Department of mathematics,
Stockholm University
Examinator: Gregory Arone

MA 5020 - Abstract Algebra
Final Exam (at home)

August 20, 2021

Instructions: You are allowed to consult the textbook. Notes and calculators are not allowed. Searching the internet for solutions is NOT 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. 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

On the first page, write the following

1. Your name
2. Your personal number
3. Write and sign the following pledge on the first page:

> *On my honor as a student, I have not received help or used inappropriate resources on this exam.*

After this, begin every problem on a new page (but you do not have to begin every part of a problem on a new page).
Unless you have made provisions for extra time, the exam must be uploaded no later 15:00.

---

1. Here and throughout the test, $\mathbb{Z}/n$ denotes the cyclic group of order n, S_n is the group of permutations of $\{1, \dots, n\}$ and $A_n \subset S_n$ is the subgroup of even permutations.

   (a) [3 pts] Which of the following groups of order 60 are isomorphic to each other? Give a brief and clear justification

   1. $\mathbb{Z}/60$, 2. A_5, 3. $\mathbb{Z}/10\times\mathbb{Z}/6$, 4. $\mathbb{Z}/3\times\mathbb{Z}/5\times\mathbb{Z}/4$, 5. $\mathbb{Z}/2\times\mathbb{Z}/2\times\mathbb{Z}/3\times\mathbb{Z}/5$, 6. $A_4\times\mathbb{Z}/5$.

   Solution: (1) is isomorphic to (4), (3) is isomorphic to (5), and otherwise the groups are all distinct.
   To prove that (1) is isomorphic to (4) and (3) is isomorphic to (5), use the Chinese remainder theorem. To prove that the groups (1) and (4) are *not* isomorphic to (3) and (5) use the fact that (1) and (4) have an element of order 4, while (3) or (5) don't. I leave the details of this to you.
   Note that the groups (1), (4), (3) and (5) are abelian, while (2) and (6) are not abelian. It follows that (2) and (6) are not isomorphic to any of the other 4 groups. It remains to prove that (2) and (6) are not isomorphic to each other. There are many ways to do it. One way is to note that the 5-Sylow subgroup of A_5 is not normal, while the 5-Sylow subgroup of $A_4 \times \mathbb{Z}/5$ is normal (and even central). Again, I leave you the details.

   (b) [1 pt] Does there exist an injective group homomorphism $\mathbb{Z}/21 \hookrightarrow A_{10}$?

   Solution: Yes. The permutation $(1, 2, 3)(4, 5, 6, 7, 8, 9, 10)$ is an even permutation of 10 elements, so it is an element of A_{10}. It has order 21, so it generates a cyclic subgroup of order 21.

(c) [1 pt] Does there exist an injective group homomorphism $Q_8 \hookrightarrow S_5$? Here Q_8 is the quaternion group.

Solution: No. Let us first prove an auxiliary claim:
Claim: Suppose σ and τ are two elements of order 4 of S_5, such that $\sigma^2 = \tau^2$. Then either $\sigma = \tau$ or $\sigma = \tau^{-1}$.
Proof of claim: Suppose $\sigma \in S_5$ is an element of order 4. Then σ must be a 4-cycle, and we can write $\sigma = (a, b, c, d)$. Then $\sigma^2 = (a, c)(b, d)$, and it is clear that the only other 4-cycle whose square is $(a, c)(b, d)$ is (a, d, c, b), which is the inverse of σ. This proves the claim.
Now suppose, by contradiction, that $f\colon Q_8 \hookrightarrow S_5$ is an injective homomorphism. Notice that i, j are distinct elements of Q_8 or order 4 satsifying $i^2 = j^2 = -1$, and $j \neq i^{-1}$. It follows that $f(i)$ and $f(j)$ are distinct elements of S_5 or order 4, whose squares are the same and that are not inverse to each other. This contradicts the claim.

2. Let G be a group, and $X \subset G$ a subset (not necessarily a subgroup). Recall that the centralizer of X, denoted $C_G(X)$, is defined as follows

$$C_G(X) = \{g \in G \mid gx = xg \text{ for all } x \in X\}.$$

You can use without proof that $C_G(X)$ is always a subgroup of G.

(a) [2 pts] Suppose N is a normal subgroup of G. Prove that $C_G(N)$ is a normal subgroup of G.

