Department of Mathematics
Stockholm University

MA 5020 - Abstract Algebra

Spring 2023 - final exam

Examiner: Gregory Arone
Date: April 19, 2023

- **No** use of textbook, notes, or calculators is allowed.
- Unless told otherwise, you may quote results that were proved in 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.
- In problems with multiple parts, results of earlier parts can be used in the solution of later parts, even if you do not solve the earlier parts

---

1. For each of the following statements, determine if it is true or false. Give a brief justification or a counterexample.
   (a) (2 points) Every group of order 8 is abelian.
   Solution: False. For example, the dihedral group of order 8 and the quaternion group are not abelian.
   (b) (3 points) Suppose x and y are elements of some group G. If $x^3 = y^3$ then $x = y$.
   Solution: False. For example, take x and y be the two non-trivial elements of the cyclic group of order 3. Then $x^3 = y^3 = e$, but $x \neq y$.

2. Let $\sigma \in S_7$ be the following permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 5 & 7 & 6 & 1 & 4 & 3 \end{pmatrix}.$$

   (a) (1 point) Write σ in cycle notation (i.e., as a product of disjoint cycles).
   Solution: (1, 2, 5)(3, 7)(4, 6).
   (b) (1 point) Find the order of σ.
   Solution: The order is the least common multiplier of the lengths of the cycles, which is 6.
   (c) (1 point) Is σ an even permutation?
   Solution: Yes. Recall that a cycle of an odd length is an even permutation, and vice versa. Since σ is a product of one even and two odd permutations, it is an even permutation.
   (d) (2 points) Find the order of σ^{10}.
   Solution: It is easy to see that $\sigma^{10} = (1, 2, 5)$. It follows that σ^{10} has order 3. Alternatively, you know that the order of σ is 6, and the order of σ^{10} is equal to $\frac{6}{\gcd(6,10)} = 3$.

3. (4 points) Suppose G is a non-abelian group of or order 2^n, for some n. Prove that G has an element of order 4.

   Solution: Note that since G is non-abelian, it follows that $n \geq 3$.

   First of all, I claim that if G has an element of order greater than 2, then G has an element of order 4. Indeed, every element of G has order 2^k for some $0 \leq k \leq n$. Let $x \in G$ be an element of order greater than 4. Then x has order 2^k, for some $2 \leq k \leq n$. Then $x^{2^{k-2}}$ is a well-defined element of G, and I claim that $x^{2^{k-2}}$ has order 4. Indeed $(x^{2^{k-2}})^4 = x^{2^{k-2} \cdot 4} = x^{2^k} = e$. On the other hand, $(x^{2^{k-2}}) \neq e$ and $(x^{2^{k-2}})^2 = (x^{2^{k-1}}) \neq e$.

In view of the claim that we just proved, it is enough to prove that G has an element of order greater than 2. We will prove that if every element of G has order at most 2 then G is a abelian. Indeed, if every element of G has order at most 2, then $x^2 = e$ for every $x \in G$. But then for every $x, y \in G$, $(xy)^2 = e$. This means $xyxy = e$. Multiplying by x on the left and by y on the right, and using that $x^2 = y^2 = e$, we find that $yx = xy$ for all $x, y \in G$.

4. (a) (2 points) Prove that a group of order 45 must be abelian.

   Solution: Let G be a group of order 45. We know that $n_5|9$ and $n_5 \equiv 1(\mod 5)$. It follows that $n_5 = 1$. Similarly, $n_3|5$ and $n_3 \equiv 1(\mod 3)$, which implies $n_3 = 1$. It follows that the 3-Sylow and the 5-Sylow subgroup of G are normal. Let P_3 and P_5 be the Sylow subgroups of G. It follows that $G \cong P_3 \times P_5$. To see this, observe that there is a homomorphism $G \to G/P_5 \times G/P_3$ that sends an element $g \in G$ to the pair $(g \cdot P_5, g \cdot P_3)$. The kernel of this homomorphism is $P_5 \cap P_3 = \{e\}$. It follows that the homomorphism $G \to G/P_5 \times G/P_3$ is injective. By counting elements, it is an isomorphism. Furthermore, the compositions $P_5 \to G \to G/P_3$ and $P_3 \to G \to G/P_5$ have trivial kernels, and therefore are isomorphisms. We have shown that $G \cong P_3 \times P_5$. P_5 is a group of order 5 and P_3 is a group of order 9. Groups of order prime or square of a prime are abelian. It follows that P_3 and P_5 are abelian, and therefore G is abelian.

   (b) (3 points) Prove that a group of order 224 can not be simple.

   Solution: Suppose G is a group of order 224. Note that $224 = 7 \cdot 32$. It follows that $n_2 = 1$ or 7. If $n_2 = 1$ then G has a normal 2-Sylow subgroup, and is therefore not simple. Suppose $n_2 = 7$. Then the action of G on the set of 2-Sylow subgroups induces a non-trivial homomorphism $G \to S_7$. If G is simple, then this homomorphism has to be injective, but this would imply that $224|7!$, which is false. So G can not be simple.

