Department of Mathematics
Stockholm University

MA 5020 - Abstract Algebra

Summer 2024 - final exam

Examiner: Gregory Arone
Date: October 15, 2024

- **No** use of textbook, notes, or calculators is allowed.
- Unless told otherwise, you may quote results that you learned during the class. When you do, state precisely the result that you are using.
- Be sure to justify your answers, and show clearly all steps of your solutions.

---

1. (a) (2 points) Let G be a group and let $g \in G$ be an element. Suppose that g satisfies $g^3 = e$ and $g^7 = e$, where e is the identity element of G. Prove that $g = e$.

   Answer: $g = g^7 g^{-6} = g^7 g^{-3} g^{-3} = e \cdot e \cdot e = e$.

   (b) (3 points) Let G be a group and H a subgroup of G. Show that there is a bijection between the set of left cosets of H and the set of right cosets of H.

   Answer: Let $g_1, g_2 \in G$ we claim that g_1 and g_2 are in the same left coset of H if and only if g_1^{-1} and g_2^{-1} are in the same right coset of H. Indeed, g_1 and g_2 are in the same left coset of H if and only if there exists an $h \in H$ such that $g_1 = g_2 h$, which is equivalent to saying that $g_2^{-1} = h g_1^{-1}$ for some $h \in H$, which is equivalent to saying that g_1^{-1} and g_2^{-1} are in the same right coset of H.

   It follows that the function $g \mapsto g^{-1}$ induces a map from the set of left cosets of H to the set of right cosets of H. By the same argument it also maps right cosets of H to left cosets of H. It is clear that it is an inverse of itself, so it induces a bijection between left and right cosets.

   Remark: Saying that we define a bijection by sending a coset gH to Hg is incorrect, because this map is not well-defined. It may depend on choice of representatives. Two elements of G may be in the same left coset, but not in the same right coset.

2. (a) (3 points) How many isomorphisms are there from the group $\mathbb{Z}/6 \times \mathbb{Z}/5$ to $\mathbb{Z}/3 \times Z/10$?

   Answer: First of all, both groups are isomorphic to $\mathbb{Z}/30$, so they are isomorphic. The answer is the same as the number of isomorphisms from $\mathbb{Z}/30$ to itself. There are 30 *homomorphisms* from $\mathbb{Z}/30$ to itself: for every integer i modulo 30, there is the homomorphism $\phi(n) = in (\text{mod } 30)$, i.e., multiplication by i mod 30. Multiplication by i is an isomorphism of $\mathbb{Z}/30$ if and only if i is invertible in $\mathbb{Z}/30^*$, which is if and only if i is relatively prime to 30. Since $30 = 2 \times 3 \times 5$, there are exactly 10 invertible elements in $\mathbb{Z}/30^*$, so the answer is **ten isomorphisms**.

   (b) (2 points) How many isomorphisms are there from the group $\mathbb{Z}/4 \times \mathbb{Z}/6$ to $\mathbb{Z}/8 \times \mathbb{Z}/3$?

   Answer: **zero** isomorphisms, because these groups are not isomorphic. You can see it from the classification of finite abelian groups, or by noticing that the second group has an element of order 8, while the first group does not have such an element.

3. (a) (2 points) Prove that there is no simple group of order 312.

   Answer: $312 = 8 \times 3 \times 13$. Let us analyse the number of Sylow subgroups. By Sylow theorems n_{13} is divides 24, and n_{13} is congruent to 1 modulo 13. It follows that $n_{13} = 1$, which means that a group of order 312 must have a normal 13-Sylow subgroup, and thus can not be simple.

(b) (3 points) Let G be a finite group, let $N \triangleleft G$ be a normal subgroup, let p be a prime, and let P be a Sylow p-subgroup of G. Prove that $N \cap P$ is a Sylow p-subgroup of N.

Answer: Clearly $N \cap P$ is a p-group. To prove that it is a Sylow p-subgroup of N, it is enough to show that $[N : P]$ is prime to p. Since N is a normal subgroup, it follows that NP is a subgroup of G. Clearly NP contains P. Since P is a Sylow subgroup of G, it also it a Sylow subgroup of NP. We know that $|NP| = \frac{|N||P|}{|N \cap P|}$, which means that $[NP : P] = [N : N \cap P]$. Since P is a Sylow p-subgroup of NP, $[NP : P]$ is prime to p, and therefore $[N : N \cap P]$ is prime to p.

4. (5 points) Let $\mathbb{Z}/5[x]$ be the ring of polynomials with coefficients in integers modulo 5. Find $\gcd(x^2 - x - 2, x^3 - 7x + 6)$ in $\mathbb{Z}/5[x]$. Furthermore, find two polynomials $p(x), q(x) \in \mathbb{Z}/5[x]$ such that

$$p(x)(x^2 - x - 2) + q(x)(x^3 - 7x + 6) = \gcd(x^2 - x - 2, x^3 - 7x + 6).$$

Answer: We apply Euclid's algorithm to polynomials over the field $\mathbb{Z}/5$. There is an equality in $\mathbb{Z}/5[x]$

$$x^3 - 7x + 3 = (x + 1)(x^2 - x - 2) + (x + 3).$$

Since $x+3$ has lower degree than x^2-x-2, it follows that $\gcd(\mathbf{x^2 - x - 2, x^3 - 7x + 6}) = \mathbf{x + 3}$. Furthermore, the equality above gives an answer to the second question, with $p(x) = -x - 1$ and $q(x) = 1$.

5. (5 points) Suppose R is a PID, and $S \subset R$ is a subring containing the unit of R. Is S necessarily a PID? Prove, or give a counterexample.

Answer: No. For example $\mathbb{Q}[x]$ is a PID, but the subring $\mathbb{Z}[x]$ is not a PID.

6. (5 points) Suppose $\mathbb{F} \subset \mathbb{K}$ are fields and $\alpha \in \mathbb{K}$ is an element for which $[\mathbb{F}(\alpha) : \mathbb{F}]$ is odd. Prove that $\mathbb{F}(\alpha^2) = \mathbb{F}(\alpha)$.

Answer: Let us introduce the notation $\mathbb{L} = \mathbb{F}(\alpha^2)$. We have $\mathbb{L} \subset \mathbb{F}(\alpha)$ and $\alpha^2 \in \mathbb{L}$. It follows that $[\mathbb{F}(\alpha) : \mathbb{L}]$ is either 1 or 2. Furthermore, we know that $[\mathbb{F}(\alpha) : \mathbb{F}] = [\mathbb{F}(\alpha) : \mathbb{L}][\mathbb{L} : \mathbb{F}]$, and $[\mathbb{F}(\alpha) : \mathbb{F}]$ is odd. It follows that $[\mathbb{F}(\alpha) : \mathbb{L}] \neq 2$, so $[\mathbb{F}(\alpha) : \mathbb{L}] = 1$, which means that $[\mathbb{F}(\alpha) = \mathbb{L} = \mathbb{F}(\alpha^2)$.