INDIAN INSTITUTE OF TECHNOLOGY, KHARAGPUR

Department of Mathematics

Modern Algebra(MA30002)

Assignment

Name: Altaf Ahmad
Roll no: 18MA20005

Solutions

1. Let $G = \mathbb{Z}/20\mathbb{Z}$ be the cyclic group. List all the generators of G. How many subgroups does G have ? List a generator for each of these subgroups.
   Ans : We know that a cyclic group is a group that is generated by a single element. That means that there exists an element g, say, such that every other element of the group can be written as a power of g. This element g is the generator of the group. So, first, we have to find all the generators of G. These can be represented as the elements $\overline{g}$ such that

   $$g \in \{x | x \in \mathbb{N},\ x < 20,\ x\ \ \&\ \ 20 \text{ are co-primes}\}$$

   So, we can conclude that, $|g| = \varphi(20)$ [here, $\varphi(x)$ is the Euler's totient function]
   Thus, the generators are : $\overline{1}, \overline{3}, \overline{7}, \overline{9}, \overline{11}, \overline{13}, \overline{17}, \overline{19}$
   A "Converse of Lagrange's Theorem" (CLT) group is a finite group with the property that for every divisor of the order of the group, there is a subgroup of that order. This holds for the quotient groups of $\mathbb{Z}$ too. So, we can use this to find the subgroups :
   All the divisors of 20 : 1,2,4,5,10,20
   Thus, total number of proper subgroups = 5. (or 6 considering the group itself). Now, we have to list a generator for each of these subgroups :

   - $\overline{1}$ generates $\mathbb{Z}/20\mathbb{Z}$
   - $\overline{2}$ generates $2\mathbb{Z}/20\mathbb{Z}$
   - $\overline{4}$ generates $4\mathbb{Z}/20\mathbb{Z}$
   - $\overline{5}$ generates $5\mathbb{Z}/20\mathbb{Z}$
   - $\overline{10}$ generates $10\mathbb{Z}/20\mathbb{Z}$
   - $\overline{0}$ generates $20\mathbb{Z}/20\mathbb{Z}$

---

2. Let G be a group of order 100. Write down the order of the Sylow 2 subgroup and order of the Sylow 5 subgroup. Write down the possible number of Sylow 2 and Sylow 5 subgroups of G.
   Ans : We know that if G is a finite group of order $n = p^k m$, where p is prime and p does not divide m. A subgroup H of order p^k is called a Sylow p-subgroup of G. In our case, we have order of G :

   $$|G| = 100 = 2^2 \times 5^2$$

   Thus, we can say that the order of Sylow 2 subgroup is $2^2 = 4 \quad \&$ the order of the Sylow 5 subgroup is $5^2 = 25$
   Now, we have to look for the possible number of Sylow 2 and Sylow 5 subgroups of G.
   Sylow 2-subgroup : number of Sylow 2 subgroups divides 25, and is congruent to 1 mod 2 (odd divisors of 25). Thus $n_2 = x$, where $x \in \{1, 5, 25\}$
   Sylow 5-subgroup : number of Sylow 5 subgroups divides 4, and is congruent to 1 mod 5. Thus $n_5 = 1$

