhd H$.

2. Let $\varphi : G \longrightarrow H$ be a set-theoretic map between groups. Show that φ is a homomorphism if and only if the graph

$$\Gamma_\varphi = \{(x, y) \in G \times H \mid y = \varphi(x)\}$$

is a subgroup of $G \times H$. When is it a normal subgroup?

Solution:

Of course $(1_G, \phi(1_H)) \in \Gamma_\phi$, so that Γ_ϕ is never empty. Each element of Γ_ϕ is of the form $(u, \phi(u))$, for $u \in G$. Now Γ_ϕ is a subgroup of $G \times H$ if and only if for each $\alpha, \beta \in \Gamma_\phi$ one has $\alpha\beta^{-1} \in \Gamma_\phi$. Writing down $\alpha = (u, \phi(u))$ and $\beta = (v, \phi(v))$, we have that $\Gamma_\phi \leq G \times H$ if and only if $(uv^{-1}, \phi(u)\phi(v)^{-1}) \in \Gamma_\phi$ for each $u, v \in G$, which is equivalent to saying that

$$(*)\ \phi(uv^{-1}) = \phi(u)\phi(v)^{-1}, \quad \forall u, v \in G.$$

This last property is satisfied when ϕ is a group homomorphism, so we are only left to prove that $(*)$ implies that ϕ is a group homomorphism. Applying $(*)$ with $u = v = 1$, we get $\phi(1) = 1$. Then applying $(*)$ with $u = 1$, we get that $\phi(v^{-1}) = \phi(v)^{-1}$ for each $v \in G$. Finally, applying $(*)$ with $v = w^{-1}$, we can conclude that

$\phi(uw) = \phi(u)\phi(w^{-1})^{-1} = \phi(u)\phi(w)$ for each $u, w \in G$, meaning that ϕ is a group homomorphism.

We now want to characterize when $\Gamma_\phi \lhd G \times H$. This happens if and only if Γ_ϕ is stable under conjugation by elements of $G \times H$, that is, if and only if

$$\forall u, g \in G, \forall h \in H, (gug^{-1}, h\phi(u)h^{-1}) \in \Gamma_\phi.$$

This last condition is equivalent to saying that, for u, g and h as above, one has $\phi(gug^{-1}) = h\phi(u)h^{-1}$, i.e., assuming that ϕ is a group homomorphism (which is a necessary condition), $\phi(u) = \phi(g)^{-1}h\phi(u)(\phi(g)^{-1}h)^{-1}$. Since $\phi(g)^{-1}h$ ranges over all the elements of H, we can say that $\Gamma_\phi \lhd G \times H$ if and only if

$$\forall u \in G, \forall h \in H, \phi(u) = h\phi(u)h^{-1}.$$

This last condition is equivalent to saying that $\phi(G) \subseteq Z(H)$. We can conclude that $\Gamma_\phi \lhd G \times H$ if and only if ϕ is a group homomorphism whose image lies in the center of H.

3. Let G_1 and G_2 be two groups, and let $G = G_1 \times G_2$ be their direct product. Let H be a subgroup of G. We denote by $\pi_i : G \longrightarrow G_i$ the two projection maps to the factors of G, and by $K_i < H$ the kernel of the restriction of π_i to H. We assume that the restrictions of π_1 and π_2 to H are both surjective.

1. Show that π_1 induces by restriction an isomorphism $K_2 \longrightarrow N_1$ where N_1 is a normal subgroup of G_1.
2. Show that if $N_1 = G_1$, then $H = G_1 \times G_2$.
3. Suppose in addition that G_1 and G_2 are simple groups. If $N_1 = \{1\}$, show that $K_1 = \{1\}$ as well. Show in that case that H is the graph of an isomorphism $G_1 \longrightarrow G_2$.

