Selected problems from Dummit and Foote

Drewseph

1.1: Problems 29

To any $(a_1,b_1),(a_2,b_2) \in A \times B$, $(a_1,b_1)\cdot(a_2,b_2) = (a_1a_2, b_1b_2) = (a_2a_1, b_2b_1) = (a_2,b_2)\cdot(a_1,b_1)$ since A,B are abelian, which leads to $a_1a_2 = a_2a_1$, $b_1b_2 = b_2b_1$. Thus $A \times B$ is abelian.

1.2: Problems 10

There are 8 vertices, so any vertex, say t has 8 potential places to be rotated to. And any vertex adjacent to t, say x has to be rotated to a vertex which is adjacent to the vertex that t rotates to, thus x has 3 places to go. Hence there are exactly $8 \times 3 = 24$ rigid motions, in other words, $|G| = 24$.

1.3: Problems 17

We just need to figure out how many choices we have if we pick up 4 elements for two groups with 2 elements each group. First, if arbitrarily pick up 4 elements, there are $C_4^n = \frac{n(n-1)(n-2)(n-3)}{4!} = \frac{n(n-1)(n-2)(n-3)}{24}$. Second, if we separate 4 elements into 2 groups with 2 elements each group, then there are $C_4^2/2 = 3$ choices. So there are $C_4^n \times C_4^2/2 = \frac{n(n-1)(n-2)(n-3)}{24} \times 3 = \frac{n(n-1)(n-2)(n-3)}{8}$ choices.

1.3: Problems 20

$S_3 = \{(1),(23),(12),(13),(123),(132)\}$. Note $(123)^2 = (132), (123)^3 = (1)$, $(123)(12) = (23), (12)(123) = (13), (123)(23) = (13), (123)(13) = (12)$, $(23)^2 = (13)^2 = (12)^2 = (1)$, also by above we can get: $(123)^{-1}(12) = (12)(123)$

Since $(12),(123)$ can generate any elements, we can set the generators can be $(12),(123)$. The relations are $(12)^2 = (1), (123)^3 = (1)$, $(123)^{-1}(12) = (12)(123)$.

1.4: Problems 11

(a)

By $XY = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & d+a & e+af+b \\ 0 & 1 & f+c \\ 0 & 0 & 1 \end{pmatrix}$,

we get $H(F)$ is closed under matrix multiplication.

Since $YX = \begin{pmatrix} 1 & d+a & e+dc+b \\ 0 & 1 & f+c \\ 0 & 0 & 1 \end{pmatrix}$,
and we may not always have $af = dc$, thus we may not always have $XY = YX$. For example, for the case that $a = b = c = 1$, $d = e = 1, f = 2$.

(b)
By the expression of XY, we know that if $XY = id$, then we have $d + a = f + c = e + af + b = 0$, i.e. $d = -a, f = -c, e = ac - b$, i.e.

$$X^{-1} = \begin{pmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix}.$$

(c)
Define $Z := \begin{pmatrix} 1 & g & h \\ 0 & 1 & i \\ 0 & 0 & 1 \end{pmatrix}$, then $(XY)Z = \begin{pmatrix} 1 & d+a & e+af+b \\ 0 & 1 & f+c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & g & h \\ 0 & 1 & i \\ 0 & 0 & 1 \end{pmatrix}$
$= \begin{pmatrix} 1 & d+a+g & h+e+af+b+(d+a)i \\ 0 & 1 & f+c+i \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & d+g & e+di+h \\ 0 & 1 & f+i \\ 0 & 0 & 1 \end{pmatrix}$=X(YZ).
So $H(F)$ satisfies the associative law, thus $H(F)$ is a group. Since each element has three entries, each entry can have $|F|$ choices, thus $|H(F)| = |F|^3$.

(d)
When $F = \mathbb{Z}/2\mathbb{Z}$, each entry can only be 0 or 1. Obviously, the order of the identity is 1.
By $XX = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2a & 2b+ac \\ 0 & 1 & 2c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & ac \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$,

thus any non-trivial element with $a = 0$ or $c = 0$ is of order 2, therefore the order of $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ is 2.
$\begin{pmatrix} 1 & 1 & b \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}^4 = \begin{pmatrix} 1 & 1 & b \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}^2 \begin{pmatrix} 1 & 1 & b \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = id.$
Thus $\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ has order 4.

(e)

By $XY = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & d+a & e+af+b \\ 0 & 1 & f+c \\ 0 & 0 & 1 \end{pmatrix}$,
we know the middle entry of the first row of XY is the sum of the middle entry of the first row of X and the middle entry of the first row of Y. Thus to any $X = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \in H(\mathbb{R})$, the middle entry of the first row of X^n is na. Similarly, the right entry of the second row of X^n is nc. It means if X has finite order, then $a = c = 0$, so if X has finite order, then $X = \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. By the expression of XY, we can get
$\begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & e \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & e+b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, which implies $\begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & 0 & nb \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, it means if X has finite order then $X = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. So every nonidentity element of the group $H(\mathbb{R})$ has infinite order.

1.5: Problems 3

By the relations, we can get $Q_8 =< i, j, k | i^2 = j^2 = k^2 = -1, ij = k, ji = -k, jk = i, kj = -i, ki = j, ik = -j >$

1.6: Problems 25

(a) We just need to prove, to any unit vector h, the matrix rotates the unit vector about the origin in a counterclockwise direction by θ radians. Without losing the generality, we may just assume the unit vector to be $(1,0)^T$, which lies on the positive half x-axis. Then $\begin{pmatrix} cos\theta & -sin\theta \\ sin\theta & cos\theta \end{pmatrix} \cdot h^T = \begin{pmatrix} cos\theta \\ sin\theta \end{pmatrix}$, which is the unit vector with the angle θ with the positive half x-axis. So the matrix rotates the unit vector h^T about the origin in a counterclockwise direction by θ radians.

