KTH Teknikvetenskap

SF2729 Groups and Rings
Exam
Monday, March 16, 2015

Time: 08:00-13:00
Allowed aids: none
Examiner: Wojciech Chachólski

Present your solutions to the problems in a way such that arguments and calculations are easy to follow. Provide detailed arguments to your answers. An answer without explanation will be given no points.

The final exam consists of six problems, each of which can give up to 6 points, for a sum of 36 points.

The final score is the better of the final exam score; and the weighted average of the final exam score (75%) and the homework score (25%). The minimum scores required for each grade are given by the following table:

Grade	A	B	C	D	E	Fx
Credit	30	27	24	21	18	16

A score of 16 or 17 is a failing grade with the possibility to improve to an E grade by additional work.

Problem 1. (6 points).

Let $\sigma = (147)(2356) \in S_7$, the symmetric group on the letters $\{1, \ldots, 7\}$.

(a) What is the order of σ?

(b) What is the centralizer $C_{S_7}(\sigma)$?

(c) How many elements of the same order as σ are there in S_7?

Solution.

(a): The order of (147) is 3, the order of (2356) is 4. Since the cycles (147) and (2356) are disjoint, they commute. It follows that the subgroup of S_7 generated by $\sigma = (147)(2356)$ is isomorphic to $\mathbb{Z}/3 \times \mathbb{Z}/4$. As $\mathbb{Z}/3 \times \mathbb{Z}/4$ is isomorphic to $\mathbb{Z}/12$, we can conclude that the order of $\sigma = (147)(2356)$ is 12.

(b): Let τ be an element in S_7. Since conjugation with τ is a group homomorphism, it takes two commuting elements to two commuting elements. Recall also that conjugation preserves the size of cycles. It follows that $\tau^{-1}(147)\tau$ and $\tau^{-1}(2356)\tau$ are two disjoint cycles of size 3 and 4 respectively. Assume now that τ is in the centralizer $C_{S_7}(\sigma)$. This means:

$$(147)(2356) = \sigma = \tau^{-1}\sigma\tau = \tau^{-1}(147)\tau\tau^{-1}(2356)\tau$$

As cycle decomposition is unique, τ is in both the centralizers $C_{S_7}(147)$ and $C_{S_7}(2356)$. Hence $C_{S_7}(\sigma) = C_{S_7}(147) \cap C_{S_7}(2356)$.

Recall that if a permutation τ centralizes a cycle, then it permutes elements not in the cycle into elements not in the cycle. It thus follows that any τ in $C_{S_7}(147) \cap C_{S_7}(2356)$ has a cycle decomposition that consists of cycles whose all elements are either in $\{1, 4, 7\}$ or in $\{2, 3, 5, 6\}$. Such a permutation then commutes with both (147) and (2356) if and only if it is of he form $(147)^n(2356)^l$. We can conclude that $C_{S_7}(147) \cap C_{S_7}(2356)$ has order 12. As it contains σ, $C_{S_7}(147) \cap C_{S_7}(2356)$ is the subgroup generated by σ. It follows that $C_{S_7}(147) \cap C_{S_7}(2356)$ is isomorphic to $\mathbb{Z}/3 \times \mathbb{Z}/4$.

(c): Any element in S_7 of order $12 = 3 \cdot 4$ has to have a decomposition into disjoint cycles of the form $(a_1a_2a_3)(b_1b_2b_3b_4)$ since the order of an element is the least common multiple of sizes of the cycles in such a decomposition. There are $7!/(3 \cdot 4) = 7 \cdot 6 \cdot 5 \cdot 2 = 420$ such elements.

Problem 2. (6 points).

Let n be a positive natural number. What is the number of solutions of the equation $x^2 - x = 0$ in $\mathbb{Z}/n\mathbb{Z}$? You might first try to solve the case where n is prime power and then use the Chinese Remainder Theorem.

Solution.

If $n = p^k$ then $0 = x^2 - x = x(x-1)$ has only 0 and 1 as solutions since

$$(\mathbb{Z}/p^k\mathbb{Z})^\times = \{[m] \in \mathbb{Z}/p^k\mathbb{Z} \mid p \nmid m\}$$

and thus one of x and $x-1$ must be a unit and hence the other zero.

If $n = p_1^{n_1} \cdots p_k^{n_k}$ is the prime decomposition of n then by the Chinese Remainder Theorem,

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{n_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{n_k}\mathbb{Z},$$

and solutions of $x^2 - x = 0$ in $\mathbb{Z}/n\mathbb{Z}$ are in one-to-one correspondence with tuples $(x_1, \cdots, x_k) \in \mathbb{Z}/p_1^{n_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{n_k}\mathbb{Z}$ such that $x_i^2 = x_i \in \mathbb{Z}/p_i^{n_i}\mathbb{Z}$ for all i. Since there are two solutions in every case, the total number of solutions modulo n of $x^2 - x$ is 2^k, where k is the number of distinct prime divisors of n.

Problem 3. (6 points).

Let $f\colon G \to H$ be a group homomorphism with kernel K and image I. Show:

(a) For every subgroup $N \leq G$, $f^{-1}(f(N)) = KN = \{kn \mid k \in K, n \in N\}$.

(b) For every subgroup $L \leq H$, $f(f^{-1}(L)) = I \cap L$.

Solution.

