Department of Mathematics
STOCKHOLM UNIVERSITY
Lecturer: A. Aumonier
Examiner: A. Sola

Written examination
Mathematics III Abstract Algebra
06 August 2026

No textbooks or notes allowed. Please explain your reasoning and write out detailed arguments. At least 12 points are needed for a passing grade.

1. **(4 points in total)**

   (a) Let G be a group and $H \leq G$ be a subgroup. Give a definition of the normalizer of H in G. (1p)

   (b) Show that $N_G(H)$ is a subgroup of G. Show that H is a normal subgroup of $N_G(H)$. (1p)

   (c) Show that $N_G(H)$ is the largest subgroup of G in which H is normal, in the sense that if $H \leq K$ is normal in K, then K is a subgroup of $N_G(H)$. (1p)

   (d) Show that for any subgroup $K \leq N_G(H)$, the set $KH = \{kh \mid k \in K,\, h \in H\}$ is a group in which H is normal. (1p)

   Solution:

   (a) $N_G(H) = \{g \in G \mid gH = Hg\}$. See Dummit & Foote page 50.

   (b) First, $N_G(H) \neq \emptyset$ because $1 \in N_G(H)$. Second, if $g \in N_G(H)$ then $gH = Hg$ and multiplying by g^{-1} on the left and on the right on both sides of this equality gives $Hg^{-1} = g^{-1}H$, so that $g^{-1} \in N_G(H)$. Hence $N_G(H)$ is closed under taking inverses. Finally, if $g, k \in N_G(H)$ then $gH = Hg$ and $kH = Hk$. Therefore $(gk)H = g(kH) = g(Hk) = (gH)k = (Hg)k = H(gk)$, so $gk \in N_G(H)$. Hence $N_G(H)$ is closed under products. We have thus shown that $N_G(H)$ is a subgroup of G.

   Because H is closed under products (it is a subgroup of G), we have that $hH = Hh$ for any $h \in H$. Hence $H \subset N_G(H)$, i.e. H is a subgroup of $N_G(H)$. By definition of the normalizer $gH = Hg$ for any $g \in N_G(H)$, hence H is normal in $N_G(H)$.

   (c) Let K be a subgroup of G in which H is normal. Let $k \in K$. Then, because H is normal in K, we have that $kH = Hk$. Hence $k \in N_G(H)$. We thus have shown that $K \subset N_G(H)$.

   (d) Let $K \leq N_G(H)$ be a subgroup. We will first verify that KH is a group. As $1 \in K$ and $1 \in H$, we have that $1 \in KH$. Let $k \in K$ and $h \in H$, then we observe that

   $$(kh)^{-1} = h^{-1}k^{-1} = (k^{-1}k)h^{-1}k^{-1} = k^{-1}(kh^{-1}k^{-1}).$$

   Now, $k^{-1} \in K$ because K is a subgroup, and $kh^{-1}k^{-1} \in H$ because $K \leq N_G(H)$. Hence $(kh)^{-1} \in KH$, so KH is closed under taking inverses. Finally, let $k_1, k_2 \in K$ and $h_1, h_2 \in H$. Then we compute that

   $$(k_1h_1)(k_2h_2) = k_1(k_2k_2^{-1})h_1k_2h_2 = (k_1k_2)((k_2^{-1}h_1k_2)h_2)$$

   and observe that $(k_2^{-1}h_1k_2) \in H$ because $K \leq N_G(H)$. As before, we conclude that $(k_1h_1)(k_2h_2) \in KH$, hence that KH is closed under product. We have thus shown that KH is a group.

   As $1 \in K$, we have $h = 1 \cdot h \in KH$ for any $h \in H$, hence H is a subgroup of KH. It is also normal. Indeed, let $kh \in KH$. Then $(kh)H = k(hH) = k(Hh) = (kH)h = (Hk)h = H(kh)$ where we have used that $hH = Hh$ (see question (b)) and $kH = Hk$ (true by assumption on K).

2. **(3 points in total)**

   Let G be a finite group of even order $|G| = 2n$, with $n \in \mathbb{N}$.

   (a) Let $H < G$ be a subgroup of order n. Show that H is normal in G. (2p)

(b) Suppose that there exist two subgroups $H_1, H_2 < G$ of order n such that $H_1 \cap H_2 = \{1\}$, where $1 \in G$ denotes the identity element of G. Show that there exists $a \in G$ with $a \notin H_1$ and $a \notin H_2$ such that $G = H_1 \cup H_2 \cup \{a\}$. (1p)

Solution:

(a) Since $|G| = 2n$ and $|H| = n$, H has index 2 in G. Thus there are exactly two left cosets and two right cosets of H. If $g \notin H$, the coset decompositions are

$$G = H \sqcup gH = H \sqcup Hg,$$

so $gH = Hg$. For $g \in H$ this equality is immediate. Hence $gH = Hg$ for every $g \in G$, and therefore H is normal in G.

