Department of Mathematics
Stockholm University

MA 5020 - Abstract Algebra

Summer 2022 - Make up exam

Examiner: Gregory Arone
Date: Oct 12, 2022

- You may use the text (Dummit and Foote).
- You may **not** use class notes and/or any notes and study guides you have created.
- You may **not** use a calculator, a cell phone or computer.
- You may quote results that are proved in the book. When you do, state precisely the result that you are using, or give a precise pointer to the book.
- 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. Let S_5 be the group of permutations of the set $\{1, 2, 3, 4, 5\}$. Let $H \subset S_5$ be the subset consisting of permutations σ that satisfy $\sigma(3) = 3$.
   (a) (2 points) Prove that H is a subgroup of S_5.
   Solution: H is the stabilizer of 3. The stabilizer of an element under a group action is always a subgroup. See Dummit & Foote, page 51.
   (b) (1 point) Find the number of elements in H.
   Solution: It is clear that the action of Σ_5 on $\{1, 2, 3, 4, 5\}$ is transitive. By the orbit-stabilizer theorem $[\Sigma_5 : H] = 5$. It follows that $|H| = \frac{5!}{5} = 24$.
   Alternatively, it is easy to prove directly that H is isomorphic to S_4, which has 24 elements.
   (c) (2 points) Is H a normal subgroup of S_5?
   Solution: No. For example $(1, 2) \in H$, but $(2, 3)(1, 2)(2, 3)^{-1} = (1, 3) \neq H$.

2. (a) (2 points) Let G be a finite group and let $\mathbb{Z}$ denote the additive group of integers. Prove that there are no non-trivial homomorphisms from G to $\mathbb{Z}$.
   Solution: Suppose $f : G \to \mathbb{Z}$ is a homomorphism. Let $x \in G$. Since G is finite, there exists a positive integer n such that $x^n = e_G$. But then $f(x^n) = nf(x) = 0$. Here I am using multiplicative notation for the group operation in G, but additive notation for $\mathbb{Z}$. It follows that $f(x)$ is an integer satsifying $nf(x) = 0$ for some $n > 0$. This means that $f(x) = 0$ for all $x \in G$, so f is trivial.
   (b) (2 points) How many group homomorphisms are there from $\mathbb{Z}/12$ to $\mathbb{Z}/15$?
   Solution: Three homomorphisms. The set of homomorphisms is in bijective correspondence with the set of elements $x \in \mathbb{Z}/15$ that satisfy $12x \equiv 0(\mod 15)$. There are three such elements: $0, 5$, and 10.
   In general, the number of homomorphism from $\mathbb{Z}/m$ to $\mathbb{Z}/n$ is $\gcd(m, n)$.

3. Let p be a prime.
   (a) (2 points) Suppose G is any group and $N \lhd G$ is a normal subgroup of **index** p. Let $K \subset G$ be any subgroup. Prove that either $K \subset N$ or $KN = G$.
   Solution: Suppose K is not a subset of N. We will prove that $KN = G$. Clearly, $N \subsetneq KN \subseteq G$. Since N is normal, it follows that KN is a subgroup of G. It follows that $[G : KN]$ is a divisor of $[G : N]$, and $[G : KN] < [G : N]$. But $[G : N]$ is a prime. It follows that $[G : KN] = 1$, which means that $NK = G$.

(b) (3 points) Suppose P is a p-group and $N \lhd P$ is a normal subgroup of **order** p. Prove that $N \subset Z(P)$, i.e., N is in the center of P.

Solution: Since N is normal in P, P acts on N by conjugation. Since P is a p group, the number of elements of N that are fixed by the action is congruent modulo p to the total number of elements of N. The total number of elements of N is p. It follows that the number of elements of N that are fixed by the action is either zero or p. The trivial element is fixed by the conjugation, so the fixed point set has at least one element. Therefore it has p elements. This means that all of N is fixed by the conjugation action. In other words, for every $n \in N$ and $p \in P$, $p^{-1}np = n$, or $np = pn$. This means that N is in the center of P.

4. (a) (3 points) Prove that every group of order 1225 is abelian. For your convenience: $1225 = 5^2 \cdot 7^2$.

Solution: Let G be a group of order 1225. By Sylow theorem $n_5 \equiv 1 (\mod 5)$ and $n_5 | 49$. It follows that $n_5 = 1$. Similarly, $n_7 = 1$. It follows that the 5-Sylow and the 7-Sylow subgroups of G are normal. Let us denote the Sylow subgroups by P_5 and P_7. These are groups of order p^2 where p is 5 or 7, and therefore they are abelian (page 125, Corollary 9).