Solution:

1. Let $\pi_i' := \pi_i|_H : H \longrightarrow G_i$, so that $K_i = \ker(\pi_i') = \ker(\pi_i) \cap H$. Since π_1' is a surjective map and $K_2 = \ker(\pi_2')$ is a normal subgroup of H, we have that $N_1 := \pi_1(K_2) = \pi_1'(K_2)$ is a normal subgroup of G_1 by Exercise 1. Then π_1' restricts to a surjective map $K_2 \longrightarrow N_1$, whose kernel is $\ker(\pi_1') \cap K_2$. This intersection lies in $\ker(\pi_1) \cap \ker(\pi_2)$, which is easily seen to be trivial by writing down the element of G as couples of elements in G_1 and G_2. Thus π_1 restricts to an isomorphism $K_2 \longrightarrow N_1$ as desired.
2. If $G_1 = N_1 = \pi_1(K_2)$, then $(\lambda, 1) \in H$ for each $\lambda \in G_1$. Also, by surjectivity of π_2, for each $\mu \in G_2$ there exists $\lambda_\mu \in G_1$ such $(\lambda_\mu, \mu) \in H$, so that $(1, \mu) = (\lambda_\mu, \mu) \cdot (\lambda_\mu^{-1}, 1) \in H$. In conclusion, for $g_i \in G_i$, we have $(g_1, g_2) = (g_1, 1) \cdot (1, g_2) \in H$, meaning that $H = G_1 \times G_2$.

See next page!

3. If $N_1 = \{1\}$, then by Point 1 we have $K_2 = 1$. Interchanging the indexes 1 and 2 in Point 1, one easily proves that π_2 restricts to an isomorphism $K_1 \longrightarrow N_2 := \pi_2(K_1)$ with $N_2 \lhd G_2$. As G_2 is simple, there are only possibilities: either $N_2 = G_2$ or $N_2 = \{1\}$. In the first case one gets, similarly as in Point 2, that $H = G_1 \times G_2$, so that $K_2 = G_1 \times \{1\} \neq \{1\}$ (as $G_1 \neq \{1\}$ because it is simple), contradiction. Hence $N_2 = K_1 = \{1\}$.

   Now we prove that $H \subseteq G_1 \times G_2$ is a graph of a map $\phi : G_1 \longrightarrow G_2$. This is equivalent to say that if $(g_1, g_2), (g_1, g_2) \in H$ for $g_1 \in G_2$ and $g_2, g_2' \in G_2$, then $g_2 = g_2'$. This implication is true since, the first condition implies $(1, g_2^{-1}g_2') \in H$, so that $g_2^{-1}g_2' = 1$ (and $g_2 = g_2'$) because $K_1 = \{1\}$.

   Then ϕ is a group homomorphism because $H \leq G_1 \times G_2$ (see Exercise 2). ϕ is surjective because π_2' is. Moreover, $\ker(\phi) = \{g \in G_1 : (g, 1) \in H\} = \{1\}$ since $K_2 = \{1\}$. Hence ϕ is a bijective, implying that it is a group isomorphism.

[**Rings**]

4. Let A be an integral domain and K its fraction field. Show that if B is any ring, then there is a "natural" bijection

$$\{\text{ring morphisms } \psi : K \longrightarrow B\} \longrightarrow$$
$$\{\text{ring morphisms } \varphi : A \longrightarrow B \text{ such that } \varphi(x) \in B^\times \text{ for all } x \neq 0 \text{ in } A\}.$$

Solution:

Let

$$X = \{\text{ring morphisms } \psi : K \longrightarrow B\} \text{ and}$$
$$Y = \{\text{ring morphisms } \varphi : A \longrightarrow B \text{ such that } \varphi(x) \in B^\times \text{ for all } x \neq 0 \text{ in } A\}.$$

Consider the canonical embedding $j : A \longrightarrow K$, with $j(a) = \frac{a}{1}$. Then we define $\varrho : X \longrightarrow Y$ as the restriction map sending $\psi \mapsto \psi|_A = \psi \circ j$. We have that ϱ is a map because for every $\psi \in X$ the map $\psi \circ j$ is a ring morphism (being a composition of ring morphisms), and for $x \in A \setminus \{0\}$ it gives $\psi(x)\psi\left(\frac{1}{x}\right) = 1$ in B, so that $\psi(x) \in B^\times$.