5. Let R, S be rings, and suppose $f\colon R \to S$ is a *surjective* homomorphism of rings. Recall that if $I \subset R$ then $f(I)$ denotes the image of I in S. Similarly, if $J \subset S$, then $f^{-1}(J)$ denotes the pre-image of J in R.

   (a) (2 points) Suppose M is a maximal ideal of S. Prove that $f^{-1}(M)$ is a maximal ideal of R.

   Solution: First, let us check that $f^{-1}(M)$ is an ideal. For concreteness, we will take "ideal" to mean "left ideal". Suppose $x, y \in f^{-1}(M)$. This means that $f(x), f(y) \in M$. But then $f(x - y) = f(x) - f(y) \in M$, so $x - y \in f^{-1}(M)$ and $f^{-1}(M)$ is an additive subgroup. Now suppose $x \in f^{-1}(M)$ and $r \in R$. Then $f(rx) = f(r)f(x)$ is in M, because $f(x) \in M$ and M is an ideal of S. It follows that $rx \in f^{-1}(M)$, so $f^{-1}(M)$ is an ideal.

   Now let us check that $f^{-1}(M)$ is maximal. Suppose we have an ideal J of R satisfying $f^{-1}(M) \subset J \subset R$. We have to prove that either $f^{-1}(M) = J$ or $J = R$. By part (b) below, $f(J)$ is an ideal of S, satisfying $f(f^{-1}(M)) \subset f(J) \subset f(R)$. Since f is surjective, it follows that $f(f^{-1}(M)) = M$ and $f(R) = S$. Thus $M \subset f(J) \subset S$. Since M is maximal in S, $f(J) = M$ or $f(J) = S$. It remains to prove that if $f(J) = M$ then $J = f^{-1}(M)$ and if $f(J) = S$ then $J = R$.

   Suppose $f(J) = M$. Then $f^{-1}(f(J)) = f^{-1}(M)$. It always holds that $J \subset f^{-1}(f(J))$, so $J \subset f^{-1}(M)$. On the other hand we assume that $f^{-1}(M) \subset J$, so $J = f^{-1}(M)$.

   Now suppose $f(J) = S$. Since $f^{-1}(M) \subset J$, $\ker(f) \subset J$. Let $r \in R$ be an arbitrary element. Since $f(J) = S$, there exists a $j \in J$ such that $f(r) = f(j)$. But then $r - j \in \ker(f) \subset J$, and therefore $r = j + (r - j) \in J$. We have shown that every element $r \in R$ is in J, so $J = R$.

(b) (2 points) Suppose I is an ideal of R. Prove that $f(I)$ is an ideal of S.

Solution: Suppose $x, y \in f(I)$. This means that there exist $a, b \in I$ such that $x = f(a)$ and $y = f(b)$. But then $x - y = f(a - b) \in f(I)$.

Now suppose that $f(a) = x \in f(I)$ as before and $s \in S$. Since f is surjective, there exists an $r \in R$ such that $s = f(r)$. But then $sx = f(r)f(a) = f(ra) \in f(I)$. We have proved that $f(I)$ is an ideal.

(c) (2 points) Show with examples that if f is not surjective, then neither (a) nor (b) need to hold.

Solution: Consider the inclusion of rings $\mathbb{Z} \hookrightarrow \mathbb{Q}$. The ideal $(0) \subset \mathbb{Q}$ is maximal, but its preimage is the ideal $(0) \subset \mathbb{Z}$, which is not maximal. Similarly, for all $n \neq 0$ (n) is an ideal of $\mathbb{Z}$, but its image is not an ideal of $\mathbb{Q}$.

6. Let $\mathbb{Q}[x]$ be the polynomial ring over the rationals.

(a) (2 points) Find the greatest common divisor of the polynomials $x^4 - 1$ and $x^5 - x^3$ in $\mathbb{Q}[x]$.

Solution: It is possible to solve the exercise using Euclid's algorithm, but in this case it is easy to do it by just finding the decompositions of the two polynomials into irreducible factors. Indeed, it is easy to see that $x^4 - 1 = (x - 1)(x + 1)(x^2 + 1)$ and $x^5 - x^3 = x^3(x - 1)(x + 1)$. It is easy to see that all these factors are irreducible, and therefore the greatest common divisor is $(x - 1)(x + 1) = (x^2 - 1)$.

(b) (3 points) Is the ideal $(x^4 - 1, x^5 - x^3)$ a maximal ideal of $\mathbb{Q}[x]$?

Solution: No. It follows from part (a) that $(x^4 - 1, x^5 - x^3) = (x^2 - 1)$. Since $x^2 - 1 = (x - 1)(x + 1)$ is not an irreducible polynomial, this ideal is not prime, and in particular not maximal.