1) Show that we get an automorphism of the group $GL(2, \mathbb{R})$ by sending
\[
\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}
\to
\begin{pmatrix} a_{22} & -a_{21} \\ -a_{12} & a_{11} \end{pmatrix}.
\]

2) Let $G$ be a group and $H, K$ be two subgroups of $G$.

a) Prove that $H \cap K$ is a subgroup of $G$.

b) Show that $Ha \cap Kb$ is a right coset of $H \cap K$ for all $a, b \in G$ with $Ha \cap Kb \neq \emptyset$.


3) Let $F(\sigma)$ the number of 1-cycles in the cyclic decomposition of $\sigma \in S_n$.

a) Prove that $\frac{1}{n!} \sum_{\sigma \in S_n} F(\sigma) = 1$.

b) Show that $\frac{1}{n!} \sum_{\sigma \in S_n} F(\sigma)^2 = 2$.

(Hint for b): Let $S_n$ act on $\{1,2,..,n\} \times \{1,2,..,n\}$.

4) Prove that $X^4 - X - 1$ is not a product of two non-constant polynomials in $\mathbb{Z}[X]$. (Hint: Consider binary polynomials.)

5) Let $K$ be the field defined by the quotient ring $\mathbb{Q}[X]/(X^4 - X - 1)$ and $\alpha \in K$ be the coset $X + (X^4 - X - 1)$. Express $\alpha^{10}$ and $1/\alpha$ as linear combinations of $1, \alpha, \alpha^2$ and $\alpha^3$ over $\mathbb{Q}$.

6a) Show that every ideal of $R = \mathbb{C}[X]/(X^n)$ is principal.

b) Let $\alpha$ be the coset $X + (X^n) \in R$. Prove that there are exactly $n$ proper ideals of $R$ and that they are given by $(\alpha^k)$ for $k \in \{1,2,..,n\}$.

You may use the theorems in Durbin’s book, but all claims should be motivated.
Brief solutions to the exam in MMG500/MVE150 2020-08-19.

1) We first note that \( \det \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \det \begin{pmatrix} a_{22} & -a_{21} \\ -a_{12} & a_{11} \end{pmatrix} \). We have thus a map \( \varphi: \text{GL}(2,\mathbb{R}) \rightarrow \text{GL}(2,\mathbb{R}) \) which sends \( \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \) to \( \begin{pmatrix} a_{22} & -a_{21} \\ -a_{12} & a_{11} \end{pmatrix} \). This map is bijective as \( \varphi(\varphi(A)) = A \) for all \( A \in \text{GL}(2,\mathbb{R}) \). We have further that

\[
\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix},
\]

\[
\begin{pmatrix} a_{22} & -a_{21} \\ -a_{12} & a_{11} \end{pmatrix} \begin{pmatrix} b_{21} & b_{22} \\ -b_{11} & b_{12} \end{pmatrix} = \begin{pmatrix} a_{21}b_{12} + a_{22}b_{22} & -a_{21}b_{11} - a_{22}b_{21} \\ -a_{11}b_{12} - a_{12}b_{22} & a_{11}b_{11} + a_{12}b_{21} \end{pmatrix}.
\]

We have thus for all \( A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \) and \( B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \) in \( \text{GL}(2,\mathbb{R}) \) that

\[ \varphi(AB) = \varphi \left( \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix} \right) = \begin{pmatrix} a_{21}b_{12} + a_{22}b_{22} & -a_{21}b_{11} - a_{22}b_{21} \\ -a_{11}b_{12} - a_{12}b_{22} & a_{11}b_{11} + a_{12}b_{21} \end{pmatrix} = \varphi(A)\varphi(B). \]

We have thus shown that \( \varphi \) is a bijective homomorphism to itself.

2a) \( e \in H \cap K \), \( a, b \in H \cap K \Rightarrow ab \in H \cap K \) and \( a \in H \cap K \Rightarrow a^{-1} \in H \cap K \). Hence \( H \cap K \) is a subgroup by the subgroup criterion.

b) If \( c \in Ha \cap Kb \), then \( Ha = Hc \) and \( Kb = Kc \). We have also trivially that \( (H \cap K)c \subseteq Hc \cap Kc \). Conversely, if \( hc = kc \in Hc \cap Kc \), then \( h = k \) be the cancellation law and hence \( hc = kc \) an element in \( (H \cap K)c \). We have therefore if \( Ha \cap Kb \neq \emptyset \) that \( Ha \cap Kb = (H \cap K)c \) for any \( c \in Ha \cap Kb \).

c) Suppose that \( [G:H] = m \) and \( [G:K] = n \). Then \( G \) is a disjoint union \( G = Ha_1 \cup \ldots \cup Ha_m = Kb_1 \cup \ldots \cup Kb_n \) by right cosets of \( H \) and \( K \). Hence \( G \) is a union of at most \( mn \) non-empty intersections \( Ha \cap Kb \) and thus by b) a union of at most \( mn \) right cosets \( (H \cap K)c \). Therefore, \( [G: H \cap K] \leq mn \).

