Lecture 7

5.2

The fundamental theorem of abelian groups is one of the basic theorems in group theory and was proven over a century before the more general theorem we will not cover of which it is a special case. Basically, the theorem says that, given a finitely generated abelian group, it can be written uniquely as a finite product of $\mathbb{Z}$s and a finite product of finite groups of one of two types.

Please ignore the discussion of Sylow theorems and p-groups. We skipped that chapter and the discussion doesn't really add to understanding even if we had done the Sylow theorems.

The big part of this chapter is finding all possible finite abelian groups of a particular order and writing them in one of two ways. The invariant factor way has the advantage that it is truly unique, but harder to compute all of them. The elementary divisor way is unique only up to the order of the factors but is much easier to be sure you have all the possibilities. So I'm going to do problem 2, the invariant factor problem, and ask you to do problem 3. I'd prefer you do the computations from scratch rather than from my list (which might be wrong or incomplete as a way of getting you to decide what is right or simply because I computed wrong since this way is harder) and then convert to do the matching. You'll learn more that way.

5.2.2a: $270 = 2 \cdot 3^3 \cdot 5$. So the possibilities for n_1 are $2 \cdot 3^3 \cdot 5,\ 2 \cdot 3^2 \cdot 5,\ 2 \cdot 3 \cdot 5$. Then $n_2 = 1,\ 3,\ 3$, respectively, and $n_3 = 1,\ 1,\ 3$. These yield $\mathbb{Z}_{270},\ \mathbb{Z}_{90} \times \mathbb{Z}_3,\ \mathbb{Z}_{30} \times \mathbb{Z}_3 \times \mathbb{Z}_3$.

5.2.2b: $9801 = 3^4 11^2$. So the possibilities for n_1 are $3^4 11^2,\ 3^3 11^2,\ 3^3 11,\ 3^2 11^2,\ 3^2 11,\ 3 \cdot 11^2,\ 3 \cdot 11$. Then $n_2 = 1,\ 3,\ 3 \cdot 11,\ 3^2$ or $3,\ 3^2 11$ or $3 \cdot 11,\ 3,\ 3 \cdot 11$. Thus $n_3 = 1,\ 1, 1,\ 1$ or $3,\ 1$ or $3,\ 3,\ 3$. Finally, $n_4 = 1,\ 1,\ 1,\ 1,\ 1,\ 3,\ 3$. These yield $\mathbb{Z}_{9801},\ \mathbb{Z}_{3267} \times \mathbb{Z}_3,\ \mathbb{Z}_{297} \times \mathbb{Z}_{33},\ \mathbb{Z}_{1089} \times \mathbb{Z}_9,\ \mathbb{Z}_{1089} \times \mathbb{Z}_3 \times \mathbb{Z}_3,\ \mathbb{Z}_{99} \times \mathbb{Z}_{99},\ \mathbb{Z}_{99} \times \mathbb{Z}_{33} \times \mathbb{Z}_3,\ \mathbb{Z}_{363} \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3,\ \mathbb{Z}_{33} \times \mathbb{Z}_{33} \times \mathbb{Z}_3 \times \mathbb{Z}_3$.