Solution: Let $c \in C_G(N)$ and $g \in G$. We need to prove that $gcg^{-1} \in C_G(N)$. For this, we need to prove that for every $n \in N$, $gcg^{-1}ngc^{-1}g^{-1} = n$. Since N is normal, we can say that $g^{-1}ng = n_1$, where $n_1 \in N$. So we have $gcg^{-1}ngc^{-1}g^{-1} = gcn_1c^{-1}g^{-1}$. Since $c \in C_G(N)$, we can say that $cn_1c^{-1} = n_1$, so $gcg^{-1}ngc^{-1}g^{-1} = gn_1g^{-1}$. Now recall that $n_1 = g^{-1}ng$, so $gn_1g^{-1} = n$. It follows that $gcg^{-1}ngc^{-1}g^{-1} = n$.

(b) [3 pts] Let A, B be (not necessarily normal) subgroups of G. Recall that $AB = \{ab \mid a \in A, b \in B\}$. Prove that $C_G(AB) = C_G(A) \cap C_G(B)$.

Solution: First, let us prove that $C_G(AB) \subset C_G(A)$. Suppose $g \in C_G(AB)$. This means that for every $a \in A$ and $b \in B$, we have $gab = abg$. In particular, we can take $b = e$, which tells us that for every $a \in A$ $ga = ag$, so $g \in C_G(A)$, and we have proved the inclusion $C_G(AB) \subset C_G(A)$. In the same way one proves that $C_G(AB) \subset C_G(B)$, and therefore $C_G(AB) \subset C_G(A) \cap C_G(B)$. It remains to prove that $C_G(A) \cap C_G(B) \subset C_G(AB)$. Suppose $g \in C_G(A) \cap C_G(B)$. This means that for every $a \in A$ and $b \in B$, $ga = ag$ and $gb = bg$. But then $gab = agb = abg$, so $g \in C_G(AB)$.

3. Let $\mathrm{GL}_3(\mathbb{R})$ be the group of invertible 3×3 matrices. Define a function

$$f\colon \mathrm{GL}_3(\mathbb{R}) \to \mathrm{GL}_3(\mathbb{R})$$

by the following formula

$$f(A) = \frac{A}{\sqrt[3]{\det(A)}}.$$

(a) [2 pts] Is f a homomorphism?

Solution: Yes. Let's do the calculation

$$f(AB) = \frac{AB}{\sqrt[3]{\det(AB)}} = \frac{A}{\sqrt[3]{\det(A)}} \cdot \frac{B}{\sqrt[3]{\det(B)}} = f(A) \cdot f(B).$$

(b) [2 pts] Is f an injective function?

Solution: No. Suppose $A = \lambda I_3$, where I_3 is the 3×3 identity matrix, and λ is a scalar. Then $\det(A) = \lambda^3$, and $\frac{A}{\sqrt[3]{\det(A)}} = \frac{\lambda I_3}{\lambda} = I_3$. So matrices of the form λI_3 are in the kernel of f. Since f has a non-trivial kernel, it is not injective.
It is worth noting that the kernel of f consists precisely of matrices of the form λI_3. The group of such matrices is what we denote by Z_3 below. We have shown that *all* matrices of the form are in the kernel. I leave it to you to check that *only* matrices of this form are in the kernel.

(c) [2 pts] is f a surjective function?

Solution: No. Recall that if A is an $n \times n$ matrix, and k is a scalar, then $\det(kA) = k^n A$. We are considering 3×3-matrices. So for any matrix A,

$$\det(f(A)) = \det\left(\frac{A}{\sqrt[3]{\det(A)}}\right) = \frac{\det(A)}{\det(A)} = 1.$$

It follows that the image of f is contained in $\mathrm{SL}_3(\mathbb{R})$. On the other hand, for every $A \in \mathrm{SL}_3(\mathbb{R})$, $f(A) = A$, so the image of f is all of $\mathrm{SL}_3(\mathbb{R})$. In any case, f is not surjective.

Let Z_3 consist of matrices of the form $\begin{bmatrix} a & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & a \end{bmatrix}$, where $a \neq 0$. It is not difficult to check that Z_3 is a normal subgroup of $\mathrm{GL}_3(\mathbb{R})$. You can assume this without proof. Recall also that $\mathrm{SL}_3(\mathbb{R})$ is the group of 3×3 matrices of determinant 1.

