Department of Mathematics
Stockholm University

MA 5020 - Abstract Algebra

Final Exam

Examiner: Gregory Arone
Date: August 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 $H \subset S_4$ be the subgroup generated by $(1, 3)$ and $(1, 2, 3, 4)$.

   (a) (2 points) List the elements of H.

   Solution: Let C_2 and C_4 be the subgroup of S_4 generated by $(1, 3)$ and $(1, 2, 3, 4)$. Clearly $C_2C_4 \subset H$. On the other hand, we claim that C_2C_4 is a subgroup (rather than just a subset) of S_4. To prove this, it is enough to check that C_2 normalizes C_4, and for this it is enough to check that $(1, 3)(1, 2, 3, 4)(1, 3)^{-1} \in C_4$. By a direct calculation

   $$(1, 3)(1, 2, 3, 4)(1, 3)^{-1} = (1, 3)(1, 2, 3, 4)(1, 3) = (1, 4, 3, 2) = (1, 2, 3, 4)^{-1} \in C_4.$$

   Since C_2C_4 is a subgroup of S_4 it follows that $C_2C_4 = H$. So the elements of H are all the possible products of the form xy, where $x \in C_2$ and $y \in C_4$. Explicitly, the elements are the following:

   $$e, (1, 2, 3, 4), (1, 3)(2, 4), (1, 4, 3, 2), (1, 3), (1, 2)(3, 4), (2, 4), (1, 4)(2, 3)$$

   Remark: H is a 2-Sylow subgroup of S_4.

   (b) (2 points) Is H a normal subgroup of S_4?

   Solution: No. A 2-Sylow subgroup of S_4 is not normal. We can verify this concretely by taking the element $(1, 3) \in H$ and conjugating it by $(1, 2)$. By a direct calculation

   $$(1, 2)(1, 3)(1, 2)^{-1} = (1, 2)(1, 3)(1, 2) = (2, 3) \notin H.$$

2. Let G be a group with the property that for every $x \in G$, $x^2 = e$

   (a) (2 points) Prove that G is abelian.

   Solution: Let $x, y \in G$. We want to prove that $xy = yx$. By assumption $xyxy = e$. Let us multiply both sides of this equality on the right by yx. We obtain the equality $xyxyyx = yx$. Using that $y^2 = e$ and then that $x^2 = e$ we get that the left hand side of this equality is the same as xy. We have proved that $xy = yx$.

   (b) (2 points) Suppose that G is also finite. Prove that the number of elements of G is a power of 2.

   Solution: Let $|G|$ be the number of elements of G. Suppose $|G|$ is not a power of 2. Then there exists an odd prime p such that p divides $|G|$. By Cauchy's theorem, G has an element of order p, contradicting the assumption that every non-identity element of G has order 2.

3. Suppose G is a group acting on a set X. Recall that the action is said to be

   - *transitive* if for all $u, v \in X$, there exists a $g \in G$ such that $gu = v$.
   - *free* if for all $g \in G \setminus \{e\}$ and all $x \in X, gx \neq x$.

   Suppose K and H are subgroups of G. Let G/H denote the set of left cosets of H. Then K acts on G/H by the formula $k \cdot (gH) = (kg)H$. This is the restriction of the standard action of G on G/H.

   (a) (2 points) Prove that the action of K on G/H is transitive if and only if $KH = G$.

   Solution: Suppose that the action of K on G/H is transitive. Then for every element $g \in G$ there exists an element $k \in K$ such that $k(eH) = kH = gH$. This means that $k^{-1}g \in H$, so $k^{-1}g = h$ for some $h \in H$. In other words, $g = kh$. We have shown that for every $g \in G$ we can find elements $k \in K$ and $h \in H$ such that $g = kh$. This means precisely that $G = KH$.

