Algebra I, Fall 2016

Solutions to Problem Set 4

1. Let S_i ($i \in \mathbf{Z}$) be the element of $\oplus_{n\in\mathbf{Z}}\mathbf{Z}_2$ whose i-th component is 1 and the other components are zero. We show the two elements $(0,1)$ and $(S_0,0)$ generate the group. Let H be the subgroup generated by these two elements. It is enough to show for every integers n and m, $(S_m,n)\in H$. Of course $(0,l)\in H$ for every integer l, and we have

$$(S_0,0)(0,l)=(S_0,l),$$

so elements of the form (S_0,l) are in H, and

$$(0,m)(S_0,n-m)=(S_m,n).$$

2. Assume that H is a finite subgroup of $\mathbf{Q}/\mathbf{Z}$. First note that if $\frac{a}{b}+\mathbf{Z}\in H$ where $\gcd(a,b)=1$, then $\frac{1}{b}+\mathbf{Z}\in H$: since $gcd(a,b)=1$, there are integers x and y such that $ax+by=1$, so $\frac{xa}{b}+\mathbf{Z}=\frac{1}{b}+\mathbf{Z}$.

Now let

$$c_0=\max\{c:\frac{1}{c}+\mathbf{Z}\in H\}.$$

We show that H is generated by $\frac{1}{c_0}+\mathbf{Z}$. If $\frac{a}{b}+\mathbf{Z}$ is in H with $\gcd(a,b)=1$, then $\frac{1}{b}+\mathbf{Z}\in H$. It is enough to show c_0 is a multiple of b. Let $d=\gcd(c_0,b)$, then $c_0=c'd$ and $b=b'd$, and there are integers x and y such that $xc_0+yb=d$. Since $\frac{1}{b}+\mathbf{Z}\in H$ and $\frac{1}{c_0}+\mathbf{Z}\in H$,

$$\frac{1}{b'c_0}+\mathbf{Z}=(\frac{x}{b}+\frac{y}{c_0})+\mathbf{Z}\in H,$$

so $b'c_0\le c_0$, so $b'=1$, and b divides c_0.

Therefore, the only subgroup of $\mathbf{Q}/\mathbf{Z}$ of order n is the subgroup generated by $\frac{1}{n}+\mathbf{Z}$.

3. It is enough to prove the statement for finite abelian p-groups for a prime number p, since if $G\cong G_1\oplus\cdots\oplus G_m$ where G_i is a p_i-group and the p_i are distinct prime

numbers, and if $H \cong H_1 \oplus \cdots \oplus H_m$ where H_i is a p_i-group, then $H_i \leq G_i$, and $G/H \cong G_1/H_1 \oplus \cdots \oplus G_m/H_m$.

Assume G is a p-group, so G/H is a p-group too. Let

$$G \cong \mathbf{Z}_{p^{r_1}} \oplus \cdots \oplus \mathbf{Z}_{p^{r_n}} \qquad r_1 \geq \cdots \geq r_n,$$

and

$$G/H \cong \mathbf{Z}_{p^{d_1}} \oplus \cdots \oplus \mathbf{Z}_{p^{d_m}} \qquad d_1 \geq \cdots \geq d_m.$$

It is enough to show $r_i \geq d_i$ for every i, because in this case $\mathbf{Z}_{p^{r_i}}$ has a subgroup A_i isomorphic to $\mathbf{Z}_{p^{d_i}}$. (since they are both cyclic.), and $A = A_1 \oplus \cdots \oplus A_r$ is a subgroup of G which is isomorphic to G/H.

Now let G_k be the subgroup of G which consists of elements of order at most r_k, and let H_k/H be the subgroup of G/H which consists of elements of order at most r_k (so $G_k \subset H_k$). Then G/G_k is generated by at most $k-1$ elements. (corresponding to the cosets generated by the generators of the factors $\mathbf{Z}_{p^{r_1}}, \ldots, \mathbf{Z}_{p^{r_{k-1}}}$). Since the quotient of G/H by H_k/H is isomorphic to G/H_k and since there is an onto homomorphism $G/G_k \to G/H_k$, we conclude that the quotient of G/H by H_k/H is also generated by at most $k-1$ elements. So there are at most $k-1$ of the d_i which are larger than r_k, so $d_k \leq r_k$.

5. We first compute the number of elements in the group: The first column of a matrix in $GL(2, F)$ could be anything except for both entries zero so there are (p^2-1) possibilities. The second column now could be anything except for scalar multiples of the first column, that gives $p^2 - p$ choices of the second column for every first column. So the total number is $(p^2-1)(p^2-p)$, so a p-Sylow subgroup has order p. Now it is easy to see matrices of the form

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \qquad a \in F$$

form a subgroup of order p.

6. Assume G is a non-cyclic group of order $2p$. We can assume $p \neq 2$. Let a be an element of order p and let b be an element of order 2. Then

$$e, a, a^2, \ldots, a^{n-1}, b, ab, a^2b, \ldots, a^{n-1}b$$

are all distinct (note that every $a^i, 1 \leq i \leq n-1$ has order p, and so $a^i b \neq a^j$ for every i and j since otherwise, $b = a^{j-i}$). So they form all the elements of G. To show that G is isomorphic to D_{2p}, it is enough to show that $ba = a^{n-1}b$. Then the morphism $\phi : G \to D_{2p}$, $\phi(a^i) = \omega^i$ and $\phi(b) = r$ would be a group homomorphism.

Of course, ba cannot be equal to any of the a^i. Assume $ba = a^i b$. Then the order of ba is either p or 2. If the order of ba is 2, then we have

$$e = (ba)(ba) = (a^i b)(ba) = a^{i+1},$$

so $i = n - 1$. If the order of ba is $p = 2k$, then

$$e = (ba)^p = (ba)(a^i bba)^k = baa^{(i+1)k} = ba^{1+(i+1)k}.$$

Therefore, b is equal to a power of a which is not possible.