(b) Since $|H_1| = |H_2| = n$ and $H_1 \cap H_2 = \{1\}$,

$$|H_1 \cup H_2| = |H_1| + |H_2| - |H_1 \cap H_2| = 2n - 1 = |G| - 1.$$

Thus there is a unique element $a \in G \setminus (H_1 \cup H_2)$. In particular, $a \notin H_1$ and $a \notin H_2$, and $G = H_1 \cup H_2 \cup \{a\}$.

3. **(5 points in total)**

   The goal of this problem is to show that any group of order 12 contains a characteristic subgroup. (Recall that a subgroup $H < G$ is a characteristic subgroup if for any automorphism ϕ of G, $\phi(H) = H$.)

   (a) Give an example of a group of order 12. (1p)

   (b) Give the definition of a Sylow p-subgroup of a finite group. (1p)

   (c) Show that a normal Sylow p-subgroup is a characteristic subgroup. (1p)

   (d) Let G be a group of order 12.

   (i) Suppose that G has a unique Sylow 3-subgroup $P < G$. Show that P is a characteristic subgroup. (1p)

   (ii) Suppose that G has at least two Sylow 3-subgroups. Show then that there are at least 8 elements of order 3 in G. Deduce that G has a unique Sylow 2-subgroup $H < G$, and that H is characteristic. (1p)

Solution:

(a) The cyclic group $\mathbb{Z}/12\mathbb{Z}$ has order 12.

(b) If $|G| = p^n m$ with $p \nmid m$, a Sylow p-subgroup of G is a subgroup of order p^n.

(c) Let P be a normal Sylow p-subgroup. By Sylow's conjugacy theorem, P is the unique Sylow p-subgroup of G. Any automorphism of G sends Sylow p-subgroups to Sylow p-subgroups, hence fixes P. Thus P is characteristic.

(d.i) If P is the unique Sylow 3-subgroup, every automorphism of G must send P to itself. Hence P is characteristic.

(d.ii) Let n_3 denote the number of Sylow 3-subgroups. By Sylow's theorems,

$$n_3 \mid 4, \qquad n_3 \equiv 1 \pmod 3.$$

Since $n_3 > 1$, we have $n_3 = 4$. Distinct subgroups of order 3 intersect only in the identity, so they contain altogether $4(3-1) = 8$ elements of order 3.

Let H be a Sylow 2-subgroup of G, so $|H| = 4$. By Lagrange's theorem, no element of H has order 3, hence H consists of the identity together with three elements of G not among these eight elements of order 3. Because $|G| = 12 = 1 + 8 + 3$, we see that H is the unique Sylow 2-subgroup. Therefore H is characteristic.

4. **(4 points in total)**

Let R be an integral domain which is finite. The goal of this problem is to show that R is a field.

(a) Let $r \in R \setminus \{0\}$. Show that the function

$$\phi(x) = rx$$

defines an automorphism of the additive group $(R, +)$. (2p)

(b) Deduce that R is a field. What are the possible orders of R? (2p)

Solution:

(a) Let $r \in R\setminus\{0\}$ and define $\phi\colon R \to R$ by $\phi(x) = rx$. One verifies directly that ϕ is a homomorphism of additive groups. If $\phi(x) = \phi(y)$, then $r(x - y) = 0$. Since R is an integral domain and $r \neq 0$, this implies that $x = y$. Thus ϕ is injective. As R is finite, ϕ is therefore bijective, hence an automorphism of $(R, +)$.

(b) Since ϕ is surjective, there exists $x \in R$ such that $rx = 1$. Thus every nonzero element of R is invertible, so R is a field.

It remains to determine the possible orders of R. Since R is a field, its characteristic is either 0 or a prime number. As R is finite, its characteristic cannot be 0, so $\operatorname{char}(R) = p$ for some prime p. Hence R contains a copy of the finite field $\mathbb{F}_p$, and R is a vector space over $\mathbb{F}_p$. Since R is finite, this vector space has finite dimension, say n. Therefore $|R| = |\mathbb{F}_p|^n = p^n$. Thus the order of a finite integral domain is necessarily a prime power.

5. **(4 points in total)**

Let R be a unique factorisation domain (UFD) with field of fractions $K = \operatorname{Frac}(R)$. Let

$$f = a_d X^d + a_{d-1}X^{d-1} + \cdots + a_0 \in R[X]$$

with $a_0 \neq 0$ and $a_d \neq 0$.

(a) Show that if $r = \frac{\alpha}{\beta} \in K$ is a root of f, with $\alpha, \beta \in R$ coprime, then $\alpha \mid a_0$ and $\beta \mid a_d$. (2p)

(b) Is the polynomial $X^3 - 4X^2 - \frac{9}{2}X - \frac{5}{2}$ irreducible over $\mathbb{Q}$? (2p)

Solution:

(a) Let $r = \frac{\alpha}{\beta} \in K$ be a root of f, where $\alpha, \beta \in R$ are coprime. Then

$$f(r) = a_d\left(\frac{\alpha}{\beta}\right)^d + a_{d-1}\left(\frac{\alpha}{\beta}\right)^{d-1} + \cdots + a_0 = 0.$$

Multiplying by β^d gives

$$a_d\alpha^d + a_{d-1}\alpha^{d-1}\beta + \cdots + a_0\beta^d = 0.$$

Hence

$$a_d\alpha^d = -\beta\big(a_{d-1}\alpha^{d-1} + \cdots + a_0\beta^{d-1}\big),$$

so $\beta \mid a_d\alpha^d$. Since α and β are coprime and R is a UFD, we must have $\beta \mid a_d$. Similarly,

$$a_0\beta^d = -\alpha\big(a_d\alpha^{d-1} + a_{d-1}\alpha^{d-2}\beta + \cdots + a_1\beta^{d-1}\big),$$

so $\alpha \mid a_0\beta^d$, hence $\alpha \mid a_0$ since α and β are coprime and R is a UFD.

