KTH Teknikvetenskap

SF2729 Groups and Rings
Exam
Wednesday, June 10, 2015

Time: 14:00-19:00
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:

Garde	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

For any element σ in the symmetric group S_n, let $c(\sigma)$ denote the number of cycles in the cycle decomposition of σ. Show that for $n \geq 2$,

$$c((12)\sigma) = c(\sigma) + 1 \text{ or } c(\sigma) \text{ or } c(\sigma) - 1.$$

Solution.

Let all a_i's, b_i's, c_i's be different and different from 1 and 2. Note:

$$(12)(a_1 \cdots a_k 1) = (a_1 \cdots a_k 21)$$

$$(12)(a_1 \cdots a_k 2) = (a_1 \cdots a_k 12)$$

$$(12)(a_1 \cdots a_k 1 b_1 \cdots b_l 2 c_1 \cdots c_t) = (a_1 \cdots a_k 2 c_1 \cdots c_t)(1 b_1 \cdots b_l)$$

$$(12)(a_1 \cdots a_k 1)(b_1 \cdots b_l 2) = (a_1 \cdots a_k 2 b_1 \cdots b_l 1)$$

Write σ as a product of disjoint cycles.

- If none of these cycles contains 1 or 2, then clearly $c((12)\sigma) = c(\sigma) + 1$.
- If 1 is present in cycles of σ and not 2, or 2 is present and not 1, then according to the first two equalities above $c((12)\sigma) = c(\sigma)$.
- If both 1 and 2 are present in a single cycle of σ, then $c((12)\sigma) = c(\sigma) + 1$.
- If both 1 and 2 are present but in different cycles of σ, then $c((12)\sigma) = c(\sigma) - 1$.

Problem 2. (6 points).

Let R and S be rings. Recall that a ring homomorphism $f\colon R \to S$ is a function such that $f(x+y) = f(x) + f(y)$ and $f(xy) = f(x)f(y)$ for any x and y in R. Let p be a prime integer and n a natural number.

(a) Prove that any ring homomorphism $f\colon R \to \mathbb{Z}/p^n\mathbb{Z}$ is either the 0 function or maps 1 in R to 1 in $\mathbb{Z}/p^n$.

(b) Conclude that any non-zero ring homomorphism $f\colon R \to \mathbb{Z}/p^n\mathbb{Z}$ is surjective.

(c) Give an example of n and m and a non-zero ring homomorphism $f\colon \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ which is not surjective.

Solution.

(a) Since $f(1) = f(1 \cdot 1) = f(1)^2$, either $f(1) = 0$, in which case $f(x) = f(1 \cdot x) = f(1)f(x) = 0x = 0$ for all x, or $f(1)$ is an element x such that $x^2 - x = 0$ in $\mathbb{Z}/p^n\mathbb{Z}$. Since

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

one of x and $x-1$ must be a unit and hence the other zero. Since we have already dealt with the case $x = 0$, the only remaining possibility is $x = f(1) = 1$.

(b) $\operatorname{im}(f)$ is an additive subgroup of $\mathbb{Z}/p^n\mathbb{Z}$ which contains a generator (namely, 1), hence $\operatorname{im}(f) = \mathbb{Z}/p^n\mathbb{Z}$.

(c) The smallest example is $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ given by $[1] \mapsto [3]$. One only needs to verify that $[3]^2 = [9] = [3] \in \mathbb{Z}/6\mathbb{Z}$.

Problem 3. (6 points).

Let G be a group and $N \lhd G$ a normal subgroup of order 5 such that $G/N \cong S_3$, the symmetric group on three letters. Show:

(a) $|G| = 30$;

(b) G has a normal subgroup of order 15;

(c) G has three non-normal subgroups of order 10.

Solution.

(a): Recall that $|G| = |N||G : N|$. Since $|G : N| = |S_3| = 6$, we get $|G| = 5 \cdot 6 = 30$.

(b): Consider the following composition:

$$G \to G/N = S_3 \xrightarrow{\text{sign}} \mathbb{Z}/2$$

Note that this composition is a surjective homomorphism. Its kernel is therefore a normal subgroup of order $30/2 = 15$.