(d) [2 pts] Prove that there is a group isomorphism

$$\mathrm{GL}_3(\mathbb{R})/Z_3 \cong \mathrm{SL}_3(\mathbb{R}).$$

Solution: By previous discussion, f can be considered as a surjective homomorphism $f\colon \mathrm{GL}_3(\mathbb{R}) \to \mathrm{SL}_3(\mathbb{R})$, whose kernel is exactly Z_3. The desired result follows by the first isomorphism theorem.

4. Let p, q be prime numbers satisfying $3 < p$, $p \equiv 2 (\mathrm{mod}\ 3)$, $q = 2p + 1$. For example, it could be that $p = 11$ and $q = 23$.

Let G be a group with $3pq$ elements.

(a) [1 pt] Prove that G has a normal q-Sylow subgroup.

Solution: We know that $n_q | 3p$. So n_q is one of $1, 3, p$, and $3p$. We want to prove that $n_q = 1$. We also know that $n_q \equiv 1 (\mathrm{mod}\ q)$. This excludes 3 and p, since $1 < 3, p < q$. We also know that $3p \equiv p - 1 (\mathrm{mod}\ q)$. Since $1 < p - 1 < 2p + 1 = q$, it follows that $3p \not\equiv 1 (\mathrm{mod}\ q)$. So $n_q = 1$.

(b) [4 pts] Prove that G has a normal 3-Sylow subgroup.

Solution: We know that n_3 can be one of $1, p, q$, and pq. By assumption, $p \equiv 2 (\text{mod } 3)$, and $q \equiv 2 \cdot 2 + 1 \equiv 2(\text{mod } 3)$. So n_3 can not be p or q. We also know that G has a normal q-Sylow subgroup C_q, so we can take the quotient of G by C_q, and we have the quotient homomorphism

$$q\colon G \to G/C_q.$$

The group G/C_q has $3p$ elements, where $p > 3$ and $p \not\equiv 1(\text{mod } 3)$. It follows that G/C_q has a normal 3-Sylow subgroup. Let H be the preimage of this 3-Sylow subgroup in G. Then H is a normal subgroup of G of order $3q$, where $q \not\equiv 1(\text{mod } 3)$. It follows that H has a normal 3-Sylow subgroup, and therefore G has a normal 3-Sylow subgroup.

5. Let $R = \{a + b\sqrt{7} \mid a, b \in \mathbb{Z}\}$. You can use without proof that R is a subring of the real numbers. Let

$$I = \{a + b\sqrt{7} \in R \mid a \text{ is divisible by } 7\}$$

(a) [2 pts] Prove that I is an ideal of R.

Solution: I leave you to check that I is an additive subgroup of R. Suppose $a+b\sqrt{7} \in I$ and $c + d\sqrt{7} \in R$ Then we have

$$(a + b\sqrt{7})(c + d\sqrt{7}) = ac + 7bd + (ad + bc)\sqrt{7}.$$

By assumption, a is divisible by 7, and therefore $ac + 7bd$ is divisible by 7. It follows that $(a + b\sqrt{7})(c + d\sqrt{7}) \in I$, and we have proved that I is an ideal.

(b) [2 pts] Prove that I is a *prime* ideal.

Solution: Suppose that $a + b\sqrt{7} \in R$ and $c + d\sqrt{7} \in R$, and $(a + b\sqrt{7})(c + d\sqrt{7}) \in I$. This means that $ac + 7bd + (ad + bc)\sqrt{7} \in I$. This in turn means that $ac + 7bd$ is divisible by 7, which in turn implies that ac is divisible by 7. Since 7 is a prime, it follows that either a or c is divisible by 7, which means that either $a + b\sqrt{7} \in I$ or $c + d\sqrt{7} \in I$.

(c) [2 pts] Describe the quotient ring R/I.

Answer: The quotient ring is isomorphic to $\mathbb{Z}/7$. Consider the homomorphism $f\colon R \to \mathbb{Z}/7$ defined by the formula $f(a+b\sqrt{7}) = a(\text{mod } 7)$. I leave you to check that f is a surjective ring homomorphism, with kernel exactly I. The result follows.

(d) [1 pt] Is I a maximal ideal?

Solution: Yes. We saw that the quotient R/I is isomorphic to $\mathbb{Z}/7$, which is a field. It follows that I is a maximal ideal.