Let us now prove that ϱ is a bijection:

- ϱ is injective: let $\psi, \psi' \in X$, and suppose that $\varrho(\psi) = \varrho(\psi')$. This means that $\psi|_A = \psi'|_A$. Then for each $a, c \in A$, with $c \neq 0$, we get

  $$\psi\left(\frac{a}{c}\right) = \psi(a)\psi(c)^{-1} = \psi'(a)\psi'(c)^{-1} = \psi'\left(\frac{a}{c}\right),$$

  so that $\psi = \psi'$.

Please turn over!

- ϱ is surjective: we just need to prove that each map $\phi : A \longrightarrow B$ such that $\phi(x) \in B^\times$ for all $x \neq 0$ does admit an extension $\psi : K \longrightarrow B$ such that $\psi|_A = \phi$. This is easily done by defining $\psi\left(\frac{a}{c}\right) := \phi(a)\phi(c)^{-1}$ for each $a, c \in A$ with $c \neq 0$. The map ψ is well-defined: suppose that $\frac{a}{c} = \frac{a'}{c'}$ with $c, c' \neq 0$, so that $ac' = a'c$; then $\phi(c), \phi(c') \in B^\times$, and

$$\phi(cc')(\phi(a)\phi(c)^{-1} - \phi(a')\phi(c')^{-1}) = \phi(a)\phi(c') - \phi(a')\phi(c) = \phi(ac' - a'c) = 0,$$

and being $\phi(cc') \in B^\times$ we get $\phi(a)\phi(c)^{-1} = \phi(a')\phi(c')^{-1}$. Also, ψ is a ring morphism: $\psi(1) = 1$, and for $a, a', c, c' \in A$ with $c, c' \neq 0$ we obtain

$$\begin{aligned}\psi\left(\frac{a}{c} + \frac{a'}{c'}\right) &= \psi\left(\frac{ac' + a'c}{cc'}\right) = \varphi(ac' + a'c)\varphi(cc')^{-1} = \\ &= \varphi(a)\varphi(c)^{-1} + \varphi(a')\varphi(c')^{-1} = \psi\left(\frac{a}{c}\right) + \psi\left(\frac{a'}{c'}\right) \quad \text{and} \\ \psi\left(\frac{a}{c} \cdot \frac{a'}{c'}\right) &= \psi\left(\frac{ac' + a'c}{cc'}\right) = \varphi(aa')\varphi(cc')^{-1} = \\ &= \varphi(a)\varphi(c)^{-1}\varphi(a')\varphi(c')^{-1} = \psi\left(\frac{a}{c}\right) \cdot \psi\left(\frac{a'}{c'}\right).\end{aligned}$$

Clearly, $\psi(a) = \psi(\frac{a}{1}) = \varphi(a)\varphi(1)^{-1} = \varphi(a)$, so that $\psi|_A = \varphi$ and we have proven that ϱ is surjective.

5. Let A be an integral domain and K its fraction field. Let $I \subset A$ be a *non-zero* prime ideal. Denote

$$A_I = \{x \in K \mid x = a/b \text{ for some } a \text{ and } b \text{ in } A \text{ with } b \notin I\}.$$

1. Show that A_I is a subring of K, and that $A \subset A_I$.
2. Let $J = IA_I$ be the ideal in A_I generated by I. Show that

$$J = \{x \in K \mid x = a/b \text{ for some } a \in I \text{ and some } b \text{ in } A - I\}.$$

3. Show that J is a maximal ideal in A_I, and that it is the unique maximal ideal.
4. Show that the natural ring homomorphism

$$A \longrightarrow A_I/J$$

induces an injective ring homomorphism $A/I \longrightarrow A_I/J$.

1. First, $A_I \subseteq K$ by definition. I is a prime ideal, so that $I \neq A$ and $1 \notin I$. Thus for each $a \in A$, we have that $a = \frac{a}{1} \in A_I$, meaning that $A \subseteq A_I$. In particular, A_I contains 0 and 1. Also, for each $a/b \in A_I$, written with $b \notin I$, we have $-\frac{a}{b} = \frac{-a}{b} \in A_I$, so that we are only left to prove that A_I is stable under sum and multiplication. This is immediate: the denominator of a sum or multiplication of two fractions a/b and a'/b' can always be taken to be the product bb' of the two denominators. But for $b, b' \notin I$, one needs to have $bb' \notin I$ (as I is a prime ideal).

