Algebra 2 Homework 4

Gandhar Kulkarni (mmat2304)

1

We know that the commutator subgroup of F, the free group on two generators, will be generated by all elements of the form $w_1 w_2 w_1^{-1} w_2^{-1}$, where w_1, w_2 are words in the free group. Let the set of generators be denoted by S. We consider DF, the commutator subgroup of F. By the universal property of free groups, we have the commutative diagram

$$\begin{tikzcd} & F(S) \arrow[dr, two heads, "\exists!\Phi"] & \\ S \arrow[ur, hook, "i"] \arrow[rr, hook, "i"] & & DF \end{tikzcd}$$

where $F(S)$ surjects onto DF. Then see that for any element $w \in \ker \Phi$, the action on the map is given by the inclusion of each letter of the word, and where it is sent. Due to this, we must have that $F(S) \cong DF$. Since DF is isomorphic to a free group of infinite rank, it is not finitely generated.

2

See that for all $i \in \{1, 2, 3, 4, 5\}$ we have t'_i is a product of disjoint transpositions. We know that the order of t'_i is the least common multiple of all the cycles, which is clearly 2 in this case. Then we have $t'^2_i = 1$.

Now see that $t'_1 t'_2 = (1, 2)(3, 4)(5, 6) \circ (1, 4)(2, 5)(3, 6) = (1, 3, 5)(2, 6, 4)$, $t'_2 t'_3 = (1, 4)(2, 5)(3, 6) \circ (1, 3)(2, 4)(5, 6) = (1, 6, 2)(3, 4, 5)$, $t'_3 t'_4 = (1, 3)(2, 4)(5, 6) \circ (1, 2)(3, 6)(4, 5) = (1, 4, 6)(2, 3, 5)$, and $t'_4 t'_5 = (1, 2)(3, 6)(4, 5) \circ (1, 4)(2, 3)(5, 6) = (1, 5, 3)(2, 6, 4)$. These are all products of disjoint $3-$cycles, thus they have order 3.

It is also interesting to see that $t'_1 t'_3 = (1, 2)(3, 4)(5, 6) \circ (1, 3)(2, 4)(5, 6) = (1, 4)(2, 3)$, $t'_1 t'_4 = (1, 2)(3, 4)(5, 6) \circ (1, 2)(3, 6)(4, 5) = (3, 5)(4, 6)$, $t'_1 t'_5 = (1, 2)(3, 4)(5, 6) \circ (1, 4)(2, 3)(5, 6) = (1, 3)(2, 4)$, $t'_2 t'_4 = (1, 4)(2, 5)(3, 6) \circ (1, 2)(3, 6)(4, 5) = (1, 5)(2, 4)$, $t'_2 t'_5 = (1, 4)(2, 5)(3, 6) \circ (1, 4)(2, 3)(5, 6) = (2, 6)(3, 5)$, and $t'_3 t'_5 = (1, 3)(2, 4)(5, 6) \circ (1, 4)(2, 3)(5, 6) = (1, 2)(3, 4)$, which is a product of disjoint $2-$cycles.

See that $i'_3 t'_5 t'_1 = (6, 5)$, and $t'_1 t'_2 t'_4 = (6, 5, 4, 3, 2, 1)$. These two can generate S_6, since a transposition and a $n-$cycle can generate S_n. Thus we have a presentation for S_n. We also know that transpositions that change consecutive elements generate S_n, hence the map defined for the five such elements of S_6 suffice to determine an automorphism. This automorphism is clearly not inner.

3

Let $\alpha \in \mathbb{Q}$. It satisfies a monic polynomial $f(x) \in \mathbb{Z}[x]$. Then we have

$$\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_0 = 0.$$

Let $\alpha = \frac{p}{q}$, with $(p, q) = 1$. Then we have

$$p^n + c_{n-1}p^{n-1}q + \cdots + c_0 q^n = 0.$$

Reducing this equation modulo q, we have

$$p^n \equiv 0 \mod q.$$

Since $(p, q) = 1$, we have $q = 1$. Thus $\alpha \in \mathbb{Z}$.

4

We have $f(x) = x^5 - ax - 1$. For $a = 0$, $f(x) = (x-1)(x^4 + x^3 + x^2 + x + 1)$, which is a non-trivial reduction. For $a = 2$, we have $f(-1) = 0$, so this is also reducible. For $a = -1$, we have $f(x) = x^5 - x - 1$ which can be factored as given by the problem. Now assume $a \neq -1, 0, 2$. If $f(x)$ factors, it will either have a linear factor or a quadratic factor. Then we shall see that there can never be zero remainder, to prove that it is irreducible.

If there was a linear factor, then f would have an integer root, say k. By the rational roots theorem, we must have $k| - 1$. Thus we have $k = 1, -1$. In either case, f is not zero. Thus there is no linear factor.