(b) By the words at the bottom of P.38, we just need to verify that the relations are kept in the image of the generators. So just need to verify if $\phi(r)^n = id$, $\phi(s)^2 = id$, $(\phi(s)\phi(r))^2 = id$.

First, $\phi(s)^2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = id$.

Second, note $\begin{pmatrix} cos\theta & -sin\theta \\ sin\theta & cos\theta \end{pmatrix} \cdot \begin{pmatrix} cos\beta & -sin\beta \\ sin\beta & cos\beta \end{pmatrix} = \begin{pmatrix} cos\theta cos\beta - sin\theta sin\beta & -cos\theta sin\beta - sin\theta cos\beta \\ cos\theta sin\beta + sin\theta cos\beta & cos\theta cos\beta - sin\theta sin\beta \end{pmatrix}$
$= \begin{pmatrix} cos(\theta+\beta) & -sin(\theta+\beta) \\ sin(\theta+\beta) & cos(\theta+\beta) \end{pmatrix}$, it implies that $\begin{pmatrix} cos\theta & -sin\theta \\ sin\theta & cos\theta \end{pmatrix}^n = \begin{pmatrix} cosn\theta & -sinn\theta \\ sinn\theta & cosn\theta \end{pmatrix} =$

id, in other words, $\phi(r)^n = id$.

Third, $(\phi(s)\phi(r))^2 = \begin{pmatrix} sin\theta & cos\theta \\ cos\theta & -sin\theta \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = id$. That finishes the proof.

(c) By $\begin{pmatrix} cos\theta & -sin\theta \\ sin\theta & cos\theta \end{pmatrix} \cdot \begin{pmatrix} cos\beta & -sin\beta \\ sin\beta & cos\beta \end{pmatrix} = \begin{pmatrix} cos(\theta+\beta) & -sin(\theta+\beta) \\ sin(\theta+\beta) & cos(\theta+\beta) \end{pmatrix}$ it implies that $\begin{pmatrix} cos\theta & -sin\theta \\ sin\theta & cos\theta \end{pmatrix}^m = \begin{pmatrix} cosm\theta & -sinm\theta \\ sinm\theta & cosm\theta \end{pmatrix}$. Thus by the definition of θ, $\phi(\theta^m) = \phi(\theta)^m = id$ iff $m = n$. And $\phi(r^m s) = \phi(r^m)\phi(s) = \begin{pmatrix} cosm\theta & -sinm\theta \\ sinm\theta & cosm\theta \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -sinm\theta & cosm\theta \\ cosm\theta & sinm\theta \end{pmatrix}$, which is never trivial. And recall $D_{2n} = \{1, r, r^2, ..., r^{n-1}, s, rs, ..., r^{n-1}s\}$, thus only $\phi(1) = id$. Thus ϕ is injective.

1.7: Problems 12

Define the set consisting of pairs of opposite vertices of a regular n-gon as A. By the definition of group action, we need to show any $h, g \in D_{2n}, a \in A$, $g \cdot a \in A$, $1 \cdot a = a$, $h \cdot (g \cdot a) = (gh) \cdot a$.

Since 1 doesn't make any change to the n-gon, thus $1 \cdot a = a$, for any $a \in A$. And any element of A is a combination of s, r, thus in order to show $g \cdot a \in A$, we just need to show $s \cdot a \in A$, $r \cdot a \in A$. We may define the vertices clockwise as $0, 1, 2, ..., n-1$. Let the $n/2$ pairs of opposite vertices defined to be $a_i := \{i, i+n/2\}, 0 \leq i < n/2$. If we define $r(j) = j - 1 \mod n$ with $0 \leq j \leq n-1$, then we get $r(i) = i - 1$, if $i \geq 1$ and $r(0) = n - 1$. Then to any pair $(i, i+n/2)$ with $0 < i < n/2$, $r(i) = i - 1, r(i + n/2) = i - 1 + n/2$, i.e. $r(i, i+n/2) = (i-1, i-1+n/2) = a_{i-1} \in A$. To $(0, n/2)$, $r(0) = n-1$, $0 < r(n/2) = n/2 - 1 < n/2$, thus $r(0, n/2) = (n/2 - 1, n - 1) \in A$. Thus we can conclude $r(a_i) = a_{i-1 \mod n/2}$. And we define the reflection is about the line connecting vertices $0, 3$, thus $s(j) = -j \mod n$, thus to any a_i, $s(i) = -i \mod n = n - i, s(i + n/2) = n/2 - i$, thus $s(a_i) = (n/2 - i, n - i) = a_{-i \mod n/2}$. Thus we have proved $s \cdot a \in A$, $r \cdot a \in A$ for any $a \in A$, therefore $g \cdot a \in A$, for any $g \in D_{2n}, a \in A$.

Since any $g \in D_{2n}$ is in the form of $r^i s^j$, we just need to show $(r^a s^b) \cdot ((r^x s^y) \cdot a_i) = ((r^a s^b)(r^x s^y)) \cdot a_i$. Indeed, by computation, we can get

$$((r^a s^b)(r^x s^y)) \cdot a_i = (r^{a+(-1)^b x} s^{b+y}) \cdot a_i = a_{-1^{y+b} i + (-1)^{b+1} x - a \mod n/2} = r^a s^b \cdot a_{-1^y i - x \mod n/2}$$

Thus it is an action.