   Conversely suppose that $G = KH$. We want to prove that the action of K on G/H is transitive. This means that we want to show that for every $g_1, g_2 \in G$ there exists an element $k \in K$ such that $g_2H = kg_1H$. Equivalently, we want to show that for every $g_1, g_2 \in G$ there exists an element $k \in K$ such that $g_2^{-1}kg_1 \in H$. Since $G = KH$, we can write $g_1 = k_1h_1$ and $g_2 = k_2h_2$ for some $k_1, k_2 \in K$, $h_1, h_2 \in H$. Let $k = k_2k_1^{-1}$. Then

   $$g_2^{-1}kg_1 = h_2^{-1}k_2^{-1}k_2k_1^{-1}k_1h_1 = h_2^{-1}h_1 \in H.$$

   (b) (2 points) For which values of n is the action of A_n on S_n/C_n transitive? Here A_n denotes the alternating group, and C_n is the cyclic subgroup of S_n generated by the cycle $(1, 2, ..., n)$.

   Solution: By part (a), the action is transitive if and only if $S_n = A_nC_n$. This is equivalent to the condition $|S_n| = |A_nC_n|$. Recall that

   $$|A_nC_n| = \frac{|A_n||C_n|}{|A_n \cap C_n|} = \frac{\frac{n!}{2}n}{|A_n \cap C_n|}.$$

   We have obtained the condition that the action is transitive if and only if

   $$n! = \frac{\frac{n!}{2}n}{|A_n \cap C_n|}.$$

   This is equivalent to the condition $|A_n \cap C_n| = \frac{n}{2}$, so the question becomes: for which n do we have this equality?

   Recall that if n is odd, then the permutation $(1, 2, \ldots, n)$ is even, and therefore every power of this permutation is even. This means that if n is odd then $C_n \subset A_n$, and therefore $|A_n \cap C_n| = n$ in this case.

   On the other hand, if n is even then $(1, 2, \ldots, n)$ is an odd permutation, but $(1, 2, \ldots, n)^2$ is even. More generally $(1, 2, \ldots, n)^i$ is an even permutation if and only if i is even. So in this case half of the elements of C_n are even, and thus $|A_n \cap C_n| = \frac{n}{2}$ when n is even.

   Answer: the action is transitive if and only if n is even.

(c) (3 points) Let p and q be distinct primes. Suppose that P and Q are a p-subgroup and a q-subgroup of G respectively. Prove that the action of P on G/Q is free.

Solution: Let $x \in P$ be a non-identity element. We want to prove that for every $g \in G$, $xgQ \neq gQ$. This is equivalent to showing that for every $g \in G$ $g^{-1}xg \notin Q$. But $x \in P$, so x is an element whose order is a power of p (and is greater than 1, since x is not the identity). For all $g \in G$, the element $g^{-1}xg$ has the same order as x, so it is a power of p. But every element of Q has order that is a power of q, and a non-zero power of p can not be a power of q. So $g^{-1}xg$ can not be an element of Q.

4. (a) (3 points) Prove that a group with 132 elements can not be simple.

Solution: Let us start with the observation that $132 = 2^2 \cdot 3 \cdot 11$. Let G be a group with 132 elements. As usual, let n_p denote the number of p-Sylow subgroups of G. We know that $n_{11} \equiv 1 \pmod{11}$ and $n_{11}|12$. It follows that $n_{11} = 1$ or 12. If $n_{11} = 1$ then G has a normal 11-Sylow subgroup, is not simple, and we are done. Suppose $n_{11} = 12$. Then G has 120 elements of order 11. Let us consider n_3. By the Sylow theorem, $n_3|44$ and $n_3 \equiv 1 \pmod{3}$. The possibilities are $n_3 = 1, 4$ or 22. If $n_3 = 1$ then G is not simple. If $n_3 = 22$ then G has 44 elements of order 3, which together with 120 elements of order 11 gives more than 132 elements, a contradiction. If $n_3 = 4$ then G has 8 elements of order 3, so it has 128 elements of order either 3 or 11. This leaves at most 4 elements belonging to a 2-Sylow subgroup which means that $n_2 = 1$ and G is not simple.

