Department of mathematics,
Stockholm University
Examinator: Gregory Arone

MA 5020 - Abstract Algebra
Final Exam

Oct 26, 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. (a) [2 pts] True or false: if a permutation σ has order 2 then it is an odd permutation. Prove or give a counterexample.

   Solution: False. For example, the permutation $(12)(34)$ has order 2, but it is an even permutation.

   (b) [2 pts] How many permutations $\sigma \in S_8$ are there, that satisfy $\sigma(1234)(567)\sigma^{-1} = (3572)(486)$? Note: you are not required to list them, just to say how many there are, with a brief and clear justification.

   Solution: 12. Any two such permutations differ by an element of the centralizer of $(1234)(567)$, so there are as many such permutations as there are elements in the centralizer. The centralizer is isomorphic to $C_4 \times C_3$ and has 12 elements.

2. Let G be a group, and $H \subset G$ a subgroup. Define the *core* of H as follows

$$\mathrm{Core}_G(H) = \bigcap_{g \in G} gHg^{-1}.$$

   (a) [1 pt] True or false: $\mathrm{Core}_G(H)$ is a normal subgroup of G. No justification required.

   Solution: True.

   (b) [2 pts] Describe the core of a 2-Sylow subgroup of S_4.

   Solution: The core is the group consisting of the following 4 elements:

$$V_4 = \{e, (12)(34), (13)(24), (14)(23)\}.$$

   We learned in class that V_4 is a normal subgroup of S_4. It is obviously contained in at least one 2-Sylow subgroup, therefore it is contained in their intersection. Since the 2-Sylow subgroup of S_4 is not normal, the intersection of the 2-Sylow subgroups is a proper subgroup of each 2-Sylow subgroup. The subgroup V_4 has index 2 in the Sylow subgroups, so it is a maximal proper subgroup of the Sylow subgroups, therefore it must be the entire intersection.

   (c) [2 pts] Suppose that H has index n in G. Prove that the quotient group $G/\mathrm{Core}_G(H)$ is isomorphic to a subgroup of S_n.

   Solution: The action of G on G/H induces a homomorphism $G \to S_n$. The core of H is precisely the kernel of this homomorphism. It follows that this homomorphism induces an injective homomorphism $G/\mathrm{Core}_G(H) \hookrightarrow S_n$.

3. (a) [2 pts] Let P and Q be two Sylow subgroups of G, for distinct primes p and q. Suppose that $n_p = n_q = 1$ (where n_p denotes, as usual, the number of p-Sylow subgroups of G). Prove that for every $x \in P$ and $y \in Q$, $xy = yx$.

Solution: Consider the commutator $xyx^{-1}y^{-1}$. On one hand, it can be written as $(xyx^{-1})y^{-1}$. Since $n_q = 1$, Q is normal, which means that $xyx^{-1} \in Q$, and therefore $(xyx^{-1})y^{-1} \in Q$. A similar argument shows that $xyx^{-1}y^{-1} \in P$. So $xyx^{-1}y^{-1} \in P \cap Q$. But $P \cap Q = \{e\}$, so $xyx^{-1}y^{-1} = e$, which means that $xy = yx$.

(b) [2 pts] Suppose G has $p^m q^n$ elements, where p and q are distinct primes. Let P and Q be a p-Sylow and q-Sylow subgroup of G. Suppose that P is contained in the center of G. Prove that G is isomorphic to $P \times Q$.

Solution: The assumption clearly implies that P is normal in G. We claim that Q is normal too. Since $P \cap Q = \{e\}$, PQ has as many elements as G, and therefore $G = PQ$. This means that every element of G can be written as pq for some $p \in P$ and $q \in Q$. This means that for every element $pq \in G$ and every $x \in Q$,

$$(pq)x(pq)^{-1} = pqxq^{-1}p^{-1} = qxq^{-1} \in Q$$

Which means that Q is normal in G.

Now we just need the standard fact that if all the Sylow subgroups of a group are normal, then the group is isomorphic to the product of its Sylow subgroups. In our case we can prove it by considering the canonical homomorphism

$$G \to G/Q \times G/P.$$

The kernel of this homomorphism is $Q \cap P = \{e\}$. So this homomorphism is injective. Counting elements tells us that it is an isomorphism.

Finally, consider the composite homomorphism

$$P \times Q \to G \times G \to G/Q \times G/P.$$

Again, the kernel of this homomorphism is $(P \cap Q) \times (Q \cap P)$, which is trivial. So the homomorphism is injective, and counting elements tells us that it is an isomorphism. So $G \cong P \times Q$.

4. [5 pts] Prove that a group of order $132 = 3 \cdot 4 \cdot 11$ is not simple.

Solution: Suppose G is a group with 132 elements. By Sylow theorems, $n_{11} = 1$ or 12. If $n_{11} = 1$ then G has a normal 11-Sylow subgroup and is not simple. Suppose $n_{11} = 12$. Then G has 120 elements of order 11.

