Homework 5

1a) Recall that $\mathbb{Q} \subset \mathbb{R}$ and that $\mathbb{Q}$ and $\mathbb{R}$ are groups of their own under addition.

Therefore $(\mathbb{Q},+) \leq (\mathbb{R},+)$.

Also observe that $(\mathbb{R},+)$ is abelian:

Let $g,h \in \mathbb{R}$. Then $gh = g+h = h+g = hg$.
We know from 4.1.2 that any subgroup of an abelian group is normal. Thus $(\mathbb{Q},+) \trianglelefteq (\mathbb{R},+)$.

1b) Let $a \in \mathbb{R}/\mathbb{Q}$ such that $|a|$ is finite and $a \neq \mathbb{Q}$, the identity element.
Then $a = r_a \mathbb{Q}$ for some $r_a \in \mathbb{R}$.

Observe that $r_a \notin \mathbb{Q}$, as if $r_a \in \mathbb{Q}$ then

$$a = r_a \mathbb{Q} = \mathbb{Q},$$

as $\mathbb{Q}$ is a closed group. Therefore r_a is irrational. Finally, let $|a| = n$. Then

$$a^n = \mathbb{Q} \iff$$

$$(r_a \mathbb{Q})^n = \mathbb{Q} \iff$$

$$r_a^n \mathbb{Q}^n = \mathbb{Q} \iff$$

$$n r_a \mathbb{Q} = \mathbb{Q}.$$

However, $r_a \notin \mathbb{Q}$, and thus this is a contradiction. Therefore $|a|$ is infinite.

Homework 5

1c) First observe that $\mathbb{Q}$ is countable and $\mathbb{R}$ is uncountable:

Consider the function $\phi(a,b) = 2^a \cdot 3^b \cdot 5^{c+1}$ for $\mathbb{Q} = \{q \mid q = \frac{a}{b} \cdot c,\ a \in \mathbb{Z}^+, b \in \mathbb{N}, c = 1, 0, -1\}$
This would map every rational number q to a natural number unique to every value a, b, c within the construction of q. Therefore ϕ is a bijection of $\mathbb{N}$ and $\mathbb{Q}$ is countable.

Assume the function $\alpha : \mathbb{R} \to \mathbb{N}$ is a bijection. Then $\alpha(r) = n$ for $\forall r \in n$. However, consider every r on the interval $(0,1)$: Given α is one-to-one, each of the infinite values of r must map to a unique $n \in \mathbb{N}$, and as such the cardinality of the mappings is exhausted. Thus as we consider the intervals $(1,2)$ or (a,b) for $\mathbb{R}$, we find that $\mathbb{R}$ is uncountable

Assume that there is a countable subset of $\mathbb{R}/\mathbb{Q}$ that generates $\mathbb{R}/\mathbb{Q}$; then $\mathbb{R}/\mathbb{Q}$ must be countable as each element $a \in \mathbb{R}/\mathbb{Q}$ is generated by a countable combination of generators. However,

$$\mathbb{R}/\mathbb{Q} = \bigcup_{i=1}^{K} r_i \mathbb{Q} = \bigcup_{i \in \mathbb{Z}} r_i \mathbb{Q}$$

is uncountable as the cardinality of a union of sets is the sum of their own, and the sets where $r_i \notin \mathbb{Q}$ map isomorphically to $\mathbb{R}$ as $(r_i + q) \in \mathbb{R} \setminus \mathbb{Q}$.

Homework 5

2a) $N \trianglelefteq G$ and $\phi : G \to G$, so

$$g^{-1}Ng = N, \forall g \in G \iff$$

$$\phi(g^{-1}Ng) = \phi(N), \forall g \in G \iff$$

$$\phi(g^{-1})\phi(N)\phi(g) = \phi(N), \forall g \in G \iff$$

$$(\phi(g))^{-1}\phi(N)\phi(g) = \phi(N), \forall g \in G,$$

From Theorem 2.3.3, since ϕ is an automorphism, we know that each $\phi(g)$ for $g \in G$ will give a unique $h \in G$, meaning

$$(\phi(g))^{-1}\phi(N)\phi(g) = \phi(N), \forall g \in G \iff$$

$$(h)^{-1}\phi(N)(h) = \phi(N), \forall h \in G.$$

Thus, $\phi(N) \trianglelefteq G$, as $\phi(N)$ forms a subgroup of G that adopts inverses, identities, and associativity from G and is closed as any two elements $a, b \in N$ shows

$$\phi(ab) = \phi(a)\phi(b) = ab \in N.$$

2b) Let $f: G \to G/\phi(N)$.

Observe that f is a homomorphism:

Let $x, y \in G$. Then

$$\begin{aligned} f(x \circ y) &= (x \circ y)\,\phi(N) \\ &= (x\phi N) \circ (y \phi N) \\ &= f(x) \circ f(y). \end{aligned}$$

Also observe that f is onto:

Let $g\phi(N)$ be an arbitrary coset in $G/\phi(N)$. Then f is obviously onto as $f(g) = g\phi(N)$, for any $g \in G$.

Now we show $\ker(f) = N$:

$\ker(f) = \{ g \in G \mid f(g) = \phi(N) \}$.

Observe that $f(g) = g\phi(N)$, as above, and that $g\phi(N)g^{-1} = \phi(N)$ as $\phi(N) \trianglelefteq G$.

Thus $f(g) = \phi(N)$ only when

a) $g = e$, as $f(e) = \phi(N)$ trivially, or
b) $g \in N$, as $f(g) = g\phi(N) = \phi(N)g$, and

therefore $g\phi(N)g^{-1} = \phi(N)$. If $g \notin N$, then $g\phi(N) \neq \phi(N)g$ and $f(g) \neq \phi(N)$. Therefore $\ker(f) = N$. Finally we can see $G/\ker(f) \cong \operatorname{im}(f)$, or $G/N \cong G/\phi(N)$, by the first isomorphism theorem.

3a) Since $\gcd(|H|, [G:N]) = 1$ and $H \leq G$, we know that

$$|G| = [G:H]|H|$$

$$|G| = [G:N]|N|$$

$\gcd(|H|, [G:N]) = 1$, so there exists $a, b \in \mathbb{Z}$ such that

$$a|H| + b[G:N] = 1.$$

Therefore

$$a\frac{|G|}{[G:H]} + b\frac{|G|}{|N|} = 1.$$

However, this is only possible if

$H \leq N$, as Then $[G:H] = [G:N][N:H]$

and $[G:H] = \frac{|G|}{|N|}\frac{|N|}{|H|}$.

Then $a\frac{|G|}{[G:H]} = a\frac{|G|}{|N|}\frac{|N|}{|H|} = a|H|$ as above.

3b) Assume there is another subgroup $H \leq G$ with $|N|$. Then by Theorem 4.2.9,

$$|NH| = \frac{|N|^2}{|N \cap H|},$$ which as

$\gcd(|N|, [G:N]) = 1$, we know

$$|G| = [G:N]|N| \iff$$