Department of mathematics,
Stockholm University
Examinator: Gregory Arone

MA 5020 - Abstract Algebra
Final Exam

Oct 27, 2020

Instructions: Textbooks, notes and calculators are 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

---

1. (a) [2 pts] Suppose G is a finite group, and m, n are positive integers, where m divides n. Furthermore, suppose G has an element of order n. Prove that G has an element of order m.

   Solution: Let $k = \frac{n}{m}$. Since m divides n, k is a positive integer. Let g be an element of order n. We claim that g^k has order m. Indeed, $(g^k)^m = g^n = e$. Suppose $0 < m' < m$ is a smaller integer for which $(g^k)^{m'} = e$. Then $g^{km'} = e$ and $0 < km' < n$, contradicting that n is the order of g. So m is the smallest positive integer satisfying $(g^k)^m = e$.

   (b) [2 pts] Suppose $f\colon G \to H$ is a surjective homomorphism between finite groups. Suppose H has an element of order n. Prove that G has an element of order n.

   Solution: Let $h \in H$ be an element of order n. Since f is surjective, there exists an element $g \in G$ satisfying $f(g) = h$. It follows that $f(g^n) = h^n = e$, so $g^n \in \ker(f)$. Since $\ker(f)$ is a finite group, g^n has a finite order, let's say k. Then $g^{nk} = e$. We claim that nk is the order of g. Indeed, suppose that $0 < m < nk$ is an integer satisfying $g^m = e$. Using division with remainder, write $m = qn + r$ with $0 \leq r < n$. If $r = 0$ then $m = qn$, with $0 < q < k$ and $g^m = (g^n)^q = e$, contradicting that k is the order of g^n. Supposing $0 < r < n$ we have the following equality of elements of H:

   $$e = f(g^m) = f(g^{qn+r}) = h^{qn+r} = h^r.$$

   This contradicts the assumption that n is the order of h.
   We now know that G has an element g of order nk. By previous part, g^k has order n.

   (c) [1 pt] Suppose $f\colon G \to H$ is a surjective homomorphism between finite groups. Suppose G has an element of order n. Does it follow that H has an element of order n? Prove or give a counterexample.

   Solution: No. For example there is a surjective homomorphism $\mathbb{Z}/4 \twoheadrightarrow \mathbb{Z}/2$. The group $\mathbb{Z}/4$ has an element of order 4, but the group $\mathbb{Z}/2$ does not.

2. [5 pts] Suppose G is a simple group of order 168. How many elements of order 7 does G have?

   Solution: The primary decomposition of 168 is $2^3 \cdot 3 \cdot 7$. It follows that the 7-Sylow subgroup of G is $\mathbb{Z}/7$, and the intersecion of any two 7-Sylow subgroups consists of just the identity element. Each 7-Sylow subgroup contains 6 elements of order 7, and those sets are disjoint.

   Next, let us analyze the possible values of n_7. We know that $n_7 \equiv 1 \pmod 7$ and $n_7 | 24$. It follows that $n_7 = 1$ or 8. Since G is simple, n_7 can not be 1, so $n_7 = 8$. It follows that G has $8 \cdot 6 = 48$ elements of order 7.

3. (a) [3 pts] Let G be a finite group and $N \triangleleft G$ a normal subgroup. Suppose G acts on a set X in such a way that the induced action of N on X is *transitive*. This means that for any two elements $x, y \in X$, there exists an element $n \in N$ such that $nx = y$.

   Let $x \in X$ and let G_x be the stabilizer of x. Prove that $G = G_x N$.

   Solution: Let $g \in G$. We want to show that there exist elements $g_x \in G_x$ and $n \in N$ such that $g = g_x n$. Consider the element gx of X. Since N acts transitively on X, there exists an element $n_1 \in N$ such that $gx = n_1 x$. This implies that $x = n_1^{-1} gx$, so $n_1^{-1} g \in G_x$. Let $g_x = n_1^{-1} g$. Since N is normal, there exists an $n \in N$ such that $n_1^{-1} g = g n^{-1}$. So we have the equality $g_x = g n^{-1}$ and $g = g_x n$.

