SKETCH OF SOLUTIONS (HOMEWORK III)

4. Suppose that for some $n \in \mathbb{Z}$, $a^n = e$. Then $a^{n-1}a = e$ so $a^{n-1} = a^{-1}$, therefore $(a^{-1})^n = (a^{n-1})^n = (a^n)^{n-1} = e$, but this implies that $|a^{-1}| \leq |a|$. Since $(a^{-1})^{-1} = a$ we get $|a| \leq |a^{-1}|$. The two inequalities imply $|a| = |a^{-1}|$. If a has infinite order a^{-1} must also have infinite order, otherwise, if $|a^{-1}| = n$ we can conclude with the same argument that $|a| \leq |a^{-1}| = n$, (contradiction).
5. Use exercise 4 and the fact that 2 is the inverse of 28 and 8 is the inverse of 22 (in $\mathbb{Z}_{30}$). Also in $U(15)$, 2 is the inverse of 8 and 7 is the inverse of 13.
6. Suppose $x^4 = e$ then
$$e = x^6 = x^2x^4 = x^2e = x^2!$$
Suppose $x^5 = e$ then
$$e = x^6 = xx^5 = xe = x!$$
The order of x must be ether 3 or 6
7. By exercise 2.32 we know that for $r_0 = R_{\frac{360}{n}}$ and any reflection f, $fr_0f = r_0^{-1}$, i.e. $fr_0 = r_0^{-1}f$. Since any rotation is of the form r_0^m we can show using induction that $fr = r^{-1}f$ for *any* rotation r. If n is even $R_{180} = r_0^{n/2}$. Since $R_{180} \circ R_{180} = R_{360} = id$ we get $r_0^{n/2} = (r_0^{n/2})^{-1}$ therefore $fr_0^{n/2} = r_0^{n/2}f$. Thus R_{180} commutes with all reflections. Clearly R_{180} commutes with all reflections since $R_a \circ R_b = R_{a+b} = R_{b+a} = R_b \circ R_a$.
8.
$$\begin{array}{lcl} \mathrm{U}(14) & = & \{1,3,5,9,11,13\} \\ <3> & = & \{1=3^0, 3=3^1, 5=3^5, 9=3^2, 11=3^4, 13=3^3\} \\ <5> & = & <3^{-1}>=<3> \\ <11> & = & <11^{-1}=9>=<3^2>=\{1=3^0, 9=3^2, 11=3^4\} \end{array}$$
$\therefore \mathrm{U}(14) =< 3 >=< 5 >\neq< 11 >$

12. $H =< \gcd(18,30,40) >=< 2 >$
14. (1) Since $e \in H$ and $e \in K$, $e \in H \cap K$. Therefore $H \cap K \neq \varnothing$.
    (2) Suppose $a, b \in H \cap K$ i.e. $a, b \in H$ and $a, b \in K$. Then $ab^{-1} \in H$ and $ab^{-1} \in K$ (since both H and K are subgroups) therefore $ab^{-1} \in H \cap K$.

    By the one-step test we get that $H \cap K$ is a subgroup.
23. Let $H = \{x \in G \mid x^n = e\}$
    (1) $e \in H$: Clear since $e^n = e$
    (2) $a, b \in H$ implies $ab^{-1} \in H$: Suppose $a^n = e$ and $b^n = e$. By exercise 4 we know that $(b^{-1})^n = e$ therefore $(ab^{-1})^n = a^n(b^{-1})^n = e$ (we have the first equality since G is abelian)

    For the example try D_4
29. In $\mathrm{SL}(2,\mathbb{R})$, $|A| = \infty$. In $\mathrm{SL}(2,\mathbb{Z}_p)$, $|A| = p$

32.

$$|x^2| = 3, |x^3| = 2, |x^4| = 3, |x^5| = 6$$

$$|y| = 9, |y^2| = 9, |y^3| = 3, |y^4| = 9, |y^5| = 9, |y^6| = 3, |y^7| = 9, |y^8| = 9$$

Relation: $|y^i| = \frac{|y|}{\gcd(i,|y|)} = \frac{\mathrm{lcm}(i,|y|)}{i}$

44. (1) $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in H$ since $\det I = 1 = 2^0$

(2) Suppose $A, B \in H$ i.e. $\det A = 2^a$ and $\det B = 2^b$ then $\det(AB^{-1}) = \det(A)\det(B^{-1}) = \det(A)\det(B)^{-1} = 2^a 2^{-b} = 2^{a-b}$ therefore $AB^{-1} \in H$

46. (1) $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) \equiv 1$ is in H

(2) Suppose $f, g \in H$, i.e. $f(1) = g(1) = 1$, then $f \cdot g^{-1}(1) = f \cdot \frac{1}{g}(1) = \frac{f(1)}{g(1)} = 1$ Thus $f \cdot g^{-1} \in H$

50. a $< 2 >$

b $\mathbb{Z}$

c $< 3 >$

d $< \gcd(m,n) >$

e $< 3 >$

51. a $\left\{ A = \begin{bmatrix} a+b & a \\ a & b \end{bmatrix} \mid a, b \in \mathbb{R},\ \det A = ab + b^2 - a^2 \neq 0 \right\}$

b $\left\{ A = \begin{bmatrix} a & b \\ b & a \end{bmatrix} \mid a, b \in \mathbb{R},\ \det A = a^2 - b^2 \neq 0 \right\}$

c $\left\{ A = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \mid a \in \mathbb{R},\ \det A = a^2 \neq 0 \right\}$