Department of Mathematics
Stockholm University

MA 5020 - Abstract Algebra

Summer 2024 - final exam

Examiner: Gregory Arone
Date: August 13, 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. Let S_n denote the symmetric group on n letters, and $\mathbb{Z}/n$ the cyclic group of order n. For each of the following statements, determine if it is true or false. Give a brief justification or a counterexample.

   (a) (2 points) All subgroups of S_4 of order 8 are isomorphic to each other.

   Answer: True, because they are 2-Sylow subgroups, and thus conjugate.

   (b) (2 points) If two subgroups of S_4 are each isomorphic to $\mathbb{Z}/4$ then they are conjugate.

   Answer: True, because every such group is generated by an element of order 4 and all elements of order 4 in S_4 are conjugate.

   (c) (2 points) If two subgroups of S_4 are each isomorphic to $\mathbb{Z}/2\times\mathbb{Z}/2$ then they are conjugate.

   Answer: False. The groups

   $$\{e,(1,2),(3,4),(1,2)(3,4)\} \quad \text{and} \quad \{e,(1,2)(3,4),(1,3)(2,4),(1,4),(2,3)\}$$

   are both isomorphic to $\mathbb{Z}/2\times\mathbb{Z}/2$, but they are not conjugate. You can see this for example because the first group has elements that are not conjugate to any of the elements of the second group.

2. (4 points) How many abelian groups of order 500 are there, up to isomorphisms? Describe each one of them explicitly, as a product of cyclic groups (There may be more than one way to formulate the answer. It is enough to give one description of each group).

   Answer: $500 = 2^2\times 5^3$. An abelian group of order 500 will be a product of an abelian group of order 4 and an abelian group of order 125. The possible abelian groups of order 4 are $\mathbb{Z}/2\times\mathbb{Z}/2$ and $\mathbb{Z}/4$. The possible abelian groups of order 125 are $\mathbb{Z}/5\times\mathbb{Z}/5\times\mathbb{Z}/5$, $\mathbb{Z}/5\times\mathbb{Z}/25$, and $\mathbb{Z}/125$. There are, therefore, 6 different abelian groups of order 500. They are

   $$\mathbb{Z}/2\times\mathbb{Z}/2\times\mathbb{Z}/5\times\mathbb{Z}/5\times\mathbb{Z}/5 \quad \mathbb{Z}/2\times\mathbb{Z}/2\times\mathbb{Z}/5\times\mathbb{Z}/25 \quad \mathbb{Z}/2\times\mathbb{Z}/2\times\mathbb{Z}/125,$$

   $$\mathbb{Z}/4\times\mathbb{Z}/5\times\mathbb{Z}/5\times\mathbb{Z}/5 \qquad \mathbb{Z}/4\times\mathbb{Z}/5\times\mathbb{Z}/25 \qquad \mathbb{Z}/4\times\mathbb{Z}/125$$

3. (a) (2 points) Let Q be a normal p-subgroup of a finite group G. Prove that Q is contained in every p-Sylow subgroup of G.

   Answer: Let P be a p-Sylow subgroup of G. By the second Sylow theorem, Q is contained in some conjugate of P. This is equivalent to saying that some conjugate of Q is contained in P. But Q is normal, so every conjugate of Q is the same as Q. So Q is contained in P.

   (b) (3 points) Prove that a group of order 132 must have a normal p-Sylow subgroup for some prime p that divides 132.

   Answer: $132 = 4\times 3\times 11$. We need to show that one of the numbers n_2, n_3 and n_{11} must be 1. By Sylow theorem, $n_{11} = 1$ or 12. If $n_{11} = 1$, we are done. Suppose $n_{11} = 12$. Then

G has 120 elements of order 11. Again by Sylow theorem if $n_3 \neq 1$ then n_3 is at least 4. Suppose $n_3 \geq 4$. Then G has *at least* 8 elements of order 3. Thus if n_{11} and n_3 are both greater than one, then G has at least 128 elements of order 3 or 11. It means that the union of 2-Sylow subgroups can contain at most 4 elements, which means that there can be at most one 2-Sylow subgroup, so $n_2 = 1$ in this case.

4. (5 points) Let R be a commutative ring with unit. Suppose that there is a non-zero ring homomorphism $\phi\colon R \to \mathbb{Z}$. Prove that R has infinitely many maximal ideals.

Answer: First of all we claim that ϕ must be surjective. Indeed $\phi(1)$ satisfies $\phi(1)^2 = \phi(1)$, so $\phi(1) = 0$ or 1. If $\phi(1) = 0$ then $\phi(r) = 0$ for all $r \in R$. So $\phi(1) = 1$. But then $\phi(n \cdot 1) = n$ for all $n \in \mathbb{Z}$, so ϕ is surjective.