(b) We will show that the polynomial $P(X) = X^3 - 4X^2 - \frac{9}{2}X - \frac{5}{2}$ is not irreducible over $\mathbb{Q}$. Because it has degree 3 and $\mathbb{Q}$ is a field, P is reducible if and only if it has a root in $\mathbb{Q}$. [Now, either you can find a root directly or you can use the criterion of question (a) to help you find one. We will do the latter.] Notice that $P \in \mathbb{Q}[X]$ has a root in $\mathbb{Q}$ if and only if $2P \in \mathbb{Z}[X]$ has a root in $\mathbb{Q} = \operatorname{Frac}(\mathbb{Z})$. Suppose that $r = \alpha/\beta \in \mathbb{Q}$ is a root of $2P$, with $\alpha, \beta \in \mathbb{Z}$ coprime. Then, by question (a), $\alpha \mid 5$ and $\beta \mid 2$, so $\alpha \in \{1, 5\}$ and $\beta \in \{1, 2\}$. This leaves eight possibilities, namely $r \in \{\pm 1, \pm\frac{1}{2}, \pm 5, \pm\frac{2}{5}\}$. By trying them, we see that $P(5) = 0$ so that 5 is a root of P. Hence P is reducible over $\mathbb{Q}$.

6. **(4 points in total)**

Let R be a commutative ring with identity $1 \neq 0$, and let $I, J \subset R$ be ideals. Denote by

$$\pi_I\colon R \longrightarrow R/I \qquad \text{and} \qquad \pi_J\colon R \longrightarrow R/J$$

the two projections onto the associated quotient rings.

(a) Show that $\pi_I(J) = \frac{I+J}{I} \subset R/I$, and that $\pi_J(I) = \frac{I+J}{J} \subset R/J$. (1p)

(b) Deduce that $(R/I)/\pi_I(J)$ and $(R/J)/\pi_J(I)$ are isomorphic. (1p)

We now want to apply this result to give a criterion for when a prime ideal $(p) \subset \mathbb{Z}$ remains prime upon a ring extension. Let $f \in \mathbb{Z}[X]$ be an irreducible monic polynomial and $p \in \mathbb{Z}$ be a prime number.

(c) Show that $(\mathbb{Z}[X]/(f))/(p) \cong \mathbb{F}_p[X]/(\bar{f})$. (Recall that $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ and we write $\bar{f}$ for the reduction of f modulo p.) (1p)

(d) Conclude that $(p) \subset \mathbb{Z}[X]/(f)$ is a prime ideal if and only if $\bar{f}$ is irreducible in $\mathbb{F}_p[X]$. (1p)

Solution:

(a) By definition,

$$\pi_I(J) = \{j + I \mid j \in J\}.$$

On the other hand,

$$\frac{I+J}{I} = \{i + j + I \mid i \in I,\ j \in J\} = \{j + I \mid j \in J\}.$$

Hence

$$\pi_I(J) = \frac{I+J}{I}.$$

Similarly,

$$\pi_J(I) = \frac{I+J}{J}.$$

(b) By the third isomorphism theorem,

$$\frac{R/I}{(I+J)/I} \cong \frac{R}{I+J} \qquad \text{and} \qquad \frac{R/J}{(I+J)/J} \cong \frac{R}{I+J}.$$

Using part (a), it follows that

$$(R/I)/\pi_I(J) \cong (R/J)/\pi_J(I).$$

(c) We apply part (b) with

$$R = \mathbb{Z}[X], \qquad I = (f), \qquad J = (p).$$

Then

$$\frac{\mathbb{Z}[X]/(f)}{(p)} \cong \frac{\mathbb{Z}[X]/(p)}{(\bar{f})}.$$

Since $\mathbb{Z}[X]/(p) \cong \mathbb{F}_p[X]$, we obtain

$$\frac{\mathbb{Z}[X]/(f)}{(p)} \cong \frac{\mathbb{F}_p[X]}{(\bar{f})}.$$

(d) The ideal $(p) \subset \mathbb{Z}[X]/(f)$ is prime if and only if the quotient

$$\frac{\mathbb{Z}[X]/(f)}{(p)}$$

is an integral domain. By part (c), this is equivalent to $\mathbb{F}_p[X]/(\bar{f})$ being an integral domain. Since $\mathbb{F}_p[X]$ is a PID, this happens if and only if $(\bar{f})$ is a prime ideal, equivalently if and only if $\bar{f}$ is irreducible in $\mathbb{F}_p[X]$.