(c): Let $\pi \colon G \to G/N = S_3$ be the quotient homomorphism. Let $T \subset G$ be a subgroup of order 10. The subgroup $\pi(T) \subset S_3$ is non trivial, since T is too big to be in the kernel of π. The order of $\pi(T)$ divides the order of $S_3 = 6$ and the order of $T = 10$. Thus $|\pi(T)| = 2$. Consequently the kernel of π restricted to T is of order 5. It follows that N is a subgroup in T.

Let S be another subgroup of order 10 in G. We claim that $S = T$ if and only if $\pi(S) = \pi(T)$. If $S = T$, then clearly $\pi(S) = \pi(T)$. Assume $\pi(S) = \pi(T)$. Let $s \in S$. Choose $t \in T$ such that $\pi(t) = \pi(s)$. Note that st^{-1} belongs to $N = \ker(\pi)$ and hence we can write s as a product $st^{-1}t$ of an element st^{-1} in N and hence in T (see above) and an element t in T. It follows that s belongs to T. We can conclude that $S \subset T$ and hence $S = T$.

To finish the proof we just notice that S_3 has tree different subgroup of order 2. This translates into the statement that G has 3 different subgroups of order 10. As none of the subgroups of order 2 in S_3 is normal, the subgroups of order 10 in G can not be normal either.

Problem 4. (6 points).

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

Solution.

Let $x \in R[S^{-1}]$ be any nonzero element. Then $x = \frac{y}{s}$ where $s \in S$ and $y \in R$. Since R is a UFD, $y = p_1 \cdots p_k$ for prime elements p_i. Then

$$\frac{1}{s} p_1 \cdots p_k$$

is a factorization into a unit times a product of primes. For uniqueness, assume

$$x = p_1 \cdots p_k = q_1 \cdots q_l \in R[S^{-1}].$$

for primes p_i and q_j. There is an element $s \in S$ such that $sp_i \in R$ and $sq_j \in R$ for all i and j, for instance the product of all the denominators. Assuming w.l.o.g. that $l \leq k$, we have

$$s^k x = (sp_1) \cdots (sp_k) = s^{k-l}(sq_1) \cdots (sq_l) \in R.$$

Since R was assumed to be a UFD, $k = l$ and (possibly after reordering) $sp_i = u_i sq_i$ for some units u_i. Thus $p_i = u_i q_i$ and hence the decomposition is unique up to order and units.

Problem 5. (6 points).

Show that a group of order 80 cannot be simple.

Solution.

We have the prime factorization $80 = 2^4 \cdot 5$. For the number of Sylow 5-subgroups n_5 and of Sylow 2-subgroups n_2 we have

$$n_5 \equiv 1 \pmod 5, \quad n_5 \mid 16 \Rightarrow n_5 = 1 \text{ or } 16$$

and

$$n_2 \equiv 1 \pmod 2, \quad n_2 \mid 5 \Rightarrow n_2 = 1 \text{ or } 5.$$

If the group was simple, we would have $n_5 = 16$ and $n_2 = 5$. But that would lead to $16 \cdot 4 = 64$ elements of order 5 and at least $5 \cdot (2^4 - 2^3) = 40$ elements of order a power of 2, the latter because any two Sylow 2-subgroups can intersect in a group of order up to 2^3. But this adds up to 104 distinct elements already, which is impossible.

Problem 6. (6 points).

Is the polynomial $x^3 + 4$ reducible or irreducible in $\mathbb{Q}[x]$?

Solution.

If we let $x = y - 1$, we have

$$x^3 + 4 = (y-1)^3 + 4 = y^3 - 3y^2 + 3y + 3.$$

Eisenstein's criterion applies for $p = 3$ since 3 divides all coefficients except for the leading one, and 9 does not divide the constant coefficient. Hence $x^3 + 4$ is irreducible in $\mathbb{Z}[x]$ and, by Gauss's lemma, also in $\mathbb{Q}[x]$.

Alternatively, a degree 3 polynomial is reducible if and only if it has a zero, and $x^3 + 4$ has one irrational and two imaginary roots in $\mathbb{C}$, namely $\sqrt[3]{-4}$, $\sqrt[3]{-4}\rho$, $\sqrt[3]{-4}\rho^2$, where ρ is a primitive third root of unity. Thus it has no rational roots.