5.2.2c: $320 = 2^6 5$. So the possibilities for n_1 are $2^6 5,\ 2^5 5,\ 2^4 5,\ 2^3 5,\ 2^2 5,\ 2 \cdot 5$. Then $n_2 = 1,\ 2,\ 2^2$ or $2,\ 2^3$ or 2^2 or $2,\ 2^2$ or $2,\ 2$. Thus $n_3 = 1,\ 1,\ 1$ or 2, 1 or 2^2 or $2,\ 2^2$ or 2^2 or $2,\ 2$. Therefore, $n_4 = 1,\ 1,\ 1,\ 1,\ 1, 1$ or 1 or 2, 1 or 2 or $2,\ 2$. Lastly, n_5 is 1 until the last two which are 2, and n_6 is 1 until the last one which is 2. These correspond to $\mathbb{Z}_{320},\ \mathbb{Z}_{160}\times\mathbb{Z}_2,\ \mathbb{Z}_{80}\times\mathbb{Z}_{2^2}$ or $\mathbb{Z}_{80}\times\mathbb{Z}_2\times\mathbb{Z}_2,\ \mathbb{Z}_{40}\times\mathbb{Z}_{2^3}$ or $\mathbb{Z}_{40}\times\mathbb{Z}_{2^2}\times\mathbb{Z}_2$ or $\mathbb{Z}_{40}\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2,\ \mathbb{Z}_{20}\times\mathbb{Z}_{2^2}\times\mathbb{Z}_{2^2}$ or $\mathbb{Z}_{20}\times\mathbb{Z}_{2^2}\times\mathbb{Z}_2\times\mathbb{Z}_2$ or $\mathbb{Z}_{20}\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2,\ \mathbb{Z}_{10}\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$.

5.2.2d: $105 = 3\cdot 5\cdot 7 = n_1$. Therefore the only abelian group of order 105 is $\mathbb{Z}_{105}$.

5.2.2e: $44100 = 2^2 3^2 5^2 7^2$. So the possibilites for n_1 are $2^2 3^2 5^2 7^2,\ 2\cdot 3^2 5^2 7^2,\ 2^2 3\cdot 5^2 7^2,\ 2^2 3^2 5\cdot 7^2,\ 2^2 3^2 5^2 7,\ 2\cdot 3\cdot 5^2 7^2,\ 2\cdot 3^2 5\cdot 7^2,\ 2\cdot 3^2 5^2 7,\ 2^2 3\cdot 5\cdot 7^2,\ 2^2 3\cdot 5^2 7,\ 2^2 3^2 5\cdot 7,\ 2\cdot 3\cdot 5\cdot 7^2,\ 2\cdot 3\cdot 5^2 7, 2\cdot 3^2 5\cdot 7,\ 2^2 3\cdot 5\cdot 7,\ 2\cdot 3\cdot 5\cdot 7$. Thus $n_2 = 1,\ 2,\ 3,\ 5,\ 7,\ 6,\ 10, 14,\ 15,\ 21,\ 35,\ 30,\ 42,\ 70,\ 105,\ 210$. These correspond to $\mathbb{Z}_{44100},\ \mathbb{Z}_{22050}\times\mathbb{Z}_2,\ \mathbb{Z}_{14700}\times\mathbb{Z}_3,\ \mathbb{Z}_{8820}\times\mathbb{Z}_5,\ \mathbb{Z}_{6300}\times\mathbb{Z}_7, \mathbb{Z}_{7350}\times\mathbb{Z}_6,\ \mathbb{Z}_{4410}\times\mathbb{Z}_{10},\ \mathbb{Z}_{3150}\times\mathbb{Z}_{14},\ \mathbb{Z}_{2940}\times 15,\ \mathbb{Z}_{2100}\times\mathbb{Z}_{21},\ \mathbb{Z}_{1260}\times\mathbb{Z}_{35},\ \mathbb{Z}_{1470}\times\mathbb{Z}_{30},\ \mathbb{Z}_{1050}\times\mathbb{Z}_{42},\ \mathbb{Z}_{630}\times\mathbb{Z}_{70},\ \mathbb{Z}_{420}\times\mathbb{Z}_{105},\ \mathbb{Z}_{210}\times\mathbb{Z}_{210}$.

5.2.5: Let G be a finite abelian group of type $\{n_1, n_2, \dots, n_t\}$. Suppose G contains an element of order m. If m does not divide the order of n_1, then the order of m is divisible by a prime to an power s greater than the power t that prime divides n_1. Thus G contains a cyclic group of order p^s, which contradicts the corresponding elementary factor decomposition. Thus, m divides n_1.

Conversely, if m divides n_1, then the invariant factor $\mathbb{Z}_{n_1}$ contains a cyclic subgroup H of order m, whence G has an element of order m, namely any generator of H.

