MA 5020 - Abstract Algebra

Spring 2023 - final exam

- **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. Let G be a group, and $N \triangleleft G$ a normal subgroup. For each of the following statements, determine if it is true or false. Give a brief justification or a counterexample.

   (a) (2 points) If N and G/N are both abelian, then G is abelian.
   Solution: False. For example, the symmetric groups S_3 has a normal subgroup isomorphic to the cyclic group $\mathbb{Z}/3$ with quotient group $\mathbb{Z}/2$. Both the subgroup and the quotient are abelian, but S_3 is not abelian.

   (b) (2 points) If G is abelian then N and G/N are both abelian.
   Solution: True. (I leave the justification as an exercise).

2. Let G be a group and $H_1, H_2 \subset G$ two subgroups. Recall that H_1H_2 is the set of all products $\{h_1h_2 \in G \mid h_1 \in H_1, h_2 \in H_2\}$.

   (a) (3 points) Show an example where H_1H_2 is not a subgroup of G.
   Solution: Take the symmetric group S_3. Let $H_1 = \{e, (1,2)\}$ and $H_2 = \{e, (23)\}$. Then

   $$H_1H_2 = \{e, (12), (23), (1,2,3)\}.$$

   This is not a subgroup of S_3. For example,

   $$(2,3)(1,2,3) = (1,3) \notin H_1H_2.$$

   (b) (3 points) Prove that if $H_1H_2 \subseteq H_2H_1$ then in fact $H_1H_2 = H_2H_1$.
   Solution: Let $h_1 \in H_1, h_2 \in H_2$. We need to prove that $h_2h_1 \in H_1H_2$. We know that

   $$(h_2h_1)^{-1} = h_1^{-1}h_2^{-1} \in H_1H_2 \subseteq H_2H_1.$$

   It follows that there exist $g_1 \in H_1, g_2 \in H_2$ such that $h_1^{-1}h_2^{-1} = g_2g_1$. But then $h_2h_1 = g_1^{-1}g_2^{-1} \in H_1H_2$.

3. Suppose G is a group that acts transitively on the left on a set X. Recall that "transitively" means that for every two elements $x_1, x_2 \in X$ there exists a $g \in G$ such that $gx_1 = x_2$.

   (a) (3 points) Let $x_1, x_2 \in X$. Prove that the stabilizers of x_1 and x_2 are conjugate subgroups of G.
   Solution: Choose an element $g_0 \in G$ such that $g_0x_1 = x_2$. Let G_x denote the stabilizer of x. I claim that $G_{x_1} = g_0^{-1}G_{x_2}g_0$. To see this, suppose first that $g \in G_{x_2}$. Then $gx_2 = x_2$ and $g_0^{-1}gg_0x_1 = g_0^{-1}gx_2 = g_0^{-1}x_2 = x_1$. We have proved that $g_0^{-1}G_{x_2}g_0 \subseteq G_{x_1}$. Interchanging the roles of x_1 and x_2 one can prove in the same way that $g_0G_{x_1}g_0^{-1} \subseteq G_{x_2}$, which means that $G_{x_1} \subseteq g_0^{-1}G_{x_2}g_0$. Thus $G_{x_1} = g_0^{-1}G_{x_2}g_0$.

(b) (2 points) Suppose in addition that G is finite. Prove that there exists an element $g \in G$ that satisfies $gx \neq x$ for all $x \in X$ (in other words, prove that there exists an element of G that does not fix any element of X).

Solution: The statement is equivalent to proving that

$$\bigcup_{x \in X} G_x \subsetneq G.$$

Let $|S|$ denote the number of elements in a set S. Since G is finite, it is enough to prove that

$$\left| \bigcup_{x \in X} G_x \right| < |G|.$$

We know that the groups G_x are not pairwise disjoint, because they have at least the identity element in common. It follows that

$$\left| \bigcup_{x \in X} G_x \right| < \sum_{x \in X} |G_x|.$$

Therefore it is enough to prove that

$$\sum_{x \in X} |G_x| \leq |G|.$$

By part (a) the stabilizer groups G_x are conjugate to each other. By the orbit-stabilizer theorem for any choice of $x_0 \in X$, $|X| = [G : G_{x_0}]$. It follows that

$$\sum_{x \in X} |G_x| = |X| \cdot |G_{x_0}| = [G : G_{x_0}]|G_{x_0}| = |G|.$$

4. (a) (2 points) Prove that a group of order 56 can not be simple.

