KTH Teknikvetenskap

SF2729 Groups and Rings
Exam
Wednesday, June 8, 2016

Time: 08:00-13:00
Allowed aids: none
Examiner: Roy Skjelnes

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. The homework problems will contribute with up to 9 points on the three first problems in the exam. Credits on the three first problems in the exam will together with the contribution from the homeworks give at most 18 points.

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

1. Define the concept *Sylow p-subgroup*. **(2 p)**
2. Formulate Sylow's theorem. **(2 p)**
3. Use Sylow's theorem to prove that there is a unique group of order 33. **(2 p)**

Solution

1. If $|G| = p^k m$ where p is a prime, $k \geq 1$ and m is not divisible by p then a Sylow p-subgroup of G is a subgroup of G of order p^k.
2. If G is a finite group then G contains a Sylow p-subgroup for any prime p dividing $|G|$. All p-groups of G are contained in a Sylow p-subgroup and all Sylow p-subgroups of G are conjugate. The number of Sylow p-subgroups of G is congruent to 1 modulo p and divides $|G|$.
3. Since the number of Sylow 3-subgroups is congruent to 1 modulo 3 and divides 11, it has to be 1. Moreover, the number of Sylow 11-subgroups has to be congruent to 1 modulo 11 and a divisor of 3. Hence this is also equal to 1. Both of these subgroups are normal and their intersection is trivial. Hence the group is a direct product of C_3 and C_{11} and therefore it has to be isomorphic to C_{33}.

Problem 2

Let $f\colon R \to S$ be a homomorphism of commutative unitary rings where $f(1) = 1$.

1. Give the definition of an ideal being a prime ideal. **(2 p)**
2. Let P be a prime ideal in S, show that $f^{-1}(P)$ is prime. **(2 p)**
3. Let P be a maximal ideal in S. Is $f^{-1}(P)$ necessarily maximal? **(2 p)**

Solution

1. The ideal I is prime if it is a proper ideal and such that $ab \in I$ then $a \in I$ or $b \in I$.
2. The composite map $R \to S \to S/P$ has kernel $f^{-1}(P)$, which is a proper ideal. The induced map
$$R/f^{-1}(P) \to S/P$$
is injective. Hence $R/f^{-1}(P)$ have no non-trivial zero divisors, and is then an integral domain. That is $f^{-1}(P)$ is a prime ideal.
3. Consider $\mathbb{Z} \subseteq \mathbb{Q}$, where f is the inclusion. Then 0 is a maximal ideal in $\mathbb{Q}$, but its inverse image is the zero ideal in $\mathbb{Z}$, which is not maximal.

Problem 3

Let G be a finite group acting on a finite set X. Burnside's theorem states that the number of orbits is $\frac{1}{|G|}\sum_{g\in G}|X_g|$, where $X_g = \{x \in X \mid g.x = x\}$.

1. Show that $\sum_{g\in G}|X_g| = \sum_{x\in X}|G_x|$. (Hint: consider $\{(g,x) \mid g.x = x\} \subseteq G \times X$) **(1 p)**

2. Prove Burnside's Theorem. **(2 p)**

3. The symmetric group on three letters acts naturally on the set X of 64 (equilateral) triangles having each edge painted with one of four colours. Apply Burnside's theorem to determine the number of distinguishable triangles. **(3 p)**

Solution

1. We compute the cardinality of $N = \{(g,x) \mid g.x = x\}$ in two different ways. For each $g \in G$ there are $|X_g|$ pairs in N having g as the first component. Thus $|N| = \sum_{g\in G}|X_g|$. On the other hand, for each $x \in X$ there are $|G_x|$ pairs having x as the second component. Thus $|N| = \sum_{x\in X}|G_x|$.

2. We have, from the course book, that $|G : G_x|$ the index of the stabilizer of $x \in X$, equals elements in the orbit $|Gx|$ of x. We have furthermore that $|G : G_x| = |G|/|G_x|$, and we can write
$$|N| = \sum_{x\in X}|G_x| = \sum_{x\in X}\frac{|G|}{|Gx|} = |G|(\sum_{x\in X}\frac{1}{|Gx|}).$$
For any $y \in X$ that are in one orbit Gx, we get $\sum_{y\in Gx}\frac{1}{|Gx|} = 1$. Therefore we have that $|N| = |G| \cdot r$, where r is the number of orbits, and we have proved Burnside's theorem.

3. The number of distinguishable triangles is the number of orbits r, and by the Burnside theorem we have
$$r = \frac{1}{|S_3|}\sum_{g\in S_3}|X_g|.$$
List the group elements as $S_3 = \{1, \rho_1, \rho_2, \mu_1, \mu_2, \mu_3\}$ where $\rho_2 = \rho_1^2$, and ρ_1 is rotation (counter clockwise) with $1/3$ of a circle. The μ_1, μ_2 and μ_3 are reflections fixing one corner of the triangle. The identity element fixes every triangle, so $|X_1| = 64$. A triangle being fixed by a rotation means that all sides in the triangle have the same colour. Thus
$$|X_{\rho_1}| = |X_{\rho_2}| = 4.$$
A triangle fixed by a reflection means that the two reflecting sides of the triangle have same colour, hence
$$|X_{\mu_1}| = |X_{\mu_2}| = |X_{\mu_3}| = 16.$$

We then get that

$$r = \frac{1}{6}(64 + 2 \cdot 4 + 3 \cdot 16) = \frac{1}{6}8(8 + 1 + 6) = 20.$$

Problem 4

Let $R = \mathbb{Z}[x]/(x^2 + 1)$ be the ring of Gaussian integers.