Since $r^x s^y \cdot a_i = a_{-1^y i - x \mod n/2}$, thus if $r^x s^y \cdot a_i = a_i$, then $x = n/2, 0, y = 0$, if $y = 1$, then x depends on i, thus if $r^x s^y \cdot a_i = a_i$ for any i, then $y = 0, x = n/2, 0$. In other words, kernel is $\{r^0 = 1, r^{n/2}\}$.

1.7: Problems 20

Note tetrahedron has 4 vertices, say $1, 2, 3, 4$, so any element from the group of rigid motions (say G) can be seen as a permutation of the 4 vertices, thus it can be seen as an element of S_4. Thus it induces a map $\phi : G \to S_4$ Given $g, h \in G$, $\phi(gh)$ denotes the permutation resulting from performing h and then g. This is the same as performing the rigid motion h first, writing down the permutation $\phi(h)$, then performing the rigid motion g, writing down the permutation $\phi(g)$, and then multiplying the permutations $\phi(g)\phi(h)$. In other words, ϕ is a group homomorphism. Since different rigid motions are mapped to different permutations by definition, thus ϕ is injective, thus ϕ induces an isomorphism between G and a subgroup of S_4.

2.1: Problems 15
$\cup_{i=1}^{\infty} H_i$. And to any $a \in \cup_{i=1}^{\infty} H_i \neq \emptyset$, since $\emptyset \neq H_i \subset \cup_{i=1}^{\infty} H_i$. To any $a, b \in \cup_{i=1}^{\infty} H_i$ exists i, j s.t. $a \in H_i$, $b \in H_j$. Without losing generality, we may assume $i \leq j$, thus $H_i \subset H_j$. Thus $a, b, b^{-1}, a^{-1} \in H_j$, thus $ab^{-1}, ba^{-1} \in H_j \subset \cup_{i=1}^{\infty} H_i$. By the criterion of the subgroup, $\cup_{i=1}^{\infty} H_i$ is a subgroup of G.

2.2: Problems 10
(1) Assume $H = \{1, h\}$. If $g \in N_G(H)$, then $g1g^{-1} = gg^{-1} = 1$, $ghg^{-1} \in H$, note $ghg^{-1} \neq 1$, since otherwise, $gh = g$, which implies $h = 1$, contradiction. Therefore $ghg^{-1} = h$. Hence, if $g \in N_G(H)$, then $g \in C_G(H)$, thus $N_G(H) \subset C_G(H)$. And by definition of $C_G(H)$, to any $g \in C_G(H)$, since $g1g^{-1}, ghg^{-1} = h$, we have $gHg^{-1} = H$, thus $C_G(H) \subset N_G(H)$, thus $C_G(H) = N_G(H)$.

(2) Since $C_G(H) = N_G(H) = G$, any $g \in G$, $ghg^{-1} = h$, i.e. $gh = hg$. thus $h \in Z(G)$ and $1 \in Z(G)$, thus $H \leq Z(G)$.

2.3: Problems 13
(1) Note $(0, 1) \in \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, has order 2 $((0, 1) + (0, 1) = (0, 2) = (0, 0))$. While, in $\mathbb{Z}$, no element has finite order, while order is kept under isomorphism, thus $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is not isomorphic to $\mathbb{Z}$.

(2) Similarly, $(0, 1) \in \mathbb{Q} \times \mathbb{Z}/2\mathbb{Z}$, has order 2, however, in $\mathbb{Q}$, no element has finite order, while order is kept under isomorphism, thus $\mathbb{Q} \times \mathbb{Z}/2\mathbb{Z}$ is not isomorphic to $\mathbb{Q}$.

2.3: Problems 21
Note $\binom{p^{n-1}}{r}$ is an integer, thus by Binomial Theorem, $(1+p)^{p^{n-1}} = 1 + \binom{p^{n-1}}{1}p + \binom{p^{n-1}}{2}p^2 + \cdots + \binom{p^{n-1}}{n}p^n + \cdots + p^{p^{n-1}} \equiv 1 + \binom{p^{n-1}}{1}p + \binom{p^{n-1}}{2}p^2 + \cdots + \binom{p^{n-1}}{n-1}p^{n-1} \mod p^n$. Note $\binom{p^{n-1}}{r}p^r = \frac{p^{n-1}(p^{n-1}-1)\ldots(p^{n-1}-r+1)}{r(r-1)\ldots 1}p^r$. It can be proved that, when prime $p > 2$, then $p^{n-r} | \binom{p^{n-1}}{r}$, thus $p^n | \binom{p^{n-1}}{r}p^r$, thus $1 + \binom{p^{n-1}}{1}p + \binom{p^{n-1}}{2}p^2 + \binom{p^{n-1}}{n-1}p^{n-1} \equiv 1 \mod p^n$. Therefore $(1+p)^{p^{n-1}} \equiv 1 \mod p^n$.
Similarly, $(1+p)^{p^{n-2}} = 1 + \binom{p^{n-2}}{1}p + \binom{p^{n-2}}{2}p^2 + \cdots + \binom{p^{n-2}}{n}p^n + \cdots + p^{p^{n-2}} \equiv 1 + \binom{p^{n-2}}{1}p +$

$\binom{p^{n-2}}{2}p^2 + \cdots \binom{p^{n-2}}{n-1}p^{n-1} \mod p^n$. And it can be proved that when prime $p > 2$, then $p^n | \binom{p^{n-2}}{r}p^r$, thus $(1+p)^{p^{n-2}} \equiv 1+\binom{p^{n-2}}{1}p \mod p^n \equiv 1+p^{n-1} \mod p^n$.Thus $(1+p)^{p^{n-2}} \not\equiv 1 \mod p^n$.