See next page!

2. Let $x \in K$. If $x \in J$, then $x = m \cdot \frac{u}{b} = \frac{mu}{b}$ for some $m \in I$, $u \in A$ and $b \in A \setminus I$. Of course, $mu \in I$, so that $x = \frac{a}{b}$ with $a = mu \in I$ and $b \in A \setminus I$. Clearly, each x of this form $\frac{a}{b}$ can also be written as $a \cdot \frac{1}{b} \in J$, whence the desired description

$$J = \{x \in K \mid x = a/b \text{ for some } a \in I \text{ and some } b \text{ in } A - I\}.$$

3. We claim that $J = A_I \setminus A_I^\times$. Given the claim, each ideal J' of A_I strictly containing J does contain a unit and is forced to be the unit ideal, so that J is maximal. Moreover every maximal ideal of A_I does not contain any unit, so that it is contained in J and has to coincide with J by maximality. So we can conclude that J is the unique maximal ideal of A_I. Now we prove the claim:
   - $A_I^\times \cap J = \varnothing$: Suppose that $a/b \in A_I$, with $b \notin I$, is invertible in A_I. Writing $\frac{b}{a} = \frac{c}{d}$ in such a way that $d \notin I$, we get $bd = ac$. But $bd \notin I$ as I is a prime ideal, so that $a \notin I$. Now suppose that $\frac{a}{b} = \frac{e}{f}$ with $f \notin I$. The equality $af = be$ implies that I does not contain e (using the fact that I does not contain a, b and f and again that I is a prime ideal), so hat $\frac{a}{b} \notin J$.
   - $A_I^\times \cup J = A_I$: Suppose that $\frac{a}{b} \in A_I$, with $b \notin I$, does not lie in J. Then we get $a \notin I$, so that $\frac{b}{a} \in A_I$ and $\frac{a}{b} \in A_I^\times$.

   This proves that J consists of all non-units, which was our initial claim.

4. We claim that the natural ring homomorphism $p : A \longrightarrow A_I/J$ sending $a \mapsto \frac{a}{1} + J$ has kernel equal to I. Then, by the First Isomorphism Theorem for ring homomorphisms, p induces injective ring homomorphism $\bar{p} : A/I \longrightarrow A_I/J$ sending $a + I \mapsto p(a)$. To conclude, we show that indeed $\ker(p) = I$. For $a \in A$, we have that $a \in \ker(p)$ if and only if $\frac{a}{1} \in J$, which is equivalent to saying that $\frac{a}{1} = \frac{s}{t}$, for some $s \in I$ and $t \notin I$. This last equality is equivalent to $at = s$, and this condition is the same to asking that $a \in I$, because I is a prime ideal which is asked to contain s but not t. From this we get $I = \ker(p)$.

6. Let $n \geq 1$ and let A be a real matrix of size $n \times n$ with integral coefficients.

1. Show that
$$\Phi \; : \; \begin{cases} \mathbb{Z}^n \longrightarrow \mathbb{Z}^n \\ x \mapsto Ax \end{cases}$$
is a well-defined, $\mathbb{Z}$-linear map.
2. Show that $\ker \Phi$ and $\mathrm{Im}(\Phi)$ are finitely-generated $\mathbb{Z}$-modules. Are they free $\mathbb{Z}$-modules ?
3. Show that $\det(A) \neq 0$ if and only if $\mathrm{Im}(\Phi)$ has finite index in $\mathbb{Z}^n$. Show with an example that Φ is not necessarily surjective.
4. Assume $\det(A) \neq 0$. Try to guess what is the cardinality of the finite set $\mathbb{Z}^n/\mathrm{Im}(\Phi)$, as a function of A (and try to prove that this guess is correct...)

Solution:

Please turn over!