1. Determine the maximal ideal I such that $I^2 = (2)$. **(3 p)**
2. Show that the quotient ring $R/(2 + 3x)$ is a field with 13 elements. **(3 p)**

Solution

1. We have $2 = (1 + x)(1 - x)$. As $(1 + x)$ and $(1 - x)$ both have norm two, we get that $(1 + x)$ and $(1 - x)$ are both irreducible, hence prime elements. We then have that these two elements generate maximal ideals. As the two irreducible elements are associates $(1 + x)(-x) = 1 - x$, we get the equality of ideals $M = (1 + x) = (1 - x)$. As $2 = (1 + x)(1 - x)$ it follows that we have the equality of ideals $(2) = M^2$.

2. As 13 is a prime congruent to 1 modulo 4, we know that $(13) = (2 + 3x) \cdot (2 - 3x)$, where the two factors are irreducible, and hence prime, hence maximal in $R = \mathbb{Z}[x]/(x^2 + 1)$. We have that $\mathbb{Z}[x]/(x^2 + 1, 13) = \mathbb{Z}_{13}[x]/(x^2 + 1)$, where $\mathbb{Z}_{13} = \mathbb{Z}/(13)$. It then follows that $R/(13)$ is the Gaussian integers with coefficients in $\mathbb{Z}_{13}$, and that $|R/(13)| = 13 \cdot 13$. By the Chinese Restminder we also have that $R/(13) = R/(2 + 3x) \times R/(2 - 3x)$. The only possibility for the order of the non-trivial ring $R/(2 + 3x)$ is 13.

Problem 5

A *short exact sequence* of groups is given by the following diagram of groups and homomorphisms

$$1 \to G \to H \to K \to 1$$

where the kernel of each homomorphism is equal to to the image of the homomorphism preceeding it, and where 1 denotes the trivial group.

1. Show that if $1 \to G \to H \to K \to 1$ is a short exact sequence and H is finite, then both G and K are finite and $|H| = |G| \cdot |K|$. **(2 p)**
2. Determine whether for odd integers $n \geq 3$ there is a short exact sequence

   $$1 \to C_2 \to D_{2n} \to C_n \to 1,$$

   where D_{2n} is the dihedral group, and C_n is the cyclic group, and their order is given by their indices. **(2 p)**

3. Determine whether for odd integers $n \geq 3$ there is a short exact sequence

$$1 \to C_n \to D_{2n} \to C_2 \to 1.$$

(2 p)

Solution

1. The image of the leftmost homomorphism is trivial which shows that the kernel of the second homomorphism is trivial. Hence this homomorphism is injective. The kernel of the rightmost homomorphisms is all of K which shows that the third homomorphism is surjective. Since a subgroup of a finite group is finite and the homomorphic image of a finite group is finite we get that G and K are finite if H is finite. By the isomorphism theorem we get that K is isomorphic to H/G and hence $|K| = |H|/|G|$, which proves that $|H| = |G| \cdot |K|$.

2. By the first part we have that C_2 needs to be a normal subgroup of D_{2n}. However all reflexions in D_{2n} generate subgroups of order two and these are all conjugated by Sylow's theorem. Hence D_{2n} doesn't have any normal subgroup of order two which shows that there cannot be such a short exact sequence.

3. The subgroup of rotations is normal since $sr^i s = r^{-i}$ for any reflection s. The quotient of D_{2n} by this normal subgroup has order two and is therefore isomorphic to C_2. This proves the existence of such a short exact sequence.

Problem 6

1. In $R = \mathbb{Z}[x]/(x^2 - 7)$ we have the equality $2 \cdot 3 = (1 + x)(-1 + x)$. Does this equality imply that R is not a UFD? **(2 p)**

2. Show that $\mathbb{Z}[x]/(x^2 + d)$ is not a UFD when $d \geq 3$. **(4 p)**

Solution

1. No, the factors are not irreducible. We have that $2 = (3+x)(3-x)$, and $3 = (2+x)(2-x)$. By looking at the norm $N(a, b) = a^2 - 7b^2$, we see that the elements $3+x, 3-x, 2+x$ and $2-x$ are irreducible. We have $(3+x)(2-x) = -1-x$ and that $(3-x)(2+x) = -1+x$, and in particular we have that

$$6 = 2 \cdot 3 = (3 + x)(3 - x)(2 + x)(2 - x) = (1 + x)(1 - x).$$

Therefore the given equality only appears to give two different factorizations, but gives in fact only a partial factorization with factors not being irreducible.

2. In a UFD an element is prime if and only if its irreducible. It then suffices to show that one particular element is irreducible, but not prime. The element we will consider is the number 2. We have the norm $N(a+bx) = a^2 + db^2$, which is multiplicative. The norm of 2 is 4. If 2 was reducible it would be the product of two elements $2 = \pi \cdot \pi'$ where both factors would have norm 2. However, as $d \geq 3$, it is impossible to write $2 = a^2 + db^2$. So, 2 is irreducible.

   Now, if $d = 2n$ is even, consider the product $(2+x)(2-x) = 4 + (2n) = 2(2+n)$ which is in the ideal generated by 2. However neither $2+x$ or $2-x$ is in the ideal (2). So 2 is not prime for even $d = 2n$. If $d = 2n+1$ is odd, then we consider the product $(1+x)(1-x) = 1+(2n+1) = 2(n+1)$ which is in the ideal generated by 2. But, neither $(1+x)$ nor $(1-x)$ is in that ideal. So 2 is not prime for odd $d = 2n+1$ either.

   Thus, for any $d \geq 3$ we have proven that 2 is not prime, but irreducible. Hence the quotient ring $\mathbb{Z}[x]/(x^2+d)$ is not a UFD.