Note $\mathbb{Z}/p^n\mathbb{Z}^* \cong \mathbb{Z}/p^{n-1}(p-1)\mathbb{Z}$, thus the order of $1+p$ divides $p^{n-1}(p-1)$. By above, we have the order of $1+p$ divides p^{n-1} (it implies the order is in the form of p^t), but not p^{n-2}. Thus the order of $1+p$ is in the form of p^t, but $t > n-2$, since otherwise by $p^t | p^{n-2}$, we have $(1+p)^{p^{n-2}} \equiv 1 \mod p^n$, contradiction. Thus the order of $1+p$ is p^{n-1}.

2.4: Problems 17

(a) This part is direct from 2.1: Problems 15.

(b) Since C is a nontrivial chain thus H is non-trivial. We need to show $H \neq G$: If not, each g_j must lie in H and so must lie in some element of the chain C. Then we have at most n elements in the chain with each one contains a g_j, and we can select the largest group say $T \subset H$, s.t. $g_1, ...g_n \in T$. Then $T = G$. Thus T is not proper, contradiction. Hence $H \neq G$, thus H is proper.

(c) To any chain C of proper subgroups with oder via inclusion, we have a upperbound H. H is the upperbound since by (b) H is proper,and by (a), any elements is included in H. Thus by Zorn's Lemma, S has a maximal element.

2.5: Problems 14

Solution: (1) Since the order of v is 8 by the presentation, it's immediately to get $< v > \cong \mathbb{Z}_8$. By $vu = uv^5$, we have $vuv^5 = uv^{10} = uv^2$, thus $v(vu) = uv^2$, i.e. $v^2u = uv^2$, in other words, v^2, u commutes, thus $< u, v^2 >$ is abelian. Also u, v^2 are generators in $< u, v^2 >$ with order 2 and 4 respectively. Thus $< u, v^2 > \cong \mathbb{Z}_2 \times \mathbb{Z}_4$. Note $(uv)^2 = u(vu)v = u(uv^5)v = u^2v^6 = v^6$, which has order 4, thus uv has order 8. Thus $< uv > \cong \mathbb{Z}_8$.

(2) By $vu = uv^5$, the elements of M are in the form of v^i or uv^j, we may use them to determine the subgroups.

Note $(uv^2)^2 = u(v^2u)v^2 = u^2v^2v^2 = v^4$, Thus $< uv^2 >$ is cyclic with order 4. Observe $< uv^2 > \ni (uv^2)^3 = uv^6$, thus $< uv^2 > = < uv^6 >$.

Note $(uv^4)^2 = 1$, thus $< uv^4 >$ is a group of order 4, contained in the group $< u, v^4 >$ with order 4.

Note $(vu)^2 = (uv^5)^2 = v^6$, thus $< vu >$ has a subgroup $< v^6 >$ with order 4, and $< v^6 >$ has a subgroup $< v^4 >$ of order 2.

Note $(uv)^2 = u(vu)v = u(uv^5)v = v^6$, which has order 4, thus the order of uv is 8, hence $< uv >$ has order 8. Thus $< uv > = (vu >$, similarly, for uv^3, uv^7.

Now it's easy to see that $< v >$ has subgroups $< v^2 >$ with order 4, $< v^4 >$ with order 2. $< u, v^2 >$ has 3 possible proper subgroups generated by u, $(v^2)^i, i \neq 4$: $< u, v^4 >, < uv^2 > = < uv^6 >$, $< u, v^6 >$, however, $< u, v^6 > = < u, v^2 >$. And $< uv^2 >$ is a cyclic group with order 2 with subgroup $< v^4 >$.

So the lattice of subgroups of M is:

So we can conclude that the lattice of subgroups of M is the same as the lattice of subgroups of $\mathbb{Z}_2 \times \mathbb{Z}_8$. But they are not isomorphic since $\mathbb{Z}_2 \times \mathbb{Z}_8$ is abelian while M is not abelian as $uv \neq vu$.

3.1: Problems 34
Solution: (a) Recall, the elements of D_{2n} are in the form of r^j, sr^i. To any element $(r^k)^i \in < r^k >$, we have $r^j((r^k)^i)(r^j)^{-1} = (r^k)^i$. And $sr^i(r^k)^i(sr^i)^{-1} = sr^i(r^k)^i r^{-i}s^{-1} = s(r^k)^i s = r^{-ik} = r^{n-ki}$. Since $i|n$, $i|(n-ki)$, thus $r^{n-ki} = (r^k)^j$ for some j, therefore $sr^i(r^k)^i(sr^i)^{-1} \in < r^k >$. Thus $< r^k >$ is normal.

(b) Note any $x \in D_{2n}/< r^k >$ is in the form of $\bar{r^j}, \overline{sr^i} = s\bar{r^i}$.Thus there are exactly k elements in the form of $\bar{r^j}$, and k elements in the form of $s\bar{r^i}$. It also implies that the generators are $\bar{r}$ and $\bar{s}$. And it's easy to see $\bar{r}^k = 1, \bar{s}^2 = 1$. Also $\bar{r}\bar{s} = \overline{rs} = \overline{sr^{-1}} = \bar{s}\overline{r^{-1}} = \bar{s}\bar{r}^{-1}$. Thus $D_{2n}/< r^k >$ and D_{2k} have the same presentation, thus they are isomorphic.

