Department of mathematics,
Stockholm University
Examinator: Gregory Arone

MA 5020 - Abstract Algebra
Final Exam

Nov 30, 2021

Instructions: Textbooks, notes and calculators are not allowed. You may quote results that you learned during the class. When you do, state precisely the result that you are using. Unless explicitly instructed otherwise, 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. For each of the following statements, determine if it is (always) true or (sometimes) false. Justify your answers either by a brief and clear argument or by a counterexample.

   (a) [2 pts] Suppose G is a group, with subgroups G_1, G_2 and H. If $H \subset G_1 \cup G_2$ then either $H \subset G_1$ or $H \subset G_2$.

   Solution: True. Suppose, by contradiction, that $H \subset G_1 \cup G_2$, but H is not a subgroup of either G_1 or G_2. Then H has elements h_1 and h_2 such that h_1 is in G_1 but is not in G_2, while h_2 is in G_2 but is not in G_1. But then h_1h_2 can not be either in G_1 or in G_2 (why?), but $h_1h_2 \in H$, so we obtain a contradiction to the assumption $H \subset G_1 \cup G_2$.

   (b) [2 pts] Let G_1, G_2 be groups. For every subgroup $K \subset G_1 \times G_2$, there exist subgroups $H_1 \subset G_1$ and $H_2 \subset G_2$ such that $K = H_1 \times H_2$.

   Solution: False. For example, the diagonal subgroup of $G \times G$ consisting of pairs (x, x), where x is any element of G is not of this form, for any non-trivial group G. Indeed, for any subgroup of $G \times G$ of the form $H_1 \times H_2$, if $(x, y) \in H_1 \times H_2$ then $(x, e) \in H_1 \times H_2$. But this is not the case for the diagonal subgroup.

   (c) [2 pts] Let R, S be commutative rings with unit. For every ideal I of $R \times S$, there exists ideals I_1 of R and I_2 of S such that $I = I_1 \times I_2$.

   Solution: True. Suppose I is an ideal of $R \times S$. Then for every element $(x, y) \in I$, the element $(x, 0) = (x, y) \cdot (1, 0)$ is an element of I, and similarly $(0, y) \in I$. Let $I_1 = \{x \in R \mid (x, y) \in I \text{ for some } y \in S\}$. Similarly, let $I_2 = \{y \in S \mid (x, y) \in I \text{ for some } x \in R\}$. It is easy to see that I_1 is an ideal of R, I_2 is an ideal of S, and $I_1 \times I_2 = I$.

2. Let S_{10} be the group of permutations of a set with 10 elements.

   (a) [2 pts] Does S_{10} have a cyclic subgroup of order 30?

   Solution: Yes. The permutation $(1, 2)(3, 4, 5)(6, 7, 8, 9, 10)$ has order 30, so it generates a cyclic subgroup of order 30.

   (b) [2 pts] How many elements are there in S_{10} that commute with $(12)(34)(567)$?

   Solution: The full cycle structure of this permutation, where we include the singleton cycles, is $(1, 2)(3, 4)(5, 6, 7)(8)(9)(10)$. It follows that the centralizer of this permutation has $2! \cdot 2^2 \cdot 3 \cdot 3! = 144$ elements.

3. (a) [3 pts] Let G be a finite group, and H a proper subgroup of G. Prove that there exists an element $g \in G$ that is not conjugate to any element of H.

   Soluiton: The set of elements of G that are conjugate to some element of H is the union of conjugates of H. The number of distinct conjugates of H is $[G : N_G(H)]$, where $N_G(H)$ is the normalizer of H. Each conjugate of H has as many elements as H, and the conjugates are not disjoint, since the identity element belongs to all the conjugates of H. It follows that the union of conjugates of H has strictly fewer elements that $[G : N_G(H)] \cdot |H|$. Since $H \subset N_G(H)$, it follows that $[G : N_G(H)] \leq [G : H]$. So the union of conjugates of H has strictly fewer elements that $[G : H] \cdot |H| = |G|$. It follows that there exists an element of G that is not conjugate to any element of H.

(b) [3 pts] Suppose that G is a finite group acting transitively on a set X[1]. Prove that there exists an element $g \in G$ such that $gx \neq x$ for all $x \in X$.

Solution: Let $G_x \subset G$ denote the stabilizer of x in G. Let $y \in X$ be another element. Since the action of G is transitive, there exists an element $g \in G$ such that $y = gx$. Then $G_y = gG_xg^{-1}$. It follows that for all $y \in X$, the stabilizer G_y is conjugate to G_x in G. By part (a) there exists an element $g \in G$ such that $g \notin G_y$ for all $y \in X$. It follows that $gx \neq x$ for all $x \in X$.

(c) [2 pts] (optional bonus problem!) Show that Part (a) may not hold if G is an infinite group.