Next, let us analyze n_3. We know that $n_3 | 44$, which implies that $n_3 \in \{1, 2, 4, 11, 22, 44\}$. We also know that $n_3 \equiv 1 (\text{mod } 3)$, which leaves the possibilities that $n_3 = 1, 4$, or 22. 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. So $n_3 \neq 22$. If $n_3 = 1$ then G has a normal 3-Sylow subgroup and is not simple. The remaining possibility is that $n_3 = 4$. In this case G has 8 elements of order 3, so altogether it must have 128 elements whose order is either 11 or 3.

If $n_2 > 1$ then G has at least 6 elements whose order is a power of 2 (this includes the identity element), so altogether G has at least 134 elements, which is a contradiction. So $n_2 = 1$, and G is not simple.

5. Let R, S be integral domains (i.e., commutative rings with a $1 \neq 0$, and no zero divisors). Let $f\colon R \to S$ be a ring homomorphism. You may use without proof the fact that if I is an ideal of S, then $f^{-1}(I)$ is an ideal of R.

   (a) [2 pts] Show that either $f(1) = 1$, or $f(r) = 0$ for all $r \in R$.

   Solution: We know that $f(1) = f(1^2) = f(1)^2$. This means that $f(1)(f(1) - 1) = 0$ Since R is an integral domain, either $f(1) = 0$ or $f(1) = 1$. So if $f(1) \neq 1$ then for all $r \in R$, $f(r) = f(r \cdot 1) = f(r) \cdot f(1) = 0$.

   Assume that $f(1) = 1$ in parts (b)-(d) below.

   (b) [2 pts] Suppose I is a principal ideal of S. Does it follow that $f^{-1}(I)$ is a principal ideal of R? Prove or give a counterexample.

   Solution: No. For example, consider the homomorphism $\mathbb{Z}[x] \to \mathbb{Z}$ that sends a polynomial to its constant coefficient. The idean $2\mathbb{Z} \in \mathbb{Z}$ is prinicpal, but its preimage is the ideal $(2, x)$, which is not principal.

   (c) [2 pts] Suppose I is a prime ideal of S. Does it follow that $f^{-1}(I)$ is a prime ideal of R? Prove or give a counterexample.

   Solution: Yes. Suppose $xy \in f^{-1}(I)$. Then $f(xy) \in I$, which means that $f(x)f(y) \in I$. Since I is a prime ideal, either $f(x)$ or $f(y)$ is an element of I. But then either x or y is an element of $f^{-1}(I)$.

   Furthermore, if one requires prime ideals to be proper, it also holds that if I is proper, then $1_S \notin I$. Since f is not zero, $f(1_R) = 1_S$, so $1_R \notin f^{-1}(I)$, and $f^{-1}(I)$ is a proper ideal.

   (d) [2 pts] Suppose that I is a maximal ideal of S. Does it follow that $f^{-1}(I)$ is a maximal ideal of R? Prove or give a counterexample.

   Solution: No. Consider the inclusion homomorphism $\mathbb{Z} \hookrightarrow \mathbb{Q}$. The zero ideal is maximal in $\mathbb{Q}$, but its preimage is not maximal in $\mathbb{Z}$.

   Note: if one assumes that f is surjective then the answer is yes.

6. [4 pts] Let $p(x) = x^3 + ax^2 + bx + 1$, where $a, b \in \mathbb{Z}$. Let (p) be the ideal generated by p in $\mathbb{Q}[x]$. Prove that one, and only one, of the following possibilities must hold

   1. $\mathbb{Q}[x]/(p)$ is a field
   2. $a = b$ or $a + b = -2$.

   Solution: We know that one and only one of the following holds: (a) p is irreducible in $\mathbb{Q}[x]$, (b) p is reducible in $\mathbb{Q}[x]$. The ring $\mathbb{Q}[x]/(p)$ is a field if and only if p is irreducible. So we have to prove that p is reducible if and only if $a = b$ or $a + b = -2$.

   By Gauss's lemma and its consequences, since p is a monic polynomial with integer coefficients, p is reducible over $\mathbb{Q}$ if and only if it is reducible over $\mathbb{Z}$. p is reducible over $\mathbb{Z}$ if and only if it equals the product of a linear monic polynomial and a quadratic monic polynomial with integer coefficients. In other words, if and only if there exist integers s, t, r such that

$$x^3 + ax^2 + bx + 1 = (x^2 + rx + s)(x + t).$$

This holds if and only if we have equalities

$$\begin{aligned} a &= r + s \\ b &= rt + s \\ 1 &= st. \end{aligned}$$

Since r, s, and t are integers, the equality $st = 1$ implies that either $s = t = 1$ or $s = t = -1$. In the first case $a = b = r + 1$, in the second case $a = r - 1$ and $b = -r - 1$.

To summarize, we have shown that p is reducible over $\mathbb{Q}$ if and only if either there exists an integer r such that $a = b = r + 1$ or there exists an integer r such that $a = r - 1$ and $b = -r - 1$. Clearly the last condition is equivalent to $a = b$ or $a + b = -2$.