

Math 113 Final Exam Solutions

August 14, 2009

1 Computations

Problem 1.1. Take for granted that the group of rigid motions of the tetrahedron is A_4 , where the action of $\sigma \in A_4$ is given by permuting the vertices of the tetrahedron. How many different ways can the vertices of the tetrahedron be colored with the three colors red, blue, and green, up to rigid motion?

Solution 1.1.1. The group A_4 consists of the identity, three permutations of type $(2, 2)$, and eight permutations of type $(1, 3)$. Hence A_4 has a single element with 4 disjoint cycles in its cycle decomposition, and eleven other elements with 2 disjoint cycles in their cycle decomposition. Hence by Burnside's Counting Theorem the number of colorings is

$$\frac{1}{12}(3^4 + 11 \cdot 3^2) = 15.$$

Problem 1.2. Let H be the subgroup of \mathbb{Z}^3 generated by the three elements

$$(10, 6, 10), \quad (8, 4, 4), \quad (2, 2, 6).$$

Compute \mathbb{Z}^3/H as a product of cyclic groups.

Solution 1.2.1. We apply elementary row and column operations to the matrix of generators:

$$\begin{aligned} \begin{pmatrix} 10 & 8 & 2 \\ 6 & 4 & 2 \\ 10 & 4 & 6 \end{pmatrix} &\sim \begin{pmatrix} 2 & 8 & 10 \\ 2 & 4 & 6 \\ 6 & 4 & 10 \end{pmatrix} \sim \begin{pmatrix} 2 & 0 & 0 \\ 2 & -4 & -4 \\ 6 & -20 & -20 \end{pmatrix} \sim \\ &\begin{pmatrix} 2 & 0 & 0 \\ 0 & -4 & -4 \\ 0 & -20 & -20 \end{pmatrix} \sim \begin{pmatrix} 2 & 0 & 0 \\ 0 & -4 & 0 \\ 0 & -20 & 0 \end{pmatrix} \sim \begin{pmatrix} 2 & 0 & 0 \\ 0 & -4 & 0 \\ 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 2 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 0 \end{pmatrix}. \end{aligned}$$

Hence there is a basis of \mathbb{Z}^3 such that with respect to this basis, $H = 2\mathbb{Z} \times 4\mathbb{Z} \times \{0\}$. Thus

$$\mathbb{Z}^3/H \cong \frac{\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}}{2\mathbb{Z} \times 4\mathbb{Z} \times \{0\}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}.$$

Problem 1.3. Let $p(x) = x^4 + x + 1 \in \mathbb{Z}/2\mathbb{Z}[x]$. Do the following:

1. Show that $F = (\mathbb{Z}/2\mathbb{Z}[x])/(p(x))$ is a field.

2. Let $\alpha = \bar{x} \in F$. Find the minimal polynomial of $\alpha^2 + \alpha + 1$ over $\mathbb{Z}/2\mathbb{Z}$.

Solution 1.3.1. (1) We have to check that $p(x) = x^4 + x + 1$ is irreducible over $\mathbb{Z}/2\mathbb{Z}$. First note that $p(0) = 1 = p(1)$, so $p(x)$ has no roots, hence has no degree-1 factors. It remains to show that $p(x)$ cannot factor into two degree-2 factors. Suppose we had such a factorization:

$$p(x) = (x^2 + ax + b)(x^2 + cx + d) = x^4 + (a+c)x^3 + (b+d+ac)x^2 + (ad+bc)x + bd.$$

Then $bd = 1$, so $b = d = 1$. Then we have $a + c = 0$ and $ad + bc = 1$. But then $1 = ad + bc = a + c$, contradicting that $a + c = 0$. Hence no such factorization exists, so $p(x)$ is irreducible and hence F is a field.

(2) We have $\alpha^4 + \alpha + 1 = 0$ in F , so $\alpha^4 = \alpha + 1$. Let $\beta = \alpha^2 + \alpha + 1$. Then we have

$$\begin{aligned}\beta^2 &= (\alpha^2 + \alpha + 1)^2 \\ &= \alpha^4 + 2\alpha^3 + 3\alpha^2 + 2\alpha + 1 \\ &= \alpha^4 + \alpha^2 + 1 \\ &= \alpha + 1 + \alpha^2 + 1 \\ &= (\alpha^2 + \alpha + 1) + 1 \\ &= \beta + 1.\end{aligned}$$

Hence $\beta^2 + \beta + 1 = 0$, so $q(x) = x^2 + x + 1 \in \mathbb{Z}/2\mathbb{Z}[x]$ is a polynomial which has β as a root. Moreover, this polynomial is monic and irreducible (since it is degree-2 and has no roots), hence $q(x)$ is the minimal polynomial of β .