Next we claim that if $\phi\colon R \twoheadrightarrow S$ is a *surjective* ring homomorphism and M is a maximal ideal of S then $\phi^{-1}(M)$ is a maximal ideal of R. I leave the details of this step to you, but it is basically an application of the fourth isomorphism theorem. Furthermore, if M_1, M_2 are distinct ideals of S then $\phi^{-1}(M_1)$ and $\phi^{-1}(M_2)$ are distinct ideals of R. Again, this follows from surjectivity of ϕ. Since $\mathbb{Z}$ has infinitely many maximal ideals, it follows that R has infinitely many maximal ideals.

5. (5 points) Let $\mathbb{R}$ and $\mathbb{C}$ be the fields of real and complex numbers respectively. Prove that there is an isomorphism of rings $\mathbb{R}[x]/(x^4-1) \cong \mathbb{R}\times\mathbb{R}\times\mathbb{C}$. Construct an explicit isomorphism.

Answer: Given a polynomial $p = p(x)$, we denote by $(p(x))$ the ideal of $\mathbb{R}[x]$ generated by p. We have factorisation $(x^4 - 1) = (x - 1)(x + 1)(x^2 + 1)$, which can be interpreted as a factorisation of ideals. We claim that every two of the ideals $(x - 1), (x + 1)$ and $(x^2 + 1)$ are co-maximal. For example, let us show that the ideals $(x - 1)$ and $(x^2 + 1)$ are co-maximal. For this, it is enough to show that 1 belongs to the ideal $(x - 1) + (x^2 + 1)$. This follows from the equality of polynomials.

$$1 = -\frac{1}{2}(x + 1)(x - 1) + \frac{1}{2}(x^2 + 1).$$

It follows by the Chinese Remainder theorem that the quotient homomorphisms induce an isomorphism of rings

$$\mathbb{R}[x]/(x^4 - 1) \xrightarrow{\cong} \mathbb{R}[x]/(x - 1) \times \mathbb{R}[x]/(x + 1) \times \mathbb{R}[x]/(x^2 + 1).$$

Furthermore, there are isomorphisms $\mathbb{R}[x]/(x-1) \xrightarrow{\cong} \mathbb{R}$, $\mathbb{R}[x]/(x+1) \xrightarrow{\cong} \mathbb{R}$, and $\mathbb{R}[x]/(x^2+1) \xrightarrow{\cong} \mathbb{C}$, given by evaluating a polynomial at 1, -1 and i respectively. That these homomorphisms are isomorphisms follows easily from division with remainder. Combining the isomorphisms above, we get the desired isomorphism

$$\mathbb{R}[x]/(x^4 - 1) \xrightarrow{\cong} \mathbb{R} \times \mathbb{R} \times \mathbb{C}.$$

It is defined by the formula

$$p(x) \mapsto (p(1), p(-1), p(i)).$$

6. (5 points) Let $\mathbb{K}/\mathbb{F}$ be an algebraic field extension. Suppose that $\mathbb{F} \subset R \subset \mathbb{K}$, where R is a *subring* of $\mathbb{K}$ containing $\mathbb{F}$. Prove that R is in fact a subfield of $\mathbb{K}$.

Answer: Let r be a non-zero element of R. Thus r is a non-zero element of $\mathbb{K}$, and therefore r^{-1} exists in $\mathbb{K}$. To prove that R is a field we need to prove that $r^{-1} \in R$. Since $\mathbb{K}$ is algebraic over $\mathbb{F}$, r is algebraic over $\mathbb{F}$. There exists a polynomial in $p(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{F}[x]$

such that $p(r) = 0$. We may assume that $a_0 \neq 0$, because otherwise we may divide $p(x)$ by some power of x and get a polynomial of smaller degree that vanishes at r. Furthermore, we can divide the polynomial by $-a_0$, and thus assume that $a_0 = -1$.

We have the following equality in $\mathbb{K}$

$$-1 + a_1 r + \cdots + a_n r^n = 0.$$

Therefore, the following is a valid equality in $\mathbb{K}$

$$r(a_1 + a_2 r + \cdots a_n r^{n-1}) = 1.$$

It follows that the following is a valid equality in $\mathbb{K}$:

$$r^{-1} = a_1 + a_2 r + \cdots a_n r^{n-1}.$$

The right hand side is obtained by adding and multiplying elements of R (but no dividing by elements of R), therefore it is an element of R. It follows that $r^{-1} \in R$.