3.1: Problems 41
Solution: (1) Any element $[x,y] := xyx^{-1}y^{-1}$ has inverse $[y,x]$. And to any $[a_1,b_1]...[a_n,b_n]$, $[c_1,d_1]...[c_m,d_m] \in N$,$[a_1,b_1]...[a_n,b_n]([c_1,d_1]...[c_m,d_m])^{-1} = [a_1,b_1]...[a_n,b_n][d_m,c_m]...[d_1,c_1] \in N$, thus N is a subgroup.
To any $x := [a_1,b_1]...[a_n,b_n] \in N$, and $g \in G$, $gxg^{-1} = g[a_1,b_1]g^{-1}g...g^{-1}g[a_n,b_n]g^{-1} \in N$, since $g[a_i,b_i]g^{-1} = ga_ib_ia_i^{-1}b_i^{-1}g^{-1} = ga_ig^{-1}gb_ig^{-1}ga_i^{-1}g^{-1}gb_i^{-1}g^{-1} = [ga_ig^{-1}, gb_ig^{-1}]$.

(2) To any $\bar{x}, \bar{y} \in G/N$, we have $\bar{x}\bar{y} = \overline{xy} = \overline{xy} \cdot \bar{1} = \overline{xy}\overline{y^{-1}x^{-1}yx} = \overline{xyy^{-1}x^{-1}yx} = \overline{yx} = \bar{y}\bar{x}$. Therefore $\bar{x}\bar{y} = \bar{y}\bar{x}$. Thus G/N is abelian.

3.1: Problems 42
To any $x \in H, y \in K$, $xyx^{-1}y^{-1} = (xyx^{-1})y^{-1} \in K$, since by K is normal, $(xyx^{-1}) \in K$, thus $(xyx^{-1})y^{-1} \in K$. Similarly, by H is normal, $yx^{-1}y^{-1} \in H$, thus $xyx^{-1}y^{-1} \in H$, thus $xyx^{-1}y^{-1} \in H \cap K = 1$, i.e. $xyx^{-1}y^{-1} = 1, xy = yx$.

3.2: Problems 11
Assume $G = \coprod_{i \in I} g_i K$, $K = \coprod_{j \in J} k_j H$. Then $|I| = [G : K]$, $|J| = [K : H]$. So $G = \cup_{i,j} g_i k_j H$. If $g_i k_j H \cap g_m k_n H \neq \emptyset$, then there is an $h \in H$, s.t. $g_i k_j = g_m k_n h$, so $g_i = g_m(k_n h k_j^{-1}) \in g_m K$, thus $g_i K \cap g_m K \neq \emptyset$, contradiction. Therefore $G = \coprod_{i,j} g_i k_j H$, thus $[G : H] = |I||J|$, i.e. $[G : H] = [G : K][K : H]$.

3.2: Problems 19
If there is a subgroup H with $|H|$ and $|G : N|$ are relatively prime. To any $h \in H$, we consider $hN \in G/N$. Note since N is normal, G/N is a group with order $|G/N|$. Thus the order of hN divides $|G/N|$. Also the order of hN divides H. Since $|H|$ and $|G : N|$ are relatively prime, we get the order of hN has to be 1, which implies that $h \in N$, hence $H < N$. Now if there is a group H with order N, then we get $|H| = |N|$ and $|G : N|$ are relatively prime, since by assumption $(|N|, [G : N]) = 1$, thus $H < N$ by we just proved, and since $|H| = |N|$, we have $H = N$.

3.3: Problems 1
Consider the homomorphism $det : GL_n(F) \to F^*$, which is onto since to any $a \in F^*$, the matrix $(a_{i,j})$ with $a_{i.j} = 0$ if $i \neq j$, and $a_{i,j} = 1$ if $i = j \neq 1$, and $a_{1,1} = a$, would be mapped to a by det. And the kernel is just $SL_n(F)$. Thus $|GL_n(F)/SL_n(F)| = |F^*| = q - 1$.

3.3: Problems 7
Since $G = MN$, thus any $g \in G$ can be expressed as ab with $a \in M$, $b \in N$. And $ab/M = \bar{b}, ab/N = \bar{a}$. Consider the homomorphism $f : G \to (G/M) \times (G/N)$, by $f(g) \mapsto (gM \times gN)$. This is onto since to any $(aM \times bN) \in (G/M) \times (G/N)$, we may assume $a = mn$, $b = m'n'$ with $m, m' \in M, n, n' \in N$. Then $aM = nM, bN = m'N$. Thus $m'n \in MN = G$. Observe $f(m'n) = (nM \times m'N) = (aM \times bN)$. So we have shown that f is onto. And the kernel is exactly $M \cap N$.Thus $G/(M \cap N) \cong G/M \times G/N$.
3.4 Problem 11
Since H is a subgroup of the solvable group G, H is also solvable. By the alternative definition of solvable group we can get that there exists an n such that

$$H = H^{(0)} > H^{(1)} > H^{(2)} > H^{(3)} > ...H^{(n)} = 1,$$

where $H^{(i+1)}$ is the commutator subgroup of $H^{(i)}$, also by 3.1 problem 41, $H^{(i+1)}$ is the normal subgroup of $H^{(i)}$, with $H^{(i)}/H^{(i+1)}$ abelian. Thus $H^{(n-1)}$ is a non-trivial abelian subgroup of G. We need to show $H^{(1)}$ is a normal subgroup of G.
Note by $H \trianglelefteq G$, to any $g \in G$, $h \in H$, $hgh^{-1} \in H$. Thus to any $x = [a_1, b_1][a_2, b_2]...[a_n, b_n] \in H^{(1)}$, $gxg^{-1} = g[a_1, b_1]g^{-1}g[a_2, b_2]g^{-1}...g[a_n, b_n]g^{-1} \in H^{(1)}$ since each $g[a_i, b_i]g^{-1} =$