To summarize: We have shown that at least one of n_{11}, n_3, n_2 is 1, so G is not simple.

(b) (3 points) Prove that a group with 216 elements can not be simple.

Solution: Let G be an group with 216 elements. Observe that $216 = 2^3 \cdot 3^3$. Applying Sylow theorems, we find that $n_3 = 1$ or 4. If $n_3 = 1$, G is not simple and we are done. Suppose $n_3 = 4$. Then the action of G on the set of 3-Sylow subgroups by conjugation induces a non-trivial homomorphism $G \to S_4$. Since the homomorphism is non-trivial, the kernel is a proper normal subgroup of G. Since $|S_4| = 24 < 216$, the homomorphism is not injective and the kernel is non-trivial. We have shown that if $n_3 = 4$ then G has a proper, non-trivial normal subgroup of G, and G is not simple.

5. (3 points) Find all the maximal ideals of the ring $\mathbb{Z} \times \mathbb{Z}$.

Hint: show that every ideal of $\mathbb{Z} \times \mathbb{Z}$ is of the from $I \times J$, where I and J are ideals of $\mathbb{Z}$.

Solution: Let us first do the hint. Suppose A is an ideal of $\mathbb{Z} \times \mathbb{Z}$. Let

$$I = \{x \in \mathbb{Z} \mid \exists y \in \mathbb{Z}, (x, y) \in A\}.$$

Similarly define $J = \{y \in \mathbb{Z} \mid \exists x \in \mathbb{Z}, (x, y) \in A\}$.

First of all I claim that I and J are ideals of $\mathbb{Z}$. Let's prove that I is an ideal. Suppose $x_1, x_2 \in I$. This means that there exists integers y_1, y_2 such that $(x_1, y_1), (x_2, y_2) \in A$. But then, since A is an ideal of $\mathbb{Z} \times \mathbb{Z}$, we have that $(x_1, 0) = (x_1, y_1)(1, 0) \in A$. Similarly $(x_2, 0) \in A$. But then $(x_1, 0) + (x_2, 0) \in A$, which implies that $x_1 + x_2 \in I$. We have proved that I is closed under addition. Similarly, for any $a \in \mathbb{Z}$, $(ax_1, 0) \in A$, so $ax_1 \in I$. We have proved that I is an ideal. In the same way one proves that J is an ideal.

Next, I claim that $A = I \times J$. Suppose $(x, y) \in A$. Then by definition $x \in I$, $y \in J$, and $(x, y) \in I \times J$, so $A \subset I \times J$. On the other hand, if $x \in I$ and $y \in J$, we have seen that $(x, 0) \in A$, and similarly $(0, y) \in A$, so $(x, y) = (x, 0) + (0, y) \in A$. We have shown that $I \times J \subset A$, so $A = I \times J$.

We know that every ideal of $\mathbb{Z}$ is principal, and it has the form (m), where we can assume that $m \geq 0$, since $(m) = (-m)$. It follows that every ideal of $\mathbb{Z} \times \mathbb{Z}$ has the form $(m) \times (n)$ for some non-negative integers m, n.

The question is, which of these ideals are maximal? An ideal in a commutative ring is maximal if and only if the quotient of the ring by the ideal is a field. Now the quotient ring $\mathbb{Z}\times\mathbb{Z}/(m)\times(n)$ is isomorphic to $\mathbb{Z}/m \times \mathbb{Z}/n$. This is a field if and only if one of the numbers m, n is 1, and the other one is a prime. I leave this step as an exercise to you. It follows that the maximal ideals of $\mathbb{Z} \times \mathbb{Z}$ are ideals of the form $(1) \times (p)$ and $(p) \times (1)$, where p is a prime number.