1. The map Φ is well-defined because for each $x = (x_1, \ldots, x_n) \in \mathbb{Z}^n$ and $A = (a_{ij}) \in M_n(\mathbb{Z})$ the components of Ax are integral, as they are obtained by multiplying and summing integer numbers. Linearity is immediately checked as in classical linear algebra (the fact that $\mathbb{Z}$ is not a field is not a problem).

2. Since $\mathbb{Z}$ is a PID and $\mathbb{Z}^n$ is a free $\mathbb{Z}$-module of rank n, we know that its submodules $\ker \Phi$ and $\mathrm{Im}(\Phi)$ are both free $\mathbb{Z}$-modules of rank $\leq n$, by Proposition 2 from the Note on finitely-generated modules over a principal ideal domain. In particular, both $\ker \Phi$ and $\mathrm{Im}(\Phi)$ are finitely generated and free $\mathbb{Z}$-modules.

3. We have that $\mathrm{Im}(\Phi)$ has finite index in $\mathbb{Z}^n$ if and only if the finitely generated $\mathbb{Z}$-module $\mathbb{Z}^n/\mathrm{Im}(\Phi)$ has rank 0, i.e. $\mathrm{Im}(\Phi)$ has rank n.

   Let $\Phi_{\mathbb{Q}} : \mathbb{Q}^n \longrightarrow \mathbb{Q}^n$ be the $\mathbb{Q}$-linear map sending $x \mapsto Ax$. We have that $\det(A) \neq 0$ if and only if the images via $\Phi_{\mathbb{Q}}$ of the vectors of the canonical basis of $\mathbb{Z}^n \subseteq \mathbb{Q}^n$ are $\mathbb{Q}$-linear independent in $\mathbb{Q}^n$. In particular, if $\det(A) \neq 0$, then the images via Φ of the vectors of the canonical basis of $\mathbb{Z}^n$ are $\mathbb{Z}$-linear independent, so that $\mathrm{Im}(\Phi)$ is a free $\mathbb{Z}$-module of rank n.

   Conversely, suppose that $\mathrm{Im}(\Phi)$ has $\mathbb{Z}$-rank n. A free $\mathbb{Z}$-basis for $\mathrm{Im}(\Phi)$ consists of $\mathbb{Q}$-linear independent vectors in $\mathbb{Q}^n$ (since each $\mathbb{Q}$-linear combination is a positive multiple of a $\mathbb{Z}$-linear combination), and since $\mathrm{Im}(\Phi) \subseteq \mathrm{Im}(\Phi_{\mathbb{Q}})$, the map $\Phi_{\mathbb{Q}}$ needs to be surjective. This implies that $\det(A) \neq 0$.

   The map Φ is not surjective even if $\det(A) \neq 0$. For instance, take $A = \mathrm{diag}(2, 1, \ldots, 1)$. Then $\det(A) = 2 \neq 0$, but $(1, 0, \ldots, 0) \notin \mathrm{Im}(\Phi)$.

4. If $n = 1$ and $A = (\lambda) \in \mathbb{Z}$, then $\mathbb{Z}^n/\mathrm{Im}(\Phi) = \mathbb{Z}/a\mathbb{Z}$ has cardinality equal to $|a|$. For arbitrary n, if $\det(A) = \pm 1$, then A^{-1} is invertible in $M_n(\mathbb{Z})$, and so is the map Φ, so that $\mathbb{Z}^n/\mathrm{Im}(\Phi) = 1$. A good guess for the cardinality of $\mathbb{Z}^n/\mathrm{Im}(\Phi)$ seems then to be $|\det(A)|$.

