Department of Mathematics
STOCKHOLM UNIVERSITY
Examiner: A. Sola

Written examination
Matematics III Abstract Algebra
7 October 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)** Let G be a group.

   (a) Give the definition of a normal subgroup of G. (1p)

   (b) Let A and B be subgroups of G. Prove that the product AB is a subgroup if at least one of A and B is normal. Prove that AB is normal if both A and B are normal. (3p)

   Solution:

   (a) See Dummit–Foote, §3.1, for the definition of a normal subgroup.

   (b) Suppose first that $A \trianglelefteq G$. If $a \in A$ and $b \in B$, then

   $$ab = b(b^{-1}ab) \in BA,$$

   so $AB \subseteq BA$. Similarly $BA \subseteq AB$, hence $AB = BA$. Therefore

   $$(AB)(AB) = A(BA)B = A(AB)B = AB$$

   and

   $$(AB)^{-1} = B^{-1}A^{-1} = BA = AB.$$

   Thus AB is a subgroup. The case $B \trianglelefteq G$ is symmetric.

   If both A and B are normal, then for every $g \in G$,

   $$g(AB)g^{-1} = (gAg^{-1})(gBg^{-1}) = AB.$$

   Hence $AB \trianglelefteq G$.

2. **(4 points in total)** Let G be a group and let $A \neq \emptyset$ be a subset of G.

   (a) Define the *centralizer* $C_G(A)$ of A in G and prove that $C_G(A)$ is a subgroup of G. (1p)

   (b) Let the dihedral group D_8 act on itself by conjugation. Which conjugacy classes form the center $Z(D_8)$? Compute $|C_{D_8}(g)|$ for $g \notin Z(D_8)$. (2p)

   (c) Determine the conjugacy classes of D_8. (1p)

   Solution:

   (a) See Dummit–Foote, §2.2, for the definition:

   $$C_G(A) = \{g \in G : ga = ag \text{ for every } a \in A\}.$$

   Clearly $1 \in C_G(A)$. If $x, y \in C_G(A)$ and $a \in A$, then

   $$(xy^{-1})a = xay^{-1} = axy^{-1},$$

   so $xy^{-1} \in C_G(A)$. Hence $C_G(A) \leq G$.

   (b) Write

   $$D_8 = \langle r, s \mid r^4 = s^2 = 1,\ srs = r^{-1} \rangle.$$

Then

$$Z(D_8) = \{1, r^2\},$$

so the conjugacy classes contained in the center are $\{1\}$ *and* $\{r^2\}$*. For* $g = r$ *or* r^3*,*

$$C_{D_8}(g) = \langle r \rangle,$$

which gives us the conjugacy class $\{r, r^3\}$*. whereas for a reflection* g*,*

$$C_{D_8}(g) = \{1, r^2, g, r^2 g\}.$$

Thus

$$|C_{D_8}(g)| = 4 \qquad \text{for every } g \notin Z(D_8).$$

(c) The conjugacy classes are

$$\{1\}, \qquad \{r^2\}, \qquad \{r, r^3\}, \qquad \{s, r^2 s\}, \qquad \{rs, r^3 s\}.$$

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

We suppose that there exists a simple group G of order 180.

(a) Show that G contains 36 Sylow 5-subgroups. (2p)

(b) Show that G contains 10 Sylow 3-subgroups. Show furthermore that for any distinct Sylow 3-subgroups $H \neq K$, we have $H \cap K = \{1\}$. (Hint: Let $g \in H \cap K$ and consider the possible orders of the centralizer of g in G. Observe as well that a group of order 18 has a unique Sylow 3-subgroup.) (2p)

(c) Conclude that a simple group of order 180 cannot exist. (1p)

Solution:

(a) By the Sylow theorems,

$$n_5 \equiv 1 \pmod 5, \qquad n_5 \mid 36,$$

so $n_5 \in \{1, 6, 36\}$*. Since* G *is simple,* $n_5 \neq 1$*.*

Suppose $n_5 = 6$*. Conjugation on the six Sylow* 5*-subgroups gives a nontrivial homomorphism*

$$G \longrightarrow S_6.$$

Its kernel is normal in G*, hence it is trivial, so the homomorphism is injective. The composition with the sign homomorphism* $S_6 \to \mathbb{Z}/2\mathbb{Z}$ *is trivial, again by simplicity, so* G *embeds in* A_6*. Its image has order* 180*, hence index* 2 *in* A_6*, and is therefore normal in* A_6*. This contradicts the simplicity of* A_6 *(Dummit–Foote, §4.6). Hence*

$$n_5 = 36.$$

(b) Again by the Sylow theorems,

$$n_3 \equiv 1 \pmod 3, \qquad n_3 \mid 20,$$

so $n_3 \in \{1, 4, 10\}$*. Simplicity excludes* $n_3 = 1$*. If* $n_3 = 4$*, conjugation on the four Sylow* 3*-subgroups gives a nontrivial homomorphism*

