MATH1530, HOMEWORK 2

Section 1.3

2. $\sigma\tau : 1 \xrightarrow{\tau} 14 \xrightarrow{\sigma} 11$, $11 \xrightarrow{\tau} 8 \xrightarrow{\sigma} 3$, $3 \xrightarrow{\tau} 10 \xrightarrow{\sigma} 1$, hence $(1\,11\,3)$ is a cycle in the cycle decomposition of $\sigma\tau$. Then pick any number not in this cycle, say 2, and repeat the same procedure: $2 \xrightarrow{\tau} 9 \xrightarrow{\sigma} 4$, $4 \xrightarrow{\tau} 2 \xrightarrow{\sigma} 2$, so $(2\,4)$ is another cycle. Continue in this way until cycles exhaust all numbers from 1 through 14. The answer is $(1\,11\,3)(2\,4)(5\,9\,8\,7\,10\,15)(13\,14)$.

Likewise for $\tau\sigma$.

10. We use induction on i. When $i = 0$, $\sigma^0(a_k) = a_k = a_{k+0}$. Assume this is true for i and let us show this for $i+1$. From induction hypothesis we have $\sigma^i(a_k) = a_{k+i}$. Therefore $\sigma^{i+1}(a_k) = \sigma(\sigma^i a_k) = \sigma(a_{k+i}) = a_{k+i+1}$. (every index is under modular m)

Notice that $\sigma^m(a_k) = a_{k+m} = a_k$ for all k, so σ^m is the identity. If we pick $0 < n < m$, $\sigma^n(a_1) = a_{1+n}$ and $1 + n \neq 1 \pmod m$. Hence σ^n is not the identity for $n < m$, which shows m is the order of this element.

Section 1.4

3. It is enough to present two invertible matrices A,B such that $AB \neq BA$.

We compute $\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\cdot\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} = \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$ and $\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\cdot\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix} = \begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}$. Notice that the determinant of $\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} = -1 = 1$ in $\mathbb{F}_2$, and $\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}$ has determinant also $-1 = 1$ in $\mathbb{F}_2$, so they are invertible. ($2 = 0$ in this field)

4. If n is not prime, there exists positive integers (by definition) $a, b > 1$ such that $ab = n$. That is, $a \cdot b = 0$ in $\mathbb{Z}/n\mathbb{Z}$. If c were the multiplicative inverse of a in this group, $(c \cdot a) \cdot b = c \cdot 0 = 0$, or $b = 0$, a contradiction. Hence $\mathbb{Z}/n\mathbb{Z}$ is not a field.

11. (a). Let $X = \begin{pmatrix}1 & a & b\\ & 1 & c\\ & & 1\end{pmatrix}$ and $Y = \begin{pmatrix}1 & d & e\\ & 1 & f\\ & & 1\end{pmatrix}$ and one can compute that $XY = \begin{pmatrix}1 & a+d & b+af+e\\ & 1 & c+f\\ & & 1\end{pmatrix}$, which is still in $H(F)$.

This form of XY is not symmetric in triples (a, b, c) and (d, e, f). Pick $a = 1, b = 0, c = 0$ and $d = 0, e = 0, f = 1$. Then in XY, $af = 1$ but in YX, $dc = 0$.

(b). Given $X = \begin{pmatrix}1 & a & b\\ & 1 & c\\ & & 1\end{pmatrix}$, we are looking for Y such that $a + d = 0$, $c + f = 0$, $b + af + e = 0$. We solve these to obtain

$Y = \begin{pmatrix}1 & -a & ac-b\\ & 1 & -c\\ & & 1\end{pmatrix}$.

(c). To show the associative law, you need to explicitly compute $(XY)Z$ and $X(YZ)$ and then observe that they are equal. A comment is that any such matrix determines a linear function on 3-dimensional vector space over $\mathbb{F}_2$ and since function composition corresponds to multiplying matrices (which is clearly associative), associativity of matrix multiplication is a trivial thing.