2 Theory

Problem 2.1. Let $p(x) \in \mathbb{Z}[x]$ be a monic polynomial. Suppose that $p(x) = a(x)b(x)$ where $a(x), b(x) \in \mathbb{Q}[x]$ and $a(x)$ is monic. Show that $a(x), b(x) \in \mathbb{Z}[x]$.

Solution 2.1.1. Let $a(x) = a_0 + a_1x + \cdots + a_nx^n$, $b(x) = b_0 + b_1x + \cdots + b_mx^m$, where a_n, b_m are nonzero. By assumption $a_n = 1$. The leading coefficient of $a(x)b(x)$ is $a_nb_m = b_m$, and this is 1 since $p(x) = a(x)b(x)$ is monic by assumption; hence $b_m = 1$ also, so $b(x)$ is monic.

Now, by the Gauss lemma, there exist rational numbers $r, s \in \mathbb{Q}$ such that $ra(x) \in \mathbb{Z}[x]$, $sb(x) \in \mathbb{Z}[x]$, and $p(x) = (ra(x))(sb(x))$. Now, since $a(x)$ is monic, $ra(x)$ has leading coefficient r . Since $ra(x) \in \mathbb{Z}[x]$, we must have $r \in \mathbb{Z}$. Likewise, since $b(x)$ is monic, we have $s \in \mathbb{Z}$. We have $a(x)b(x) = p(x) = rsa(x)b(x)$. Since $\mathbb{Q}[x]$ is an integral domain, we have $rs = 1$. Thus $r = s = 1$ or $r = s = -1$. In any case we have $\pm a(x) \in \mathbb{Z}[x]$ and $\pm b(x) \in \mathbb{Z}[x]$, thus $a(x), b(x) \in \mathbb{Z}[x]$.

Problem 2.2. Let R be a commutative ring. An element $a \in R$ is called *nilpotent* if there is some $k \in \mathbb{N}$ such that $a^k = 0$.

1. Show that the set of nilpotent elements of R is an ideal.
2. Give an example of a nonzero nilpotent element in the ring $\mathbb{Q}[x]/(x^2 + 6x + 9)$.

Solution 2.2.1. (1) Let I be the set of nilpotent elements of R . We need to show that I is a subgroup of $(R, +)$ and that I is closed under multiplication by arbitrary elements of R . Note first that $0 \in I$ since $0^1 = 0$, so I is nonempty. Let $a, b \in I$ be arbitrary; then there exist $k, \ell \in \mathbb{N}$ such that $a^k = 0 = b^\ell$. We have

$$(a + b)^{k+\ell} = \sum_{i=0}^{k+\ell} \binom{k+\ell}{i} a^i b^{k+\ell-i}.$$

Now, for every i such that $i \geq k$, we have $a^i = 0$ since $a^k = 0$. And for every i such that $i < k$, we have $k + \ell - i > \ell$, so $b^{k+\ell-i} = 0$ since $b^\ell = 0$. Hence every term appearing in our sum is 0, so $(a + b)^{k+\ell} = 0$. Hence $a + b \in I$. We also have $(-a)^k = (-1)^k a^k = 0$, hence $-a \in I$. Thus I is a subgroup of $(R, +)$.

Now, let $r \in R$ be arbitrary. Then $(ra)^k = r^k a^k = r^k 0 = 0$, hence $ra \in I$. Hence I is closed under multiplication by arbitrary elements of R , so I is an ideal of R .

(2) Consider the element $a = \overline{x + 3} \in \mathbb{Q}[x]/(x^2 + 6x + 9)$. We have $a \neq 0$ since $x + 3$ is not a multiple of $x^2 + 6x + 9$ by degree considerations. And we have $a^2 = \overline{x^2 + 6x + 9} = 0$. Hence a is a nonzero nilpotent element of this ring.

Problem 2.3. Let G be a group and let N be a normal subgroup of G . Suppose that $[G : N] = p$ is prime. Show that if H is another subgroup of G and $N \subseteq H$, then $H = N$ or $H = G$.

Solution 2.3.1. Since $|G/N| = [G : N] = p$ is prime, we have that $G/N \cong \mathbb{Z}/p\mathbb{Z}$. By the lattice isomorphism theorem, the subgroups of G containing N are in bijection with the subgroups of $G/N \cong \mathbb{Z}/p\mathbb{Z}$. $\mathbb{Z}/p\mathbb{Z}$ has only two subgroups: 0 and $\mathbb{Z}/p\mathbb{Z}$. Hence there are only two subgroups of G which contain N , namely G and N .

Problem 2.4. Show that every subgroup of \mathbb{Z}^n is n -generated.

Solution 2.4.1. See class notes, Ch. 11, Thm 6.5.