---

3. Show that $\mathbb{R}[x]/(x^2 + 1)$ is a field.
   Ans : In order to show that $\mathbb{R}[x]/(x^2 + 1)$ is a field, we only need to show that $x^2 + 1$ is maximal in $\mathbb{R}[x]$.
   Suppose that $I = (x^2 + 1) \subset J \subseteq \mathbb{R}[x]$. Then there exists a function $f(x) \in J$ such that $f(x) \notin I$. Hence $f(x) = q(x)(x^2 + 1) + r(x)$ for some polynomials $q(x), r(x) \in \mathbb{R}[x]$ with $0 \leq deg(r(x)) < 2$. Moreover, $r(x) \neq 0$. Hence $r(x)$ is linear and of the form $ax + b$ for some non-zero real numbers a, b. Now, $f(x) - q(x)(x^2 2 + 1) \in J$ so $r(x) = ax + b \in J$.
   Since $ax - b \in \mathbb{R}[x]$, $(ax + b)(ax - b) = a^2x^2 - b^2 \in J$. Similarly, $a^2(x^2 + 1) \in J$. Thus $(a^2x^2 + a^2) - (a^2x^2 - b^2) = a^2 + b^2 \in J$. Since $a^2 + b^2$ in not zero, J contains a constant and all constants in $\mathbb{R}[x]$ are units. Hence $1 \in J$ and $J = \mathbb{R}$. Therefore we can conclude that $x^2 + 1$ is indeed maximal as desired.
   Hence $\mathbb{R}[x]/(x^2 + 1)$ is a field.

---

4. Show that $R = \mathbb{Z}[\sqrt{-5}]$ is not an UFD. Give an example of an element in R which is irreducible but not prime.
Ans : We have to show that the ring R is not a UFD.
Consider 6 in R. We know that the elements of 6 factor in two ways : 6 = $2 \times 3 = (1+\sqrt{-5}) \times (1-\sqrt{-5})$ (non-unique factorization).
However, this is not enough, we have to show that all of the factors above are irreducible, and the factors in one are not associates of the factors in the other, so that there are two different factorizations into irreducible elements.
Now, consider the norm map N such that $N(a + b\sqrt{-5}) = a^2 + 5b^2$. This is "multiplicative," meaning that $N(\alpha\beta) = N(\alpha)N(\beta)$ for any α, β. Also, an element α is a unit if and only if $N(\alpha) = 1$.
$N(2) = 4$, so any proper factors of 2 have norm 2. There are no elements of norm 2 ⇒ there are no integers a and b so that $a^2 + 5b^2 = 2$.
$N(3) = 9$, so any proper factors of 3 have norm 3, and there are no such elements in $\mathbb{Z}[\sqrt{-5}].N(1 \pm \sqrt{-5}) = 6$, so any proper factors have norm 2 or 3, and there are no such elements.
Thus all of these factors are irreducible, and since their norms are all different, they are not associates of each other. Therefore $\mathbb{Z}[\sqrt{-5}]$ fails to be a UFD.
In our case, for example : $1 + \sqrt{5}i$ is irreducible but not prime.

---

5. Consider the polynomial $f(x) = 3x^5 + 15x^4 - 20x^3 + 10x + 20 \in \mathbb{Z}[x]$. Show that it irreducible over $\mathbb{Q}[x]$? Is it irreducible over $\mathbb{Z}[x]$? Justify your answer.
Ans : In order to show that it is irreducible over $\mathbb{Q}[x]$, we will use the Eisenstein's criterion. Suppose we have the following polynomial with integer coefficient:

$$q(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 = \sum_{i=0}^{n} a_i x^i$$

It states that the polynomial $q(x)$ is irreducible over $\mathbb{Q}[x]$ if there exists a prime number p such that the following conditions hold :

- p divides each a_i for each i, $0 \leq i < n$
- p does not divide a_n
- p^2 does not divide a_0

In our case, let us consider $p = 5$.
Thus, 5 | 15, 5 | 20, 5 | 10, 5 | 20.
Also, 5 does not divide 3, and $p^2 = 25$ does not divide $a_0 = 20$.
Hence the given polynomial is irreducible over $\mathbb{Q}[x]$.
Now, we have to check if the polynomial is irreducible over $\mathbb{Z}[x]$. We can see that the given polynomial $f(x)$ is primitive i.e, content ($f(x)$) = 1.
Thus, by applying a corollary of Gauss's lemma, sometimes also called Gauss's lemma, which says that a primitive polynomial is irreducible over the integers if and only if it is irreducible over the rational numbers. We can say that $f(x)$ is irreducible over $\mathbb{Z}[x]$.