5.2.8: Let A be a finite abelian group written multplicatively, and let p be a prime. Define

$$A^p = \{a^p | a \in A\} \text{ and } A_p = \{x | x^p = 1\}. \qquad (1)$$

Thus A^p and A_p are the image and kernel of the p^{th}-power map, respecitvely.

5.2.8a: By definition A_p is an elementary abelian group. If $xA^p \in A/A^p$, then $(xA^p)^p = x^p A^p = 1A^p$ so the order of xA^p divides p. Thus A/A^p is an elementary abelian group as well. By 5.1.7c, they both have order p^n, so they are isomorphic to E_{p^n} and thus to each other.

5.2.8b: By the fundamental theorem of abelian groups, $A = H \times K$ where H is an abelian p-group and the order of K is not divisible by p. Thus all subgroups of order p are subgroups of $H \times \{1\}$ and all subgroups of index p are subgroups of of H direct product all of K. Therefore, we may assume that $K = \{1\}$ and $A = H$ is an abelian $p-group$ as well. Consider A written as a product of elementary factors $\mathbb{Z}_{p^{s_1}} \times \cdots \times \mathbb{Z}_{p^{s_t}}$. Every element of order p has either 1 or an element of order p in each factor. Every subgroup of index p has elements of order $p^{s_i - 1}$ in the ith factor. Since there are $p-1$ elements of order p in each factor and $p-1$ elements of order $p^{s_i} - 1$ in each factor, there are the same number of subgroups of order p as there are of index p.

7.1

In chapter 7 we are starting a new topic, namely, rings. Section 1 contains the basic definitions, simple propositions, and lots of examples. Since Proposition 1 was not completely proven, I will complete the proof.

Proposition 1 (3): By (2), $(-a)(-b) = a(-(-b)) = ab$ by Chapter 1, Proposition 1 (3).

Proposition 1 (4): Suppose R has an identity 1 and another $1'$. Then $1 = 1 \cdot 1' = 1'$. Therefore the identity is unique. Furthermore, $a + (-1)a = (1+(-1))a = 0 \cdot a = 0$, so by uniqueness of the additive inverse, $-a = (-1)a$.

The first few exercises are corollaries of Proposition 1 for a ring R with 1.

7.1.1: By Proposition 1 (3) with $a = 1 = b$, $(-1)^2 = (-1)(-1) = 1(1) = 1$.

7.1.2: Suppose u is a unit in R. Then there exists $v \in R$ such that $uv = 1 = vu$. Thus $(-u)(-v) = uv = 1 = vu = (-v)(-u)$. Therfore, $-u$ is a unit with inverse $-v$.

7.1.3: Let S be a subring of R containing the identity of R. Suppose $u \in S$ is a unit in S. Then there exists $v \in S$ such that $uv = 1 = vu$. Since $S \subseteq R$, $uv = 1 = vu \in R$. Therefore, u is a unit in R.

Let $R = \mathbb{Q}$ and $S = \mathbb{Z}$. Then $2 \in R$ is a unit in R but is not a unit in S because $1/2 \notin S$.

Just to help out with more proofs, I'll do another few problems.

7.1.7: The center $C(R)$ of a ring R is $\{z \in R | zr = rz \ \forall r \in R\}$. Since $1r = r = r1 \ \forall r \in R, 1 \in C(R)$ and $C(R)$ is not empty. Suppose $a, b \in C(R)$. Then, for all $r \in R$, $(a + b)r = ar + br = ra + rb = r(a + b)$, whence

$a + b \in C(R)$. Also, $abr = arb = rab$, so $ab \in C(R)$. Therefore C(R) is a subring of R.

Suppose R is a division ring. If $a \in C(R)$, then $a^{-1}r = (r^{-1}a)^{-1} = (ar^{-1})^{-1} = ra^{-1}$ $\forall r \in R$. Therefore, $a^{-1} \in C(R)$. Since $ar = ra$ $\forall r \in R$, $ar = ra$ $\forall r \in C(R)$. Thus $C(R)$ is commutative, whence a field.