$$ga_ib_ia_i^{-1}b_i^{-1}g^{-1} = (ga_ig^{-1})(gb_ig^{-1})(ga_i^{-1}g^{-1})(gb_i^{-1}g^{-1}) = [c, d] \in H^{(1)},$$

where $c = (ga_ig^{-1}), d = (gb_ig^{-1})$. Therefore $H^{(1)} \trianglelefteq G$, now replace H by $H^{(1)}$, $H^{(1)}$ by $H^{(2)}$, and repeat the procedure above, we get $H^{(2)} \trianglelefteq G$. Now we keep the procedure above to $H^{(i)}$, we can get $H^{(n-1)} \trianglelefteq G$. So $H^{(n-1)}$ is the required A.

3.5 Problem 9

By checking the lattice of group A_4 on p.111, we can see the only subgroup with order 4 is $< (12)(34), (13)(24) >$. Note the conjugate groups have the same order, so by $< (12)(34), (13)(24) >$ is the unique subgroup with order 4 we get $< (12)(34), (13)(24) >$ doesn't have conjugate groups, thus $< (12)(34), (13)(24) >$ is normal. Note $(12)(34)$ and $(13)(24)$ can not generate each other and they both have order 2, also $(12)(34)(13)(24) = (14)(23)$, which has order 2, thus there are 3 elements with order 2, thus we get $< (12)(34), (13)(24) > \cong V_4$.

3.5 Problem 17

There are 4 cases for x, y:

(1): $x = y$, then $< x, y > = < x > \cong \mathbb{Z}_3$, since it's generated by a 3-cycle.

(2): $x = (abc), y = (def)$, where a, b, c, e, e, f are different. Thus $xy = yx$ and $< x > \cap < y > = (1)$, i.e. $< x, y > \cong \mathbb{Z}_3 \times \mathbb{Z}_3$.

(3): $x = (abc), y = (abd)$. Thus We can embed $< x, y >$ into A_4 by $x \mapsto (123), y \mapsto (124)$. But $(123)^2 = (132)$, $(124)^2 = (142)$, $(123)(124) = (13)(24), (124)(123) = (14)(23)$, thus $< (13)(24), (14)(23) >$ is a proper subgroup of $< x, y >$ with order 4, by checking the lattice of group A_4 on p.111, A_4 doesn't have proper subgroups with order larger than 4, thus $< (123)(124) > = A_4$, thus $< x, y > \cong A_4$.

(4): $x = (abc), y = (cde)$, then we can embed $< x, y >$ into A_5 by $x \mapsto (123), y \mapsto (345)$. Note $xy = (abcde)$ and $(xy)x(xy)^{-1} = (bcd)$, $(xy)y(xy)^{-1} = (dea)$, $(xy)(dea)(xy)^{-1} = (eab)$. And $\{x, y, (eab), (bcd), (dea)\} \subset < x, y >$ can generate all the 3-cycles in A_5 (by taking each element of the 5 ones, say z, to z^2, we get 5 more 3-cycles, then with the initial 5 ones, we get all 10 distinct 3 cycles of A_5) while A_n is generated by its 3-cycles, thus $< x, y > \cong A_5$.

4.1 Problem 2

To any $g \in G_a$, $\sigma g \sigma^{-1}(\sigma(a)) = \sigma g(a) = \sigma(a)$, i.e. $\sigma g \sigma^{-1} \in G_{\sigma(a)}$, thus $\sigma G_a \sigma^{-1} \subset G_{\sigma(a)}$. Conversely, any $g \in G_{\sigma(a)}$, $\sigma^{-1} g \sigma(a) = \sigma^{-1}(\sigma(a)) = a$, so $h := \sigma^{-1} g \sigma \in G_a$ and $g = \sigma h \sigma^{-1} \in \sigma G_a \sigma^{-1}$, hence $G_{\sigma(a)} \subset \sigma G_a \sigma^{-1}$, so $G_{\sigma(a)} = \sigma G_a \sigma^{-1}$.

$\bigcap_{\sigma \in G} \sigma G_a \sigma^{-1} = \bigcap_{\sigma \in G} G_{\sigma(a)}$. Since G acts transitively, $\sigma(a)$ goes through each element of A, then any element in the intersection must fix each element of A, thus the element has to be identity, i.e.

$$\bigcap_{\sigma \in G} \sigma G_a \sigma^{-1} = \bigcap_{\sigma \in G} G_{\sigma(a)} = 1.$$

4.1 Problem 7

(a) To any $g \in G_a$, since $a \in B$, $g(B) \cap B \neq \emptyset$, and by the definition of B, either $g(B) = B$ or $g(B) \cap B = \emptyset$, thus $g(B) = B$, hence $g \in G_B$, so $G_a \subset G_B$. And to any $h \in G_B$, $h(B) = B$, which implies that $B = h^{-1}(B)$, thus $h^{-1} \in G_B$, thus to any $h, g \in G_B$, $gh^{-1}(B) = g(B) = B$, i.e. $gh^{-1} \in G_B$, thus G_B is a subgroup of G containing G_a.