There is a group homomorphism $G \to G/P_5 \times G/P_7$, whose kernel is $P_5 \cap P_7 = \{e\}$. Since the kernel is trivial, this is a monomorphism, and by counting elements it is an isomorphism. A similar argument shows that the compositions $P_5 \hookrightarrow G \to G/P_7$ and $P_7 \hookrightarrow G \to G/P_5$ are isomorphisms. It follows that G is isomorphic to $P_5 \times P_7$. So G is a product of abelian groups, and therefore is abelian.

(b) (3 points) Prove that a group of order 224 can not be simple. For your convenience: $224 = 32 \cdot 7$.

Solution: Suppose G is a group of order 224. It follows from the Sylow theorems 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. (3 points) Let $\mathbb{F}$ be a field.

(a) (2 points) Prove that there is an isomorphism of rings $\mathbb{F}[x, y]/(x - y^2) \cong \mathbb{F}[z]$.

Solution: There is a ring homomorphism $f \colon \mathbb{F}[x, y] \to \mathbb{F}[z]$, determined by the conditions $f(1) = 1$, $f(y) = z$, $f(x) = z^2$. Clearly $f(x - y^2) = 0$, so $(x - y^2) \subset \ker(f)$. It follows that f passes to a ring homomorphism $\bar{f} \colon \mathbb{F}[x, y]/(x - y^2) \to \mathbb{F}[z]$.

There also is a ring homomorphism $g \colon F[z] \to \mathbb{F}[x, y]$ determined by the conditions $g(1) = 1$ and $g(z) = y$. Composing with the quotient homomorphism $\mathbb{F}[x, y] \to \mathbb{F}[x, y]/(x - y^2)$ we obtain a ring homomorphism $\bar{g} \colon F[z] \to \mathbb{F}[x, y]/(x - y^2)$.

We will prove that $\bar{f}$ and $\bar{g}$ are isomorphisms, by proving that they are inverse of each other.

To begin with $\bar{f}(\bar{g}(1)) = 1$ and $\bar{f}(\bar{g}(z)) = f(y) = z$. It follows that $\bar{f} \circ \bar{g}$ is the identity homomorphism on $\mathbb{F}[z]$.

For the other composition, let I be the ideal $(x - y^2)$. We have $\bar{g}(\bar{f}(1)) = 1$, and

$$\bar{g}(\bar{f}(x + I)) = \bar{g}(f(x)) = \bar{g}(z^2) = y^2 + I = x + I.$$

The last equality follows because $x - y^2 \in I$.
Furthermore, $\bar{g}(\bar{f}(y + I)) = \bar{g}(f(y)) = \bar{g}(z) = y + I$.
We have shown that $\bar{g} \circ \bar{f}$ is the identity on 1, $x + I$ and on $y + I$. It follows that $\bar{g} \circ \bar{f}$ is the identity homomorphism on $\mathbb{F}[x, y]/I$.

(b) (3 points) Prove that the rings $\mathbb{F}[x, y]/(x - y^2)$ and $\mathbb{F}[x, y]/(x^2 - y^2)$ are not isomorphic.

Solution: We proved in part (a) that $\mathbb{F}[x, y]/(x - y^2) \cong F[z]$, so it is an integral domain. On the other hand $\mathbb{F}[x, y]/(x^2 - y^2)$ is not an integral domain, because $x^2 - y^2 = (x - y)(x + y)$ is a reducible element, so the ideal generated by it is not a prime ideal.

6. Let R be a commutative ring with a unit. Suppose that I and J are co-maximal ideals of R.

(a) (3 points) Prove that I and J^2 are co-maximal ideals.

Solution: It is enough to prove that 1 can be written as a sum of an element of I and and element of J^2. Since I and J are comaximal, there exists $x \in I$ and $y \in J$ such that $1 = x + y$. But then $1 = x + y(x + y) = x(1 + y) + y^2$. But then $x(1 + y) \in I$, because I is an ideal, and $y^2 \in J^2$ by the definition of J^2.

(b) (2 points) Is the assumption that R has a unit necessary in part (a)? Justify your answer with either an argument or a counterexample.

Solution: Yes, it is necessary. For example consider the ring $2\mathbb{Z}$, consisting of even integers. This is a ring without unit. Let $I = (4)$ be the ideal of numbers divisible by 4 and $J = (6)$ the ideal of numbers divisible by 6. Then I and J are comaximal in $2\mathbb{Z}$, because $6 - 4 = 2$, and every even number can be written as a sum of a multiple of 6 and a multiple of 4. But I and $J^2 = (36)$ are not comaximal, because $I + J^2$ consists of numbers divisible by 4, rather than all even numbers.