Solution: $56 = 8 \cdot 7$. By Sylow theorem n_7 is either 1 or 8. If $n_7 = 1$ then the group has a normal 7-Sylow subgroup, and is not simple. Suppose $n_7 = 8$. Then the group has $6 \cdot 8 = 48$ elements of order 7, and exactly 8 elements of order different from 7. It follows that there are enough elements for exactly one 2-Sylow subgroup of order 8. So in this case the group has a normal 2-Sylow subgroup. In any case, a group with 56 elements can not be simple.

(b) (3 points) Prove that a group of order 72 can not be simple.

Solution: Suppose G is a group with 72 elements. $72 = 8 \cdot 9$. By Sylow theorem, $n_3 = 1$ or 4. If $n_3 = 1$ then G is not simple and we are done. Suppose $n_3 = 4$. Then G has four 3-Sylow subgroups. The action of G on the set of 3-Sylow subgroups by conjugation induces a non-trivial homomorphism $G \to S_4$. Since S_4 has 24 elements, this homomorphism can not be injective. Thus the kernel of this homomorphism is a proper, non-trivial subgroup of G, and G is not simple.

5. (a) (2 points) Let R be a ring, and I, J ideals of R. Suppose that $I \cap J$ is a prime ideal of R. Prove that either $I \subseteq J$ or $J \subseteq I$.

Solution: Suppose, by contradiction, that neither of the ideals I and J contains the other. We will prove that in this case $I \cap J$ is not a prime ideal.

There exist elements $x \in I \setminus J$ and $y \in J \setminus I$. Then $xy \in I$ because $x \in I$ and $xy \in J$ because $y \in J$. Thus $xy \in I \cap J$. But $x \notin I \cap J$ and $y \notin I \cap J$, so $I \cap J$ is not a prime ideal.

(b) (3 points) Let R be a ring that satisfies $x^2 = x$ for all $x \in R$. Prove that R is commutative.

Solution: First, we prove that for every $x \in R$, $x + x = 0$. Indeed, by assumption $(x+x)^2 = x + x$. Multiplying out and using the distributivity law we find that

$$x^2 + x^2 + x^2 + x^2 = x + x.$$

By assumption $x^2 = x$, so $x + x + x + x = x + x$, and therefore $x + x = 0$. This means that $x = -x$ for all $x \in R$.

Next, let us use that for any $x, y \in R$, $(x+y)(x+y) = x + y$. Multiplying out once again we find that

$$x^2 + xy + yx + y^2 = x + y.$$

Since $x^2 = x$ and $y^2 = y$, this equality simplifies to $xy + yx = 0$. But $yx = -yx$, so $xy = yx$, for all $x, y \in R$.

6. Let $\mathbb{F}$ be a field, and $\mathbb{F}[x]$ the ring of polynomials over $\mathbb{F}$. In this question you will consider the ideals (x^2+1) and (x^2-1) in $\mathbb{F}[x]$, and the quotient rings $\mathbb{F}[x]/(x^2+1)$ and $\mathbb{F}[x](x^2-1)$. Be sure to justify your answers.

(a) (2 points) Suppose $\mathbb{F} = \mathbb{C}$ is the field of complex numbers. Are the rings $\mathbb{C}[x]/(x^2+1)$ and $\mathbb{C}[x]/(x^2-1)$ isomorphic?

Solution: Yes, because over $\mathbb{C}$ we have $x^2 - 1 = (x-1)(x+1)$ and $x^2+1 = (x-i)(x+i)$. Recall that for any constant a, there is an isomorphism of rings $\mathbb{C}[x]/(x-a) \xrightarrow{\cong} \mathbb{C}$. Using the Chinese Remainder Theorem, we obtain isomorphisms of rings

$$\mathbb{C}[x]/(x^2-1) \cong \mathbb{C}[x]/(x-1) \times \mathbb{C}[x]/(x+1) \cong \mathbb{C} \times \mathbb{C},$$

$$\mathbb{C}[x]/(x^2+1) \cong \mathbb{C}[x]/(x-i) \times \mathbb{C}[x]/(x+i) \cong \mathbb{C} \times \mathbb{C}.$$

The right hand sides are the same, so the left hand sides are isomorphic.

(b) (3 points) Suppose $\mathbb{F} = \mathbb{F}_3$ is the field with three elements. Are the rings $\mathbb{F}_3[x]/(x^2+1)$ and $\mathbb{F}_3/(x^2-1)$ isomorphic?

Solution: No. The polynomial x^2+1 does not have a root over $\mathbb{F}_3$. Since it is a quadratic polynomial, it follows that it is irreducible over $\mathbb{F}_3$. It follows that $\mathbb{F}_3[x]/(x^2+1)$ is an integral domain (a field even). On the other hand the polynomial $x^2 - 1 = (x-1)(x+1)$ is reducible, and thus $\mathbb{F}_3/(x^2-1)$ is not an integral domain. It follows that the two rings are not isomorphic.