(b) First we need to show they are pairwise disjoint. To any $\sigma_i(B), \sigma_j(B)$, if $c = \sigma_i(x) = \sigma_j(y)$,where $x, y \in B$. Then $\sigma_j^{-1}\sigma_i(x) = y \in B$, thus $\sigma_j^{-1}\sigma_i(B) = B$. Hence any $x \in B$, $\sigma_j^{-1}\sigma_i(x) \in B$, (assume $\sigma_j^{-1}\sigma_i(x) = y$) i.e. $\sigma_i(x) = \sigma_j(y) \in \sigma_j(B)$, i.e. $\sigma_i(B) \subset \sigma_j(B)$. Similarly, we can get $\sigma_j(B) \subset \sigma_i(B)$, hence $\sigma_i(B) = \sigma_j(B)$, contradiction, so they are pairwise disjoint.

Now we need to show $A = \bigcup_{i=1}^n \sigma_i(B)$. Since G is a transitive action, any $a \notin B, b \in B$, there exists $g \in G$, s.t. $g(b) = a$, thus $a \in g(B)$, and $g(B)$ as an image of B, should be equal to one of the $\sigma_i(B)$, therefore $a \in \bigcup_{i=1}^n \sigma_i(B)$, thus $A = \bigcup_{i=1}^n \sigma_i(B)$. And by the last paragraph, it's a disjoint union, thus they are a partition of A.

(c) (1) For S_4 on A, it's easy to see A and the sets of size 1 are blocks, and to any set B of size two, without losing generality, we may assume that $B = \{1, 2\}$, then $(23) \cdot B = \{1, 3\}$, which has an intersection with B but not equal to B, thus B is not a block, therefore any set of size two is not a block. Similarly, to any set B of size three, without losing generality, we may assume that $B = \{1, 2, 3\}$, then $(34) \cdot B = \{1, 2, 4\}$, which has an intersection with B but not equal to B, thus B is not a block, therefore any set of size three is not a block. So we can conclude that S_4 is primitive on A.

(2) Any two diagonal vertices of the square is a block: (without losing generality, we name the 4 vertices as $1, 2, 3, 4$ and $(1, 3)$, $(2, 4)$ are two pairs of diagonal vertices, now we focus on $(1, 3)$) since the rotations with angle $90, 270$ degrees would send $(1, 3)$ to $(2, 4)$; the rotation with 180 degrees would send $(1, 3)$ to itself. The refection about the line connecting $1, 3$ would send $(1, 3)$ to itself and the other 3 would send $(1, 3)$ to $(2, 4)$, therefore we get $(1, 3)$ is a non-trivial block, thus D_8 is not primitive as a permutation group on the four vertices of a square.

(d) If for each $a \in A$ the only subgroups of G containing G_a are G_a and G. Then there are no non-trivial blocks: Assume B is a non-trivial block. We can find an $a \in A$, s.t. $a \in B$, then by (a), we have G_B is a subgroup of G containing G_a, thus by assumption, $G_B = G$ or G_a. If $G_B = G$, then by G is transitive, to any $b \notin B$, there is a $g \in G$, s.t. $g(a) = b$, thus $g(B) \neq B$, contradiction. So $G_B = G_a$. Now since B is non-trivial, we can always find $b \in B, b \neq a$, so $G_b = G_B = G_a$. Since G is transitive, there exists a $g \in G$, s.t. $g(b) = a$. So $g \notin G_b = G_B$, but as B is a block and $g(B) \cap B \neq \emptyset$, thus $g(B) = B$, thus $g \in G_B$, which is a contradiction. So there are no non-trivial blocks.

Conversely, now we assume the transitive group G is primitive on A. Assume there is a subgroup H strictly containing some G_a for some $a \in A$. Define $B := \{h(a)|h \in H\}$. To any $g \in H, t \in B$, $t = h(a)$ for some $h \in H$, then $g(t) = gh(a) \in B$, thus $g(B) \subset B$, similarly, $g^{-1}(B) \subset B$, so $B \subset g(B)$, hence $g(B) = B$. Now to any $g \in G, \notin H$, if $c \in g(B) \cap B$, we may assume $g(h_1(a)) = c = h_2(a)$, where $h_i \in H$, thus $h_2^{-1} g h_1 \in G_a \subset H$, thus $gh_1 \in H$, hence $g \in H$, contradiction, thus to any $g \in G, \notin H$, $g(B) \cap B = \emptyset$. Therefore B is a block. Note, since H contains some elements not in G_a, $B \neq \{a\}$. Thus by assumption, $B = A$, therefore any $g \in G$, there exists some $h \in H$, s.t. $ga = ha$, thus $h^{-1}g \in G_a$, thus $g \in HG_a = H$, so $G \subset H$, i.e. $H = G$. Thus for each $a \in A$ the only subgroups of G containing G_a are G_a and G.

4.2 Problem 11

(1) Note g fixes no elements of G, thus $\pi(x)$ is a product of cycles where all the elements are contained. It's easy to see each cycle ($(x, xg, x^2g, ...x^m g)$, where $m = n - 1$, as $x^n x = 1 \cdot x = x$) is a corresponding to a coset of $< x >$, thus is with size n. And $G = \sqcup < x > g$, where each $< x > g$ represents a distinct coset of $< x >$, which also can be identified as an n-cycle in the product of $\pi(x)$. Since all the cosets are non-overlapped and with size n, also the G is the disjoint union of these cosets, we get $\pi(x)$ consists of $\frac{|G|}{|x|} = m$ n-cycles with each n-cycle is corresponding to a coset of $< x >$.

(2) Since $\pi(x)$ is a product of m n-cycles and the sgn of an n-cycle is $(-1)^{n-1}$, $sgn(\pi_x) = [(-1)^{n-1}]^m$. Thus $sgn(\pi_x) = [(-1)^{n-1}]^m = -1$ if and only if n is even, m is odd, in other words, $\pi(x)$ is an odd permutation if and only if $|x|$ is even and $\frac{|G|}{|x|}$ is odd.