3a) We apply Burnside’s counting lemma to the action of \( G = S_n \) on the set \( \{1, 2, \ldots, n\} \). This gives that the number of orbits is equal to \( \frac{1}{n!} \sum_{\sigma \in S_n} F(\sigma) \).

But the action is clearly transitive so that the number of orbits is 1. Hence \( \frac{1}{n!} \sum_{\sigma \in S_n} F(\sigma) = 1 \), as asserted.
3b) We consider the natural action of $G=S_n$ on $T=\{1,2,\ldots,n\} \times \{1,2,\ldots,n\}$, where the action of $\sigma \in G=S_n$ sends $(i,j)$ to $(\sigma(i), \sigma(j))$. There are then $F(\sigma)^2$ fixed points in $T$ under the action of $\sigma$ on $T$. We see therefore by Burnside’s lemma that there are $\frac{1}{n!} \sum_{\sigma \in S_n} F(\sigma)^2$ orbits under the action of $S_n$ on $\{1,2,\ldots,n\} \times \{1,2,\ldots,n\}$. But it is clear that there are exactly 2 orbits under this action. The first orbit consists of all pairs $(i,i)$ and the second of all pairs $(i,j)$ where $i \neq j$. Hence
$$\frac{1}{n!} \sum_{\sigma \in S_n} F(\sigma)^2 = 2,$$ as was to be shown.

4) Suppose that $X^4 - X - 1 = f(X)g(X)$ for two polynomials $f$ and $g$ in $\mathbb{Z}[X]$. We have then that the leading coefficient of $f$ and $g$ are $\pm 1$ and a factorization $X^4 - X - 1 = G(HX)$ in $\mathbb{Z}_2[X]$ for the images $F$ and $G$ of $f$ and $g$ under the evident homomorphism from $\mathbb{Z}[X]$ to $\mathbb{Z}_2[X]$. But $F(X) = X^4 - X - 1 \in \mathbb{Z}_2[X]$ has no linear factors as $F(0) = F(1) = 1$ in $\mathbb{Z}_2$. So if $X^4 - X - 1$ were reducible, then then we must have that $G(X) = H(X)$ are irreducible of degree two in $\mathbb{Z}_2[X]$. But the only irreducible polynomial of degree two in $\mathbb{Z}_2[X]$ is $X^2 + X + 1$, which means that $G(X)H(X) = (X^2 + X + 1)^2 = X^4 + X^2 + 1 \neq X^4 - X - 1$ in $\mathbb{Z}_2[X]$. Hence $X^4 - X - 1$ is irreducible in $\mathbb{Z}_2[X]$, and therefore also in $\mathbb{Z}[X]$.

5) $\alpha^{10} = \alpha^2(\alpha^4)^2 = \alpha^2(\alpha+1)^2 = \alpha^4 + 2\alpha^3 + \alpha^2 = 2\alpha^3 + \alpha^2 + \alpha + 1$ as $\alpha^4 - \alpha - 1 = 0$ in $K$.
From $\alpha^3 = \alpha + 1$, we see also that $\alpha(\alpha^3 - 1) = 1$ and hence that $\alpha^3 - 1 = \alpha - 1$ in $K$.

6a) Let $J$ be an ideal in $R = \mathbb{C}[X]/(X^n)$ and $I$ its inverse image in $\mathbb{C}[X]$. Then $I$ is the kernel of the composite ring homomorphism $\mathbb{C}[X] \to R \to R/J$. It is thus an ideal of $\mathbb{C}[X]$ by theorem 38.1 in Durbin’s book and a principal ideal $(p(X))$ of $\mathbb{C}[X]$ by theorem 40.3 in (op.cit.). $J$ is therefore a principal ideal of $R$ generated by $p(X)+ (X^n)$.

6b) Let $J$ be the principal ideal $(p(X)+ (X^n)) \subseteq R$. Then $J = \{0\} = (\alpha^n)$ if $p(X) \in \mathbb{C}[X]$ is divisible by $X^n$. If $p(X)$ is not divisible by $X^n$, then $f(X) : = \text{GCD}(p(X), X^n) = 1$ or $X^k$ for $k \in \{1, 2, \ldots, n-1\}$. It is therefore enough to show that $J = (f(X)+ (X^n))$. But $J \subseteq (f(X)+ (X^n))$ as $f(x)$ divides $p(X)$ in $\mathbb{C}[X]$. We have also by theorem 36.2 that $f(X) = a(X)p(X) + b(X)X^n$ for some $a(X), b(X) \in \mathbb{C}[X]$ and hence that $f(X)+ (X^n) = (a(X)+ (X^n))(p(X)+ (X^n))$. Therefore, $(f(X)+ (X^n)) \subseteq J$, and we are done.