If there was a quadratic factor, then we have $x^5 - ax - 1 = (x^2 + a_1x + a_0)(x^3 + b_2x^2 + b_1x + b_0)$. See that $a_0b_0 = -1$, so we have two cases $a_0 = 1, b_0 = -1$ and $a_0 = -1, b_0 = 1$. In the first, we substitute this in the other constraints

$$\begin{aligned} b_2 + a_1 &= 0 \\ a_1b_2 + a_1 + b_1 &= 0 \\ a_0b_2 + a_1b_1 + b_0 &= 0 \\ a_0b_1 + a_1b_0 &= -a \end{aligned}$$

Many substitutions later, we have $a_1^3 + a_1^2 - a_1 + 1 = 0$. If it has an integer root, we must have $a_1|1$. In either case $a_1 = 1, -1$, this equation is not satisfied. Thus there is no solution for a_1.

In the other case where $a_0 = -1, b_0 = 1$, we have the equation $a_1^3 - a_1^2 + a_1 + 1 = 0$. The same way as above, if it is possible, $1, -1$ are the only roots. However, it is not zero at those points, hence there are no solutions for this case.

Thus this polynomial is irreducible.

5

See that $x^2 - 4x + 1$ is a polynomial that $2 + \sqrt{3}$ satisfies. The minimal polynomial if it is any smaller would have degree 1. But since $2 + \sqrt{3}$ is not rational, the degree of its minimal polynomial must be at least 2. Thus we have that $2 + \sqrt{3}$ has exactly degree 2 over $\mathbb{Q}$.

Consider the number field $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, which is a degree 3 extension. It is a $\mathbb{Q}$ vector space, so it clearly contains the element $1 + \sqrt[3]{2} + \sqrt[3]{4}$. Therefore it must have degree at most 3 in $\mathbb{Q}$. Since it is not rational, its degree over $\mathbb{Q}$ must be at least 2. Let us see if any quadratic polynomial can satisfy it. Let $x^2 + ax + b \in \mathbb{Q}[x]$ be some rational polynomial. Assume $\alpha = \sqrt[3]{2}$. Assume that $(1 + \alpha + \alpha^2)$ satisfies this quadratic polynomial, so we must have

$$\begin{aligned} (1 + \alpha + \alpha^2)^2 + a(1 + \alpha + \alpha^2) + b &= 3\alpha^2 + 4\alpha + 5 + a + a\alpha + a\alpha^2 + b \\ &= (3 + a)\alpha^2 + (4 + a)\alpha + (5 + a + b). \end{aligned}$$

If this is to be 0, then we must have $a = -3$ and $a = -4$, which is absurd.

Therefore $1 + \sqrt[3]{2} + \sqrt[3]{4}$ must be of degree 3.

6

If we can find a $a + bi \in \mathbb{Q}(i)$, such that $x^3 - q$ vanishes for $q \in \{2, 3\} \in \mathbb{Q}$, then we can reduce the polynomial. If this is possible, then we must have

$$(a + bi)^3 = (a^3 - 3ab^2) + i(3a^2b - b^3) \in \mathbb{Q},$$

which forces $3a^2b = b^3$. If $b = 0$, then it is equivalent to asking if a rational root for q exists, which is not true. Thus we must have $b \neq 0$. Then we have $3a^2 = b^2$, which has no rational solution since $\sqrt{3}$ is not rational. Therefore we must have that $x^3 - 2$ and $x^3 - 3$ are both irreducible, since they have no solutions on $\mathbb{Q}(i)$.

7

Let $q(x)$ be an irreducible polynomial dividing $f(g(x))$. Then we define $K \cong \frac{F[x]}{(q(x))}$. We consider the canonical projection $\pi : F[x] \to K$. We consider the image of $g(x)$ under π. We get $\overline{g(x)} = g(x) + (q(x))$. We claim that $f(\overline{g(x)})$ is 0. We have

$$f(\overline{g(x)}) = \sum_{i=0}^{n} a_i(g(x) + (q(x)))^i = \sum_{i=0}^{n} a_i(g(x)^i + (q(x))) = \sum_{i=0}^{n} a_i g(x)^i + (q(x)) = f(g(x)) + (q(x)).$$

We know that $f(g(x))$ is a multiple of $q(x)$, thus $\overline{g(x)}$ is a root of $f(g(x))$. Let $\alpha = \overline{g(x)}$. We have a root of f over K, and we know f is irreducible on F, thus $[F(\alpha) : F] = \deg f = n$. Note that q is irreducible over F, thus we have $[K : F] = \deg q$. Now we have

$$[K : F] = [K : F(\alpha)][F(\alpha) : F],$$

which gives the required result that $n | \deg q$..