Department of Mathematics
STOCKHOLM UNIVERSITY
Examiner: A. Sola

Written examination
Matematics III Abstract Algebra
17 March 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) Show (providing a complete argument) that if G is a group and the subgroup H has index 2 then H is normal in G. (2p)

   (b) Must a subgroup of index 3 be normal? Is it possible for a subgroup of order 3 to be normal? Give proofs or counterexamples. (2p)

   Solution:

   (a) Let $g \in G$ satisfy $g \notin H$ (so in particular $g \neq 1$). There are two left cosets of H in G, necessarily H and gH. Since cosets partition G we obtain that $gH = G \setminus H$. Repeating the argument for right cosets, we obtain that $gH = Hg$, and every left coset is a right coset meaning that H is normal in G.

   (b) A subgroup of index 3 need not be normal. Consider the subgroup $\langle(12)\rangle = \{e, (1,2)\}$ in the symmetric group S_3. Since $|S_3| = 6$, the index of this subgroup is equal to 3. This subgroup is not normal since $(13)\langle(12)\rangle = \{(13), (123)\} \neq \{(13), (132)\} = \langle(12)\rangle$ A subgroup of order 3 can indeed be normal, as may be seen by considering $\{e, (123), (132)\}$ as a subgroup of S_3.

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 and Foote, p. 49.

   (b) We have (with the usual notation for dihedral groups) $D_8 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$. As was shown in class (or as can be verified from first principles, cf. Dummit and Foote, pp. 150-151), we have $Z(D_8) = \{1, r^2\}$. Since any element of the center has $gxg^{-1} = x$, we obtain the two conjugacy classes $\{1\}$ and $\{r^2\}$.

   Since $C_{D_8}(g)$ is a proper subgroup for each g, we have $|C_{D_8}(g)| \in \{2, 4\}$. Next, the class equation for D_8 implies that $6 = \sum |D_8 \colon C_{D_8}(g_j)|$ where the sum is taken over representatives of distinct conjugacy classes. This forces $|C_{D_8}(g)| = 4$ for each $g \notin Z(D_8)$.

   (c) We have already identified the conjugacy classes

   $$\{1\}, \quad \{r^2\}.$$

   The remaining three conjugacy classes contain two elements each. As $rs = sr^{-1}$, we have $srs = r^{-1} = r^3$ so $\{r, r^3\}$ is a conjugacy class. Similarly, $rsr^3 = sr^2$ so $\{s, sr^2\}$ form a second conjugacy class, which leaves $\{sr, sr^3\}$ as the third.

3. **(4 points in total)** Show that a group of order 30 has a normal subgroup which is isomorphic to the cyclic group Z_{15}.

   Solution:

   A detailed argument may be found in Dummit and Foote, pp. 143-144.

4. **(4 points in total)** Let R be a ring with $1 \neq 0$. A non-zero element $a \in R$ is said to be *nilpotent* if there exists $n \in \mathbb{N}$ such that $a^n = 0$.

(a) Let a be nilpotent. Prove that that $1 + a$ is a unit of R. (2p)

(b) Does the set of nilpotent elements of R form an ideal? (2p)

Solution:

(a) Suppose $a^n = 0$ and set $b = 1 - a + \cdots + (-1)^{n-1}a^{n-1}$. Then

$$\begin{aligned}(1+a)b &= (1+a)(1 - a + \cdots + (-1)^{n-1}a^{n-1}) \\ &= 1 - a + \cdots + (-1)^{n-1}a^{n-1} + a + \cdots + (-1)^{n-2}a^{n-1} + (-1)^{n-1}a^n \\ &= 1 + (-1)^{n-1}a^n = 1,\end{aligned}$$

since all terms but two cancel, and since a is nilpotent. A similar computation shows that $b(1+a) = 1$, and it follows that $1 + a$ is a unit.

(b) The set of nilpotent elements of R is not in general an ideal. Consider for instance

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

and view these matrices as elements of the ring $M_{2,2}(\mathbb{Z})$. Then $A^2 = 0$ and $B^2 = 0$ but

$$(A+B)^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathrm{Id}_2,$$

which is not nilpotent. This shows that the set of nilpotent elements of $M_{2,2}(\mathbb{Z})$ does not form an ideal.

5. **(4 points in total)** An ideal I in a commutative ring R is said to be a *primary ideal* of R if

- I is a proper ideal, and
- whenever $a, b \in R$ with $ab \in I$ but $a \notin I$, then there exists $n \in \mathbb{N}$ such that $b^n \in I$.

(a) Give an example of an ideal that is primary but not prime. (1p)

(b) Prove that an ideal is primary if and only if the quotient ring R/I is non-trivial and has the property that every zero divisor is nilpotent. (3p)

Solution:

(a) Consider the ring $\mathbb{Z}$ and the principal ideal $I = (p^2)$ generated by the square of a prime p. This is a proper ideal of $\mathbb{Z}$, and if $ab = rp^2$ with $a \neq qp^2$, $r, q \in \mathbb{Z}$, then b must be a power of p. On the other hand, $a = b = p$ has $ab \in (p^2)$ but neither a nor b belong to (p^2). This shows that (p^2) is not a prime ideal.

(b) Suppose first that I is a primary ideal. Since I is a proper ideal, R/I is non-trivial. Let $b \in R$ have the property that $\bar{b} = b + I$ is a zero divisor. This means that for some $\bar{a} = a + I \neq 0$ in R/I, we have $\bar{a}\bar{b} = 0$. In other words, we have

$$(a+I)(b+I) = 0$$

which implies that $ab \in I$. Since $a \notin I$ (by the assumption $\bar{a} \neq 0$ in R/I) we must have $b^n \in I$ for some $n \in \mathbb{N}$. But then $(b+I)^n = 0$ in R/I and $\bar{b}$ is nilpotent.

Conversely, suppose R/I is non-trivial and that every zero divisor in R/I is nilpotent. Then if $a \notin I$ and $\bar{a}\bar{b} = 0$, so that $\bar{b}$ is a zero divisor, we get $\bar{b}^n = 0$ for some $n \in \mathbb{N}$, meaning that $b^n \in I$ so that I is primary.

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

(a) State *Eisenstein's criterion* for the ring $\mathbb{Z}[x]$ of polynomials with integer coefficients. (1p)

(b) Let p be a prime and consider the polynomial

$$R_p(x) = \frac{x^p - 1}{x - 1}.$$

Is R_p irreducible as an element of $\mathbb{Z}[x]$? (3p)

(Hint: you may find it helpful to introduce a change of variables.)

Solution:

(a) See Dummit and Foote, Corollary 14, p. 310.

(b) Consider

$$S_p(x) = R_p(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} = \frac{(x+1)^p - 1}{x}.$$

By the binomial theorem

$$(x+1)^p = \sum_{j=0}^{p} \left(\begin{array}{c} p \\ j \end{array} \right) x^j,$$

and the terms in the numerator in S_p are divisible by x. More precisely,

$$S_p(x) = x^{p-1} + \sum_{j=1}^{p-1} \left(\begin{array}{c} p \\ j \end{array} \right) x^{j-1} + p.$$

Then S_p is monic, with each $a_0, \ldots, a_{p-1}$ divisible by the prime p, but with $a_0 = p$ not divisible by p^2. By Eisenstein's criterion, S_p is irreducible. But then R_p is irreducible also since a factorization of R_p would imply a factorization of S_p in terms of $x+1$.