7.1.8: If $a+bi+cj+dk \in C(\mathbb{H})$, then $(a+bi+cj+dk)(xj) = axj+bxk-cx-dxi$ and $(xj)(a+bi+cj+dk) = axj - bxk - cx + dxi$, whence $bxk = -bxk$ and $dxi = -dxi$, so $b = 0 = d$. Similarly, $(a+cj)(xi) = axi-cxk = (xi)(a+cj) = axi + cxk$, whence $c = 0$. Therefore $C(\mathbb{H}) = \{a|a \in \mathbb{R}\}$.

Let $S = \{a + bi|a, b \in \mathbb{R}\}$. Since $1 + 0i \in S$, S is not empty. $a + bi + c + di = a + c + (b + d)i \in S$ and $(a + bi)(c + di) = ac - bd + (ad + bc)i \in S$. Therefore, S is a subring of $\mathbb{H}$. Since $(c + di)(a + bi) = ac - bd + (ad + bc)i$, S is commutative but not in the center of $\mathbb{H}$.

7.1.11: Suppose R is an integral domain and that $x^2 = 1$ for some $x \in R$. Then $0 = x^2 - 1 = (x - 1)(x + 1)$. Since R is an integral domain, either $x - 1 = 0$ or $x + 1 = 0$. Therefore, $x = \pm 1$.

7.2

Polynomials and matrices are familiar, but in this section we put other things than numbers in our matrices. For example, we might put polynomial over the reals as entries in our matrices. But the big new thing is group rings. One of the famous group rings is the real quaternions. Recall the quternion group, Q, has 8 elements, $\pm 1, \pm i, \pm j, \pm k$. We can form the real quaternions, $\mathbb{R}Q$ by using the distributive law, the usual rules for the reals, and the multiplication in Q. For example, $(3i-j)(3i+j) = 9i^2+3ij-3ji-j^2 = -9+3k+3k+1 = -8 + 6k$. Notice that we had to be careful in our multiplication because Q is not commutative. It would have been tempting, but wrong, to say $(3i - j(3i + j) = 9i^2 - j^2$ because $ij \neq ji$.

7.2.11 Since our ring is $\mathbb{Z}/3\mathbb{Z}$, $\alpha = (2\ 3) + 2(1\ 2\ 3)$ and $\beta = 2(2\ 3) - (1\ 2\ 3)$. Note that the $\mathbb{Z}/3\mathbb{Z}$ has no effect on the cycles in S_3.

7.2.11.a $\alpha + \beta = (1\ 2\ 3)$.

7.2.11.b $2\alpha - 3\beta = 2\alpha = 2(2\ 3) + (1\ 2\ 3)$.

7.2.11.c $\alpha\beta = ((2\ 3) + 2(1\ 2\ 3))(2(2\ 3) - (1\ 2\ 3)) = 2(2\ 3)^2 - (2\ 3)(1\ 2\ 3) + (1\ 2\ 3)(2\ 3) - 2(1\ 2\ 3)^2 = 2 - (1\ 3) + (1\ 2) - 2(1\ 3\ 2)$.

7.2.11.d $\beta\alpha = (2(2\ 3) - (1\ 2\ 3))((2\ 3) + 2(1\ 2\ 3)) = 2(2\ 3)^2 + (2\ 3)(1\ 2\ 3) - (1\ 2\ 3)(2\ 3) - 2(1\ 2\ 3)^2 = 2 + (1\ 3) - (1\ 2) - 2(1\ 3\ 2)$.

7.2.11.e $\alpha^2 = ((2\ 3) + 2(1\ 2\ 3))((2\ 3) + 2(1\ 2\ 3)) = (2\ 3)^2 + 2(2\ 3)(1\ 2\ 3) + 2(1\ 2\ 3)(2\ 3) + (1\ 2\ 3)^2 = 1 + 2(1\ 3) + 2(1\ 2) + (1\ 3\ 2)$.