SAMPLE FINAL EXAM, MATH 4030

1) Use mathematical induction to prove the following statement for all natural numbers n:

$$2n \leq 2^n.$$

Note: this is really easy. In the induction step use that $2 \leq 2^n$ and $2^n + 2^n = 2^{n+1}$.

2) We say that two integers a and b are equivalent modulo 3, and write $a \equiv b \pmod 3$, if $a - b = 3k$ for some integer k. Show that this relation is an equivalence relation on the set of integers $\mathbb{Z}$. Describe the corresponding equivalence classes.

3) Write down axioms of an abelian group G. Use $+$ to denote the binary operation. Show that the identity element is unique.

4) Find the inverse of 19 modulo 101 and then solve the equation

$$19x \equiv 7 \pmod{101}.$$

5) Factor the polynomial $x^4 - x^3 - 2x + 2$ in to prime polynomials in $\mathbb{Q}[x]$ and then in $\mathbb{R}[x]$. Justify your answer!

6) Rationalize

$$\frac{1}{(\sqrt[3]{2})^2 - \sqrt[3]{2} + 2}$$

i.e. write it as $a(\sqrt[3]{2})^2 + b\sqrt[3]{2} + c$ where a, b and c are rational numbers.

SOLUTIONS ON THE NEXT PAGE!

1)

- Base of induction, $n = 1$: Then $2 \cdot 1 \leq 2^1$ obviously holds.
- Induction step: Assuming that $2n \leq 2^n$ we want to show that $2(n+1) \leq 2^{n+1}$. Here is how it is done:

$$2(n+1) = 2n + 2 \leq 2^n + 2^n = 2^{n+1}.$$

2)

- Reflexivity: Since $a - a = 3 \cdot 0$, it follows that $a \equiv a \pmod 3$ for every a.
- Symmetry: If $a \equiv b \pmod 3$ then $a - b = 3k$. Then $b - a = 3(-k)$ which means that $b \equiv a \pmod 3$, as desired.
- Transitivity: If $a \equiv b \pmod 3$ and $b \equiv c \pmod 3$ then $a - b = 3k$ and $b - c = 3k'$. Adding these two equations gives $a - c = 3(k + k')$ and this implies that $a \equiv c \pmod 3$.

There are three classes, consisting of integers congruent to 0, 1 and 2 modulo 3.

3) Uniqueness of the identity element. If 0 and $0'$ are two identities, then on one hand $0 + 0' = 0$ since $0'$ is the identity element, and on the other hand $0 + 0' = 0'$ since 0 is the identity element. Thus

$$0' = 0 + 0' = 0.$$

4)

$$101 = 5 \cdot 19 + 6$$
$$19 = 3 \cdot 6 + 1$$

Solving the first equation for 6 and substituting in the second gives

$$16 \cdot 19 - 3 \cdot 101 = 1.$$

This shows that 16 is the inverse of 19 modulo 101. So the solution of the congruence is $16 \cdot 7 = 112 \equiv 13 \pmod{101}$.

5) The possible rational roots of $x^4 - x^3 - 2x + 2$ are $\pm 1, \pm 2$. Checking, one sees that 1 is the only rational root which gives a factorization

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

Since $x^3 - 2$ is irreducible in $\mathbb{Q}[x]$ by Eisenstein's criterion this completes factorization in $\mathbb{Q}[x]$. On the other hand $x^3 - 2$ has $\sqrt[3]{2}$ as unique real root, so $x^2 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + \sqrt[3]{4})$ completes the factorization in $\mathbb{R}[x]$.

6) We need to find rational polynomials $p(x)$ and $q(x)$ such that

$$p(x)(x^3 - 2) + q(x)(x^2 - x + 2) = 1.$$

This is done using Euclidean algortihm. Dividing $x^3 - 2$ by $x^2 - x + 2$ gives a reminder $x - 5$:

$$x^3 - 2 = (x + 1)(x^2 - x + 2) - (x - 5).$$

Next, dividing $x^2 - x + 2$ by $x - 5$ gives a reminder 22:

$$x^2 - x + 2 = (x + 4)(x - 5) + 22.$$

Substituting $x - 5 = (x + 1)(x^2 - x + 2) - (x^3 - 2)$ into second, and moving to the left terms involving $x^2 - x + 2$ as a factor gives

$$-(x^2 + 5x + 3)(x^2 - x + 2) = 22 - (x + 4)(x^3 - 2)$$

and this is essentially what we want. Indeed, substituting $x = \sqrt[3]{2}$ gives the answer:

$$-\frac{1}{22}(\sqrt[3]{2})^2 - \frac{5}{22}\sqrt[3]{2} - \frac{3}{22}.$$