   The correctness of this guess can be easily checked for upper triangular matrices. If $A = (a_{i,j})$ is upper triangular (i.e., $a_{ij} = 0$ for $i > j$), then the image of Φ is

   $$\mathrm{Im}(\Phi) = \langle (b_1, \ldots, b_n) \rangle \leq \mathbb{Z}^n,$$

   where $b_j := (a_{1j}, a_{2j}, \ldots, a_{nj}) = (a_{1j}, a_{2j}, \ldots, a_{jj}, 0 \ldots, 0)$ for each $1 \leq j \leq n$. In this case, we want to prove the claim that $|\mathbb{Z}^n/\mathrm{Im}(\Phi)| = |\det(A)| = \prod_{j=1}^n |a_{jj}|$. Notice that both the image of Φ and the absolute value of $\det(A)$ do not change if we change the sign to the entries in some columns of A, so that without loss of generality we may assume that $a_{ii} > 0$ (they cannot be zero as $\det(A) \neq 0$). Let $I = \mathrm{Im}(\Phi)$ and take $s = (s_1, \ldots, s_n) \in \mathbb{Z}^n$. By adding a suitable multiple of b_n to s, we get have that $s+I = s'+I$ for some $s' = (s'_1, \ldots, s'_n, u_n)+I$, where $0 \leq u_n \leq a_{nn}$. Repeating this argument (i.e., adding suitable multiples of b_{n-1}, $b_{n-2}, \ldots, b_1$ to s'), we can say that $s + I = (u_1, \ldots, u_n) + I$, for some $1 \leq u_j \leq a_{jj}$. This proves that $|\mathbb{Z}^n/\mathrm{Im}(\Phi)| \leq \det(A)$. Now we have to prove that those representatives $(u_1, \ldots, u_n)$, where $1 \leq u_j \leq a_{jj}$, do not coincide modulo $\mathrm{Im}(\Phi)$. Suppose that $(u_1, \ldots, u_n) + \mathrm{Im}(\Phi) = (u'_1, \ldots, u'_n) + \mathrm{Im}(\Phi)$ for some $0 \leq u_j, u'_j < a_{jj}$. Let $u = (u_1, \ldots, u_n)$ and $u' = (u'_1, \ldots, u'_n)$, and write $u - u' = \sum_{j=1}^n \lambda_j b_j$ with $\lambda_j \in \mathbb{Z}$. Suppose by contradiction that $u_k \neq u'_k$ for some k, and take this k to be maximal. Then for $h > k$ we have $0 = u_h - u'_h = \sum_{j=1}^n \lambda_j a_{hj} = \sum_{j=h}^n \lambda_j a_{hj}$ and this can be

See next page!

used to prove that $\lambda_h = 0$ for $h > k$. Indeed, if $\lambda_l \neq 0$ for some maximal $l > k$, then $\lambda_{l+1}, \ldots, \lambda_n$ would all be zero and $0 = u_l - u_l' = \lambda_l a_{ll}$, contradiction with $\lambda_l \neq 0$. So, assuming by contradiction that $u_k \neq u_k'$ with k maximal, we have that $\lambda_h = 0$ for $h > k$. Then $u_k - u_k' = \sum_{j=k}^{n} \lambda_j a_{kj} = \lambda_k a_{kk}$, so that u_k and u_k' differ by a multiple of a_{kk}. But $0 \leq u_k, u_k' < a_{kk}$ implies that $|u_k - u_k'| < a_{kk}$, so that the only possibility is $u_k = u_k'$, contradiction. This proves that vectors $(u_1, \ldots, u_n) \in \mathbb{Z}^n$, with $0 \leq u_j < a_{jj}$, parametrize distinct classes modulo $\mathrm{Im}(\Phi)$ of $\mathbb{Z}^n$, so that $|\mathbb{Z}^n/\mathrm{Im}(\Phi)| = |\det(A)|$ when A is a upper triangular matrix.

For the general case, one can use the fact that for each matrix $A \in M_n(\mathbb{Z})$ one can write $A = VUW$, for $V, W \in \mathrm{SL}_n(\mathbb{Z})$ and U an upper triangular matrix in $M_n(\mathbb{Z})$. Then $|\det(A)| = |\det(U)|$, and the map $\Phi_V : \mathbb{Z}^n \longrightarrow \mathbb{Z}^n$ associated to V is an automorphism of $\mathbb{Z}^n$ sending $\mathrm{Im}(U) = \mathrm{Im}(UW)$ to $\mathrm{Im}(A)$, so that $[\mathbb{Z}^n : \mathrm{Im}(U)] = [\mathbb{Z}^n : \mathrm{Im}(A)]$.