Solution: Let $S_\infty = \cup_{n=1}^{\infty} S_n$ be the infinite symmetric group. S_∞ consists of bijections $f : \mathbb{N} \to \mathbb{N}$, with the property that $f(n) = n$ for n large enough. Let $H \subset S_\infty$ be the stabilizer of 1. I claim that every element of S_∞ is conjugate to some element of H. Indeed let $f \in S_\infty$. Choose an n_0 such that $f(n) = n$ for all $n \geq n_0$. Let $\tau \in S_\infty$ be the cycle $(1, 2, \ldots, n_0)$. Then $\tau f \tau^{-1}(1) = \tau(f(n_0)) = \tau(n_0) = 1$. So $\tau f \tau^{-1} \in H$, and thus $f \in \tau^{-1} H \tau$.

4. [4 pts] Prove that a group of order 56 has a normal p-Sylow subgroup for some prime p.

Solution: By Sylow theorem, n_7 can be either 1 or 8. If $n_7 = 1$, the group has a normal seven-Sylow subgroup. Suppose $n_7 = 8$. Then the group has $6 \cdot 8 = 48$ elements of order 7. If $n_2 > 1$, then our group has at least $8 + 8 - 4 = 12$ additional elements that are not of order 7. But then the group has at least 60 elements, contradicting the assumptions. We conclude that if $n_7 > 1$ then $n_2 = 1$, so there exists at least one normal p-Sylow subgroup.

5. [5 pts] Let R be a commutative ring with a unit element $1 \neq 0$. Suppose that $R[x]$ is a principal ideal domain (I.e., an integral domain, where every ideal is principal). Prove that R is a field.

Solution 1: Since R is a subring of $R[x]$, and $R[x]$ is an integral domain, it follows that R is an integral domain. We know that there is an isomorphism$R \cong R[x]/(x)$. So it is enough to prove that (x) is a maximal ideal of $R[x]$. Suppose that there exists an ideal $(x) \subset J \subset R[x]$. Since $R[x]$ is a PID, we can write $J = (p(x))$ for some polynomial $p(x) \in R[x]$. But then $p(x)|x$. It follows that $p(x) = a + bx$ for some $a, b \in R$, and there exists some $c, d \in R$ such that $(a + bx)(c + dx) = x$. It follows that $ac = 0$, $bd = 0$ and $ad + bc = 1$. It follows easily that either $a = 0$ and b is a unit, in which case $J = (x)$, or a is a unit and $b = 0$, in which case $J = R$. We have proved that (x) is a maximal ideal.

Solution 2: Since R is a subring of $R[x]$, and $R[x]$ is an integral domain, it follows that R is an integral domain. It is enough to prove that the only ideals of R are (0) and R. Let I be an ideal of R. Let us suppose that I has a non-zero element α, and we will prove that $I = R$. Consider the ideal $I + (x)$ of $R[x]$ consisting of polynomials $a_0 + a_1x + \cdots + a_nx^n$, such that $a_0 \in I$. Since $R[x]$ is

[1] Recall that an action is transitive if for every $x, y \in X$ there exists a $g \in G$ such that $y = gx$

a principal ideal domain, $I + (x)$ is generated by some polynomial $p(x)$. We claim that $p(x)$ must have degree zero. Indeed, the constant polynomial α is in $I + (x)$, so $p(x)|\alpha$, which is only possible if $p(x)$ is a constant polynomial. So $I + (x) = (\omega)$ for some $\omega \in I$. But then $\omega | x$, which is possible only of ω is a unit. So I contains a unit, and thus $I = R$.

6. In this question, all coefficients are taken to be in $\mathbb{Z}/5$. Let $a \in \mathbb{Z}/5$. Consider the polynomial, depending on a, $p(x) = x^2 + ax + 1$. As usual, let (p) be the ideal of $\mathbb{Z}/5[x]$ generated by $p(x)$.

   (a) [2 pts] How many elements are there in the quotient ring $\mathbb{Z}/5[x]/(p)$? If the answer depends on a, show explicitly how it depends. If it does not depend, explain why.

   Solution: The quotient ring always has 25 elements.

   (b) [2 pts] For which values of a, is the polynomial $p(x) = x^2 + ax + 1$ irreducible?

   Solution: If $p(x)$ is reducible then there exist $s, t \in \mathbb{Z}/5$ such that

$$x^2 + ax + 1 = (x + s)(x + t).$$

   It follows that $st = 1$ and $s + t = a$. Equivalently $s + s^{-1} = a$. In $\mathbb{Z}/5$ one easily checks that

$$1 + 1^{-1} = 2, \quad 2 + 2^{-1} = 2 + 3 = 0, \quad 3 + 3^{-1} = 3 + 2 = 0, \quad 4 + 4^{-1} = 4 + 4 = 3.$$

   It follows that the polynomial is reducible if $a = 0, 2,$ or 3, and thus it is irreducible if $a = \pm 1$.

   (c) [1 pt] For which values of a, is the quotient ring $\mathbb{Z}/5[x]/(p)$ a field?

   Solution: The quotient is a field if and only if p is irreducible, which is if and only if $a = \pm 1$.