Perhaps some will like a more explicit description of the following form. Let p be a prime number. The set of pairs (x, y) where x is divisible by p is a maximal ideal. So is the set of pairs where y is divisible by p. Every maximal ideal of $\mathbb{Z} \times \mathbb{Z}$ is one of these ideals for some prime p.

6. Let $R = \mathbb{Z}[\sqrt{-5}]$ be the subring of $\mathbb{C}$ consisting of elements of the form $a + b\sqrt{-5}$, where a and b are integers. Let I be the ideal of R generated by 2 and $1 + \sqrt{-5}$. We can write $I = (2, 1 + \sqrt{-5})$. Similarly, let $J = (3, 2 - \sqrt{-5})$.

   (a) (3 points) Prove that I is not a principal ideal.

   Remark: it is also true that J is not principal, but you are not required to show that.

   Solution: For every element $a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$, let us define $N(a + b\sqrt{-5}) = a^2 + 5b^2$. The number $N(a + b\sqrt{-5})$ is always an integer. Furthermore, since it is just the square of the usual norm of a complex number, it satisfies

$$N((a + b\sqrt{-5}) \cdot (c + d\sqrt{-5})) = N(a + b\sqrt{-5}) \cdot N(c + d\sqrt{-5}).$$

   It follows that if $a + b\sqrt{-5}$ divides $c + d\sqrt{-5}$ in $\mathbb{Z}[\sqrt{-5}]$ then $N(a + b\sqrt{-5})$ divides $N(c + d\sqrt{-5})$ in $\mathbb{Z}$.

   We want to show that I is not principal. Suppose by contradiction that I is principal and is generated by $a + b\sqrt{-5}$. Then $a + b\sqrt{-5}$ divides 2 and $1 + \sqrt{-5}$. It follows that $N(a+b\sqrt{-5})$ divides $N(2) = 4$ and $N(1+\sqrt{-5}) = 6$. It follows that $N(a+b\sqrt{-5})$ divides 2, so $N(a + b\sqrt{-5}) = 1$ or 2.

   It is easy to show that there do not exists integers a and b for which $a^2 + 5b^2 = 2$. So $a^2 + 5b^2 = 1$, which is only possible if $a = \pm 1$ and $b = 0$. It follows that if I is principal then $I = (1)$ is the entire ring. But I is not the entire ring: it is easy to show that if $a + b\sqrt{-5} \in I$ then $a \equiv b (\text{mod } 2)$. So I is not principal.

   (b) (3 points) Prove that $IJ = (1 + \sqrt{-5})$. In particular, IJ is principal.

   Solution: By definition, I is the ideal generated by 2 and $1 + \sqrt{-5}$, and J is the ideal generated by 3 and $2 - \sqrt{-5}$. It follows that IJ is the ideal generated by the four elements

$$6, 4 - 2\sqrt{-5}, 3 + 3\sqrt{-5}, 7 + \sqrt{-5}.$$

   We have to check that the ideal generated by these four elements is exactly the ideal generated by the single element $1 + \sqrt{-5}$. For one direction, we note that

$$1 + \sqrt{-5} = (7 + \sqrt{-5}) - 6$$

   which implies that $(1+\sqrt{-5}) \subset IJ$. For the other direction, we need to check that each one of the elements $6, 4 - 2\sqrt{-5}, 3 + 3\sqrt{-5}, 7 + \sqrt{-5}$ is divisible by $1 + \sqrt{-5}$. Using division of complex numbers, or just trial and error, one finds that $6 = (1+\sqrt{-5})(1-\sqrt{-5})$, $4-2\sqrt{-5} = (1+\sqrt{-5})(-1-\sqrt{-5})$, $3+3\sqrt{-5} = 3(1+\sqrt{-5})$ and $7+\sqrt{-5} = (1+\sqrt{-5})(2-\sqrt{-5})$. These equalities prove that $IJ \subset (1+\sqrt{-5})$, and we are done.