[Fields]

7. Let K be a field and $L = K(T)$ the field of rational functions with coefficients in K. If $x \in L$ is algebraic over K, show that $x \in K$.

Solution: Write $x = \frac{f}{g}$, where $f, g \in K[T]$ are coprime polynomials and $g \neq 0$. If x is algebraic over K, there exists a monic polinomial $p(X) \in K[X]$ such that $p(x) = 0$. By multiplying this equality by g^n, where $n := \deg(p)$, and writing $p(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$, we get

$$(*) \quad f^n + a_{n-1} f^{n-1} g + \cdots + a_1 f g^{n-1} + a_0 g^n = 0,$$

which implies that $g | f^n$. This implies that $g \in K$, because if g were non-constant, then any irreducible factor of g would divide f, in contradiction with the fact that g is coprime with f. Hence g is invertible, and the equality $(*)$ implies that $f | a_0$, so that f is a constant polynomial as well and $x \in K$.

8. Let $K = \mathbb{F}_p$ where p is a prime number and let L/K be a finite extension. Denote by $\varphi : L \longrightarrow L$ the Frobenius morphism.

1. Show that the trace map $\mathrm{tr}_{L/K} : L \longrightarrow K$, as defined in Exercise 1 of Sheet 12, is non-zero (Hint: estimate the size of the kernel of $\mathrm{tr}_{L/K}$.) Deduce that it is surjective.
2. Show also that the norm map $N_{L/K} : L^\times \longrightarrow K^\times$ is surjective.
3. Show that

$$\ker(\mathrm{tr}_{L/K}) = \{x \in L \mid x = \varphi(y) - y \text{ for some } y \in L\}$$

and that

$$\ker(N_{L/K}) = \{x \in L \mid x = \frac{\varphi(y)}{y} \text{ for some } y \in L^\times\}.$$

Please turn over!

Solution:

1. Let $n = [L : K]$. Then $\ker(\mathrm{tr}_{L/K})$ is the set of roots of the polynomial $f = \sum_{j=0}^{n-1} X^{p^j} \in L[X]$, so that $|\ker(\mathrm{tr}_{L/K})| \le \deg(f) = p^{n-1} < p^n = |L|$ and $\mathrm{tr}_{L/K}$ is non-zero. Since this map is non-zero and K-linear, its image is a non-zero K-linear subspace of K, and the only possibility is that $\mathrm{Im}(\mathrm{tr}_{L/K}) = K$.
2. Let x be a multiplicative generator of $L^\times$. Then x has order $p^n - 1$ in $L^\times$. Now
$$N_{L/K}(x) = \prod_{j=0}^{n-1} x^{p^j} = x^{\sum_{j=0}^{n-1} p^j} = x^{\frac{p^n-1}{p-1}}$$
is an element of $K^\times$ which has order $p-1$ in $L^\times$. Since the norm map is a group homomorphism $L^\times \longrightarrow K^\times$, the subgroup generated by $N_{L/K}(x)$, whose cardinality is $p-1$, is contained in the image of $N_{L/K}$. But $|K^\times| = p-1$, so that $N_{L/K}$ is surjective.
3. Since $\mathrm{tr}_{L/K}$ is surjective, by the First Isomorphism Theorem for groups we have an isomorphism of additive groups $K \cong L/\ker(\mathrm{tr}_{L/K})$. Then $|\ker(\mathrm{tr}_{L/K})| = p^{n-1}$. We want to prove that $\ker(\mathrm{tr}_{L/K}) = \mathrm{Im}(\phi - \mathrm{id}_L)$, where $\phi - \mathrm{id}_L$ is clearly a K-linear map $L \longrightarrow L$. First, we prove the containment "$\supseteq$". Writing $\mathrm{tr}_{L/K}$ as $\mathrm{tr}_{L/K} = \sum_{j=0}^{n-1} \phi^j$, and using the fact that we saw in class that $\phi^n = \mathrm{id}_L$, we get
$$\mathrm{tr}_{L/K} \circ (\phi - \mathrm{id}_L) = \sum_{j=0}^{n-1} \phi^{j+1} - \sum_{j=0}^{n-1} \phi^j = \phi^n - \mathrm{id}_L = 0,$$
so that $\mathrm{Im}(\phi - \mathrm{id}_L) \subseteq \ker(\mathrm{tr}_{L/K})$. In order to get an equality of the two sets, it is enough to show that $|\mathrm{Im}(\phi - \mathrm{id}_L)| = p^{n-1}$. As $\phi - \mathrm{id}_L$ is linear and has kernel equal to $\mathbb{F}_p$, First Isomorphism Theorem for groups gives
$$|\mathrm{Im}(\phi - \mathrm{id}_L)| = |L|/|\ker(\phi - \mathrm{id}_L)| = p^{n-1},$$
and we can conclude that
$$\ker(\mathrm{tr}_{L/K}) = \{x \in L \mid x = \varphi(y) - y \text{ for some } y \in L\}.$$
We use a similar argument to describe the kernel of the norm map. First, notice that $\beta : y \mapsto \frac{\phi(y)}{y} = y^{p-1}$ is a group map $L^\times \longrightarrow L^\times$. We claim that $\ker(N_{L/K}) = \mathrm{Im}(\beta)$. By multiplicativity of the norm, for each $y \in L^\times$ we have
$$N_{L/K}(\beta(y)) = N_{L/K}(y^{p-1}) = N_{L/K}(y)^{p-1} = 1,$$
since $N_{L/K}(y) \in K^\times$. Hence $\ker(N_{L/K}) \supseteq \mathrm{Im}(\beta)$, and to prove equality we just check that the cardinalities coincide. We have $|\ker(N_{L/K})| = \frac{p^n-1}{p-1}$ by the First Isomorphism Theorem for groups, and since $\ker(\beta) = K^\times$, the same theorem gives $|\mathrm{Im}(\beta)| = \frac{p^n-1}{p-1}$ as well. We can then conclude that
$$\ker(N_{L/K}) = \{x \in L \mid x = \frac{\varphi(y)}{y} \text{ for some } y \in L^\times\}.$$

See next page!

9. Let K be a finite field, $\bar{K}$ an algebraic closure of K. Let $x \in \bar{K}$ be any element, and $P = \mathrm{Irr}(x, K)$ the minimal irreducible polynomial of x in $K[X]$. Let $(x_1, \ldots, x_d)$ be the distinct roots of P in $\bar{K}$. Prove that

$$\prod_{\substack{1 \leq i,j \leq d \\ i \neq j}} (x_i - x_j)^2 \in K.$$

Solution:

Let $\gamma = \prod_{\substack{1 \leq i,j \leq d \\ i \neq j}} (x_i - x_j)^2$. To prove that γ lies in K, it is enough to check that $\phi(\gamma) = \gamma$, where $\phi : x \mapsto x^p$ is the Frobenius endomorphism of $\bar{K}$. Suppose that $y \in \bar{K}$ is a root of P. Then $\phi(y) = y^p$ is also a root, since $P(\phi(y)) = \phi(P(y)) = 0$. Hence ϕ restricts to a map $\phi' : \{x_1, \ldots, x_d\} \longrightarrow \{x_1, \ldots, x_d\}$. Since ϕ is injective, ϕ' is injective as well, so that it is a bijection of the set $\{x_1, \ldots, x_d\}$. Then

$$\phi(\gamma) = \phi\left(\prod_{\substack{1 \leq i,j \leq d \\ i \neq j}} (x_i - x_j)^2\right) = \prod_{\substack{1 \leq i,j \leq d \\ i \neq j}} (\phi(x_i) - \phi(x_j))^2 = \prod_{\substack{1 \leq i,j \leq d \\ i \neq j}} (x_i - x_j)^2 = \gamma,$$

where in the third equality we have used the fact that ϕ permutes the x_i's, and that γ is stable under permuting the x_i's, since the indexes in the product range on all values $1 \leq i, j \leq d$.