   (b) [2 pts] Let G be a finite group. Suppose $N \triangleleft G$ is a normal subgroup, $P \subset N$ is a Sylow subgroup of N and $N_G(P)$ is the normalizer of P in G.

   Prove that $G = N_G(P)N$.

   Solution: Consider the set of conjugates of P in G. Since N is a normal subgroup of G and $P \subseteq N$, all the G-conjugates of P are contained in N. Since P is a Sylow subgroup of N, a subgroup of N that is G-conjugate to P is also N-conjugate to P. This means that the transitive action of G on the set of G-conjugates of P restricts to a transitive action of N on this set. On the other hand, the stabilizer of P under the action of G is precisely $N_G(P)$. By part (a), $G = N_G(P)N$.

4. (a) [3 pts] Let G be a group. Suppose G has a normal subgroup N of index 4, such that the quotient group G/N is not cyclic.

   Prove that G has three distinct normal subgroups of index 2, say we call them A, B, and C, such that $G = A \cup B \cup C$.

   Solution: G/N is a non-cyclic group of order 4, so $G/N \cong \mathbb{Z}/2 \times \mathbb{Z}/2$. So we have a surjective homomorphism

   $$f : G \twoheadrightarrow \mathbb{Z}/2 \times \mathbb{Z}/2.$$

   Recall that $\mathbb{Z}/2 \times \mathbb{Z}/2$ consists of pairs $(0,0), (1,0), (0,1), (1,1)$, and the group operation is coordinate-wise addtion mod 2. Let

   $$A_1 = \{(0,0), (1,0)\}, B_1 = \{(0,0), (0,1)\}, \text{ and } C_1 = \{(0,0), (1,1)\}.$$

   It is easy to see that A_1, B_1, C_1 are (automatically normal) subgroups of $\mathbb{Z}/2 \times \mathbb{Z}/2$, and furthermore as sets

   $$\mathbb{Z}/2 \times \mathbb{Z}/2 = A_1 \cup B_1 \cup C_1.$$

   (You can think of A_1 as the group of elements where the second coordinate is zero, B_1 as the group of elements where the first coordinate is zero, and C_1 as the group of elements where the two coordinates are equal.)
   Let $A = f^{-1}(A_1)$, $B = f^{-1}(B_1)$, and $C = f^{-1}(C_1)$. These are the required subgroups.

(b) [2 pts] Show that the group $S_3 \times S_3$ has a normal subgroup of index 4 such that the quotient group is not cyclic. Describe explicitly the three normal subgroups of part (a) in this case.

Solution: The group S_3 has a normal subgroup of index 2, which we can call $\mathbb{Z}/3$ or A_3. I will think of it as the alternating subgroup A_3. It follows that $S_3 \times S_3$ has a normal subgroup $A_3 \times A_3$ of index 4, and the quotient group is $\mathbb{Z}/2 \times \mathbb{Z}/2$.

The group of $S_3 \times S_3$ consists of ordered pairs of permutations (σ, τ) of $\{1, 2, 3\}$. The three subgroups A, B, C are:

1. The subgroup of pairs (σ, τ) where τ is an even permutation.
2. The subgroup of pairs (σ, τ) where σ is an even permutation.
3. The subgroup of pairs (σ, τ) where σ and τ are either both even or both odd.

5. Let R, S be not necessarily commutative rings with identity.

(a) [2 pts] Suppose R is a division ring. Prove that the only (left, right or two-sided) ideals of R are $\{0\}$ and R

Solution: Suppose I is a left ideal of R, and $I \neq \{0\}$. Then I has a non-zero element $0 \neq x \in I$. Since R is a division ring, for every element $r \in R$, there exists and element $y \in R$ such that $r = yx$. It follows that for every $r \in R$, $r = yx$ is an element of I. In other words, if $I \neq \{0\}$ then $I = R$. This proves the claim for left ideals. The proof for right and two-sided ideals is essentially the same.