(a): Since for any k in K and n in N:

$$f(kn) = f(k)f(n) = ef(n) = f(n) \in f(N)$$

the set KN is a subset of $f^{-1}(f(N))$. It remains to show that any element in $f^{-1}(f(N))$ can be written as kn for some k in K and n in N. Let x be in $f^{-1}(f(N))$. This means that $f(x) = f(n)$ for some n in N and consequently xn^{-1} belongs to K. Since $x = xn^{-1}n$, we can conclude that x is a product of an element $k = xn^{-1}$ in K and n in N.

(b): By definition, $f^{-1}(L)$ consists of these elements in G that are maps via f to an element in L. This means $f(f^{-1}(L)) \subset L$ and hence $f(f^{-1}(L)) \subset L \cap I$, as I is the image of f. It reminds to show the inclusion $L \cap I \subset f(f^{-1}(L))$. Let x be in $L \cap I$. Since x is in I, there is y in G such that $f(y) = x$. Since x is in L, this y has to belong to $f^{-1}(L)$ and consequently $x = f(y) \in f(f^{-1}(L))$.

Problem 4. (6 points).

Let R be a PID and $S \subset R$ be a multiplicative subset. Show that $R[S^{-1}]$ is also a PID.

Solution.

Let $I \triangleleft R[S^{-1}]$ be an ideal. Then $J = I \cap R$ is an ideal in R since it is the preimage of I under the canonical inclusion $R \to R[S^{-1}]$. Hence $J = (x)$ for some $x \in R$. Now I claim that $JR[S^{-1}] = I$ and hence $I = (x)$ as an ideal in $R[S^{-1}]$. It is clear that $JR[S^{-1}] \subseteq I$, so let $a \in I$. Then there exists some $s \in S$ such that $sa \in R$. Since $sa \in I$ as well, $sa \in J$. But then $s = (sa)s^{-1} \in JR[S^{-1}]$.

Problem 5. (6 points).

Let G be a group of order $637 = 7^2 \cdot 13$. Show that G is abelian.

Solution.

Consider the number of 13-Sylow subgroups in G. Recall that this number has to divide 7^2 and is congruent to 1 modulo 13. Since 49 is 10 modulo 13 and not 1, we can conclude that there is only one 13-Sylow subgroup in G. Let us denote it by S. Note that S is a cyclic group of order 13.

Consider now the number of 7-Sylow subgroups in G. Again this number has to divide 13 and is congruent to 1 modulo 7. As 13 is 6 and not 1 modulo 7, there is only one 7-Sylow's subgroup in G. Let us denote it by T.

We claim that T is abelian. Since T is a 7-group, it has a nontrivial center $Z(T)$. If $Z(T) = T$, then T is abelian. Otherwise there is an element t in $T \setminus Z(T)$. Let $< t >$ be the subgroup generated by t in T. Since t commutes with all elements in the center, the function:

$$< t > \times Z(T) \ni (a, b) \mapsto ab \in T$$

is a group homomorphism. The image of this group homomorphism includes both $Z(T)$ and $< t >$ thus its order is a multiple of 7. This order also divides 7^2. We can conclude that this homomorphism is surjective and hence T is abelian.

Consider the action of T on S by conjugation. This actions is given by a group homomorphism $T \to \text{Aut}(S)$. Since S is a cyclic of order 13, any of its automorphism is uniquely determined by where a generator is mapped. A generator can be mapped only to a generator. It follows that $\text{Aut}(S)$ is a group of order 12. Thus the image of $T \to \text{Aut}(S)$ has an order dividing 12. As it also divides 7^2, this image is of order 1. It follows that the conjugation action of T on S is trivial and hence elements of T commute with elements of S. It follows that the function:

$$T \times S \ni (a, b) \mapsto ab \in G$$

is a group homomorphism. Since it is injective, it is an isomorphism as both groups $T \times S$ and G have the same order. We can conclude that G is abelian.

Problem 6. (6 points).

Let R be the ring $\mathbb{Z}[\sqrt{-2}]$. Recall that R is a Euclidean domain with Euclidean multiplicative norm $N(a+b\sqrt{-2}) = a^2+2b^2$.

(a) Prove that $1+2\sqrt{-2}$ is a reducible element of R.

(b) Determine a greatest common divisor in R of $2+\sqrt{-2}$ and $4+\sqrt{-2}$.

(c) Prove that $R/(3+\sqrt{-2})$ is a finite field with 11 elements.

Solution.

(a) Since the norm of $1+2\sqrt{-2}$ is 9, any nontrivial factor has norm 3. The only elements of norm 3 are $\pm 1 \pm \sqrt{-2}$. Indeed, $(1-\sqrt{-2})(-1+\sqrt{-2}) = 1+2\sqrt{-2}$.

(b) We compute

$$4+\sqrt{-2} = 2(2+\sqrt{-2}) - \sqrt{-2}$$

and see that $\sqrt{-2}$ divides $2+\sqrt{-2}$, so $\sqrt{-2}$ is the gcd.

(c) Since $N(3+\sqrt{-2}) = 9+2 = 11$ is a prime, $3+\sqrt{-2}$ is irreducible and hence $K = R/(3+\sqrt{-2})$ is a field. By the Euclidean algorithm, any element $x \in R - \{0\}$ can be written as $x = (3+\sqrt{-2}q) + r$ where $N(r) < 11$, so K is finite. Since $(3+\sqrt{-2})(3-\sqrt{-2}) = 11$, the characteristic of K is 11. Since there are not 121 elements of norm less than 11 in R (in $a+b\sqrt{-2}$, $|a| \leq 3$ and $|b| \leq 2$, so $7 \cdot 5 = 35$ is an upper bound), K must have 11 elements.