Section 1.6

2. If $\phi : G \to H$ is an isomorphism, $|\phi(x)| = |x|$ for all $x \in G$.

Proof. To begin with, assume that x has finite order of n, that is $x^n = e$ and $x^m \neq e$ for all $0 < m < n$. We claim that $\{\phi(x)\}^k = \phi(x^k)$ for all positive integer k. For $k = 1$, this is trivial and we then use induction; assume it holds for k. Then $\{\phi(x)\}^{k+1} = \{\phi(x)\}^k \cdot \phi(x) = \phi(x^k) \cdot \phi(x) = \phi(x^{k+1})$, so we are done. In particular, $\{\phi(x)\}^n = \phi(x^n) = \phi(e) = e$. If we assume that $\{\phi(x)\}^m = e$, it implies $\phi(x^m) = e$, but since ϕ is bijective, $x^m = e$. Therefore $0 < m < n$ is impossible, which shows $|\phi(x)| = n$.

Now we consider the case where x has infinite order. Assume $\phi(x)$ has finite order, say n. Then as above we can conclude that $x^n = e$, which shows $|x| \leq n$, a contradiction. □

This is not true if ϕ is not an isomorphism. For example, we always have a homomorphism sending every element in G to the identity in H.

3. Let us assume G is abelian. Then $\phi(g)\phi(h)\phi(g)^{-1}\phi(h)^{-1} = \phi(ghg^{-1}h^{-1}) = \phi(e) = e$, so $\phi(g)\phi(h) = \phi(h)\phi(g)$ for all $g, h \in G$. But from surjectivity of ϕ, for any elements $x, y \in H$ there exists g, h such that $\phi(g) = x$ and $\phi(h) = y$. That is, $xy = yx$ and H is abelian.

Now assume H is abelian. But $\phi^{-1} : H \to G$ exists and is another isomorphism, so above argument applies and G is abelian.

Now let us check what additional conditions are necessary on ϕ if it is only a homomorphism.

To show H is abelian when G is abelian, we only used the fact that ϕ is surjective. That is, if we have a surjective homomorphism $\phi : G \to H$ then G abelian implies H abelian.

On the other hand, to show G is abelian, we only needed the inverse map to be well-defined on the image of ϕ. That is, injectivity is enough.

4. Consider the equation $x^4 = 1$. In $\mathbb{C}\backslash\{0\}$ there are precisely four solutions. In $\mathbb{R}\backslash\{0\}$ there are precisely two solutions. An isomorphism, if existed, gives a bijective correspondence between solutions of this equation.

17. We need to check whether $\phi(g)\phi(h) = \phi(gh)$. Left hand side equals $g^{-1}h^{-1} = (hg)^{-1}$ and right hand side equals $(gh)^{-1}$. Therefore, we require $(hg)^{-1} = (gh)^{-1}$ for all $g, h \in G$, or equivalently, $hg = gh$. That is, ϕ is a homomorphism if and only if G is abelian. (indeed it will be isomorphism)

26. We want a group presentation of Q_8. One can check that $Q_8 =< i, j \,|\, i^4 = 1, i^2 = j^2, i^{-1}ji = j^{-1} >$. Then we define ϕ as a homomorphism from the Free Group on two elements $< i, j >$ and simply check that this homomorphism factors through relations

$$i^4 = 1, i^2 = j^2, i^{-1}ji = j^{-1},$$

which amounts to checking that

$$\phi(i)^4 = 1, \phi(i)^2 = \phi(j)^2, \phi(i)^{-1}\phi(j)\phi(i) = \phi(j)^{-1}.$$

Maybe this is the most efficient thing to do.

If you are not convinced that above is a presentation of Q_8, you better check that ϕ factors through all the relation given in page 36, namely $(-1) \cdot (-1) = 1$, $(-1) \cdot a = a \cdot (-1) = -a$, $i \cdot i = j \cdot j = k \cdot k = -1$, $i \cdot j = k$, ..., and so on, which I certainly do not want to do.