(b) [1 pt] Suppose that elements $a, b \in R$ satisfy $aba = 1$. Prove that $ab = ba$ and a is a unit.

Solution: By associativity $ab = (ab)(aba) = (aba)(ba) = ba$. Since $aba = 1$, the element $ab = ba$ is a two-sided inverse of a, so a is a unit.

(c) [1 pt] Let $f\colon R \to S$ be a ring homomorphism. Show that if $f(1) \neq 1$ then $f(1)$ is a zero divisor, or zero.

Solution: We know that $f(1) = f(1^2) = f(1)^2$. So $f(1)^2 - f(1) = f(1)(f(1) - 1) = 0$. It follows immediately that $f(1)$ is either a zero-divisor or zero.

(d) [1 pt] Show that there is a non-zero ring homomorphism $f\colon \mathbb{Z}/3 \to \mathbb{Z}/6$.

Solution: There are two non-zero group homomorphisms from $\mathbb{Z}/3$ to $\mathbb{Z}/6$, namely $f(x) = 2x$ and $f(x) = 4x$. Of these two, the second one is a ring homomorphism, because $4^2 \equiv 4 \pmod 6$. So

$$f(xy) = 4xy = 16xy = f(x)f(y).$$

6. Let $\mathbb{Z}[i]$ be the ring of Gaussian integers.

(a) [2 pts] Use Euclid's algorithm to find a greatest common divisor of $9 + 3i$ and 5 with the property that its real part and complex part are positive.

Solution: We know that $\frac{9+3i}{5} = \frac{9}{5} + \frac{3}{5}i$. The nearest integer approximation to the quotient is $2 + i$. We obtain the first step of the algorithm

$$9 + 3i = (2 + i) \cdot 5 + (-1 - 2i).$$

For the second step we calculate

$$\frac{5}{-1 - 2i} = \frac{-5 + 10i}{5} = -1 + 2i.$$

We find that the ratio is a Gaussian integer, so the algorithm stops here. The greatest common divisor is $-1 - 2i$. To get a representative with positive real and imaginary part we multiply by -1 and get the answer $1 + 2i$.

(b) [1 pt] Let $\gcd(9 + 3i, 5)$ be the answer that you found in part (a). Find $a, b \in \mathbb{Z}[i]$ such that $a(9 + 3i) + 5b = \gcd(9 + 3i, 5)$.

Solution: By reading the Euclid's algorithm backward we find easily that

$$1 + 2i = (-1) \cdot (9 + 3i) + (2 + i) \cdot 5.$$

So $a = -1$ and $b = 2 + i$ will work.

(c) [2 pts] Prove that there is an isomorphism of rings

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

Solution: There is a ring homomorphism $f\colon \mathbb{Z}[x] \to \mathbb{Z}[i]$ defined by the formula $f(p) = p(i)$, where p is an arbitrary polynomial. Clearly f is surjective, because for any $a + bi \in \mathbb{Z}[i]$, $a + bi = f(a + bx)$. It remains to prove that $\ker(f) = (x^2 + 1)$. Clearly $f(x^2 + 1) = 0$, so $(x^2 + 1) \subseteq \ker(f)$. Let $p(x) \in \ker(f)$. We need to prove that $p(x) \in (x^2 + 1)$, i.e., that $p(x)$ is a multiple of $x^2 + 1$ by a polynomial with integer coefficients.

By division of polynomials we have an equality

$$p(x) = q(x)(x^2 + 1) + r$$

where $q(x)$ is apriori a polynomial with rational coefficients and r is a constant. Since $p(i) = r$ and $p \in \ker(f)$, we obtain that $r = 0$. So $p(x) = q(x)(x^2 + 1)$. Since $x^2 + 1$ is a monic polynomial, division of $p(x)$ by $x^2 + 1$ yields a polynomial with integer coefficients. It follows that $q(x)$ is a polynomial with integer coefficients, and we are done.