$$G \longrightarrow S_4.$$

Its kernel is normal, hence trivial, which is impossible since $|G| = 180 > |S_4| = 24$*. Thus*

$$n_3 = 10.$$

Now let $H \neq K$ *be Sylow* 3*-subgroups and suppose that*

$$1 \neq g \in H \cap K.$$

Since $|H| = |K| = 9 = 3^2$, both H and K are abelian (see Corollary 9 page 125 in Dummit–Foote). Hence

$$H, K \leq C_G(g).$$

Therefore $|C_G(g)| \in \{18, 36, 45, 90\}$. The multiplication action of G on $G/C_G(g)$ induces a homomorphism

$$G \longrightarrow S_{[G:C_G(g)]}.$$

By simplicity of G, its kernel is trivial. If $|C_G(g)| \in \{36, 45, 90\}$, this would embed G in either S_5, S_4, or S_2, all of which have order less than 180. Thus

$$|C_G(g)| = 18.$$

But H and K are then Sylow 3-subgroups of $C_G(g)$. A group of order 18 has a unique Sylow 3-subgroup (seen directly from the Sylow theorems). Hence $H = K$, which is a contradiction. Therefore

$$H \cap K = \{1\}.$$

(c) The 36 Sylow 5-subgroups contribute

$$36(5 - 1) = 144$$

distinct non-identity elements. By (b), the 10 Sylow 3-subgroups contribute

$$10(9 - 1) = 80$$

distinct non-identity elements. These two sets are disjoint. Hence G would contain at least

$$1 + 144 + 80 = 225 > 180$$

elements, a contradiction.

4. **(4 points in total)** Let R be a ring with unit.

   (a) Give the definition of a left ideal of R and of a right ideal of R. (1p)

   (b) Give an example of a ring R and a left ideal of R which is not a right ideal. (2p)

   (c) Can it happen that a left ideal is also a right ideal if R is non-commutative? (1p)

   Solution:

   (a) See Dummit–Foote, §7.3, definitions of left, right, and two-sided ideals.

   (b) For one example, let

$$R = M_2(\mathbb{Q}), \qquad I = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} : a, b \in \mathbb{Q} \right\}.$$

   Then I is closed under addition and under multiplication on the left by arbitrary matrices in R, so it is a left ideal. However

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in I,$$

   while

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \notin I.$$

   Hence I is not a right ideal.

   (c) Yes. For example, let R be the noncommutative ring of upper triangular 2×2 matrices over $\mathbb{Q}$. Then

$$I = \left\{ \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} : a \in \mathbb{Q} \right\}$$

   is both a left and a right ideal.

5. **(4 points in total)** Let R be a commutative ring with unit.

   (a) Give the definitions of (i) a unit in R, and (ii) a maximal ideal in R. (1p)

   (b) Show that $a \in R$ is a unit if and only if, for each maximal ideal M of R, we have $a \notin M$. (1p)

   (c) Show that R has exactly one maximal ideal if and only if the set of non-units is an ideal. (2p)

   Solution:

   (a) For units see Dummit–Foote, §7.1; for maximal ideals see Dummit–Foote, §7.4.

   (b) If a is a unit and $a \in M$, then

   $$1 = a^{-1}a \in M,$$

   contradicting $M \neq R$.

   Conversely, if a is not a unit, then (a) is a proper ideal. Every proper ideal is contained in a maximal ideal (Dummit–Foote, §7.4), so $a \in M$ for some maximal ideal M.

   (c) Let N denote the set of non-units. If R has a unique maximal ideal M, part (b) gives

   $$N = M,$$

   so N is an ideal.

   Conversely, suppose N, defined as above, is an ideal. Since $1 \notin N$, it is proper. Any ideal properly containing N contains some unit, and hence is all of R. Thus N is maximal. Moreover every proper ideal contains no units, so every maximal ideal M satisfies $M \subseteq N$. By maximality,

   $$M = N.$$

   Hence R has exactly one maximal ideal.

6. **(3 points in total)**

   (a) State precisely Eisenstein's irreducibility criterion for polynomials in $\mathbb{Z}[X]$. (1p)

   (b) Is $X^5 - 10X^4 + 40X^3 - 80X^2 + 49X - 1$ irreducible in $\mathbb{Z}[X]$? (2p)

   Solution:

   (a) See Dummit–Foote, §9.4, Corollary 14 (Eisenstein's criterion for $\mathbb{Z}[X]$).

   (b) Let

   $$f(X) = X^5 - 10X^4 + 40X^3 - 80X^2 + 49X - 1.$$

   Making the substitution $X \mapsto X + 2$ gives

   $$f(X + 2) = X^5 - 31X - 31.$$

   This is Eisenstein at the prime 31: every nonleading coefficient is divisible by 31, while the constant coefficient -31 is not divisible by 31^2. Hence $f(X + 2)$ is irreducible in $\mathbb{Z}[X]$.

   Since $X \mapsto X + 2$ is an automorphism of $\mathbb{Z}[X]$, irreducibility is preserved. Therefore $f(X)$ is irreducible in $\mathbb{Z}[X]$.