4.3 Problem 27

By class equation, $|G| = \sum_{i=1}^{r} |G : C_G(g_i)|$. By assumption $g_i g_j = g_j g_i$, we get $g_i \in C_G(g_j)$, thus $C_G(g_i) \geq r$, thus we have $|G| = \sum_{i=1}^{r} |G : C_G(g_i)| \leq \sum_{i=1}^{r} |G|/r = |G|$, which implies that $|G : C_G(g_i)| = |G|/r$, i.e. $|C_G(g_i)| = r$, i.e. $C_G(g_i) = \{g_1, g_2, ...g_r\}$ for each i. Note 1 is among the $g_1, g_2, ...g_r$, and $C_G(1) = G$, thus $G = C_G(1) = \{g_1, g_2, ...g_r\}$, thus G is abelian.

4.4 Problem 18

(a) Assume the representative of K is k, then any $x \in K$, it is in the form of $gkg^{-1}, g \in G$, then to $\sigma \in Aut(G)$, $\sigma(x) = \sigma(g)\sigma(k)\sigma(g)^{-1}$ is in the conjugacy class of $\sigma(k)$, so $\sigma(K)$ is contained in the conjugacy class of $\sigma(k)$ (say K'), similarly, $\sigma^{-1}(K')$ is contained in K, thus $\sigma(K)$ is a conjugacy class.

(b) The number of conjugates of a cycle is $C_n^2 = \frac{n(n-1)}{2!} = \frac{n(n-1)}{2}$, i.e. $|K| = \frac{n(n-1)}{2}$. Let x be any element of order 2 in S_n, that is not a transposition. Assume x to be a product of

k-disjoint 2-cycles, then by exercise 33 of 4.3, we get that the conjugacy class K' of x is of size

$$|K'| = \frac{n!}{k!2^k}$$

So if $|K| = |K'|$, then $\frac{n(n-1)}{2} = \frac{n!}{k!2^k}$, i.e. $(n-2)! = k!2^{k-1}$, which is true iff $n = 6, k = 3$. So by the assumption $n \neq 6$, we have $|K| \neq |K'|$.

By (a), any automorphism σ of S_n maps the conjugacy class of any transposition x to the conjugacy class of $\sigma(x)$. Since automorphism keeps the order, $\sigma(x)$ is of order 2. Also by (a), these two conjugacy classes have the same order, thus $\sigma(x)$ has to be a transposition.

(c) By (b), each $\sigma \in Aut(S_n)$ maps a transpositions to transpositions, thus we have $\sigma((1i))$ is a transposition. To any $(1,j),(1,i)$ with $j \neq i; i,j \not/ 1$, since σ is an isomorphism, $\sigma((1,i)) \neq \sigma((1,j))$, and $\sigma((1,i)), \sigma((1,j))$ must contain a common number, since otherwise, $\sigma((1,j))\sigma((1,i))$ is of order 2, hence $\sigma^{-1}(\sigma((1,j))\sigma((1,i))) = (1i)(1j) = (1ji)$ is also of order 2, contradiction. Hence, $\sigma((1,i)), \sigma((1,j))$ must contain a common number say a, i.e. $\sigma((1,i)) = (ab_i)$, where the b_is are different by $\sigma((1,i)) \neq \sigma((1,j))$. Also $a \neq b_i$ for each i, since $\sigma((1,i))$ is a transposition.

(d) Recall S_n is generated by the transpositions, and any transposition $(ij) = (1i)(1j)(1i)$, thus the set of transpositions are generated by $(12), (13), ..., (1n)$, i.e. S_n is generated by $(12), (13), ..., (1n)$, hence any automorphism of S_n is determined by its action on the elements $(12), (13), ..., (1n)$.

By (c), any $\sigma \in Aut(S_n)$, $\sigma(i) \neq \sigma(j), i \not/ j$, thus for any $\sigma \in Aut(S_n)$, the $\sigma(1)$ has n choices, hence $\sigma(2)$ has $n-1$ choices,...,$\sigma(i)$ has $n-i+1$ choices,... So there are $n!$ possible choices for σ, i.e. S_n has at most $n!$ automorphisms.

By $G/Z(G) \cong Inn(G)$, we have $n! = |S_n| \leq |Inn(G)| \leq |Aut(S_n)| \leq n!$, thus $|Inn(G)| = |Aut(S_n)|$, thus $Inn(G) = Aut(S_n)$.

4.5 Problem 22

If $|G| = 132 = 3 \times 4 \times 11$, then there is a 11-subgroup, say P. We know $n_{11} \equiv 1 \mod 11$ and $n_{11}|(132/11) = 12$, if $n_{11} \neq 1$, then $n_{11} = 12$. If G is simple, then $n_{11} = 12$. And $n_3 \neq 1$, and $n_3 \equiv 1 \mod 3$, and $n_3|11 \times 4 = 44$, thus $n_3 = 4, 22$. Similarly, $n_2 \equiv 1 \mod 2$ and $n_2|11 \times 2 = 33$, thus $n_2 = 3, 11, 33$. And 2-groups, 3-groups, 11-groups are all cyclic, thus their intersections can only be $\{1\}$. The number of all non-trivial elements in the 11-groups and 3-groups is at least $12 \times (11-1) + 4 \times (3-1) = 128$, hence there are exactly 4 elements with 3 elements with order not dividing $3, 11$, (i.e. dividing 4) thus there is exactly one 4-group, which is normal, contradiction. Thus G can not be simple.

4.5 Problem 33
Since the intersection of two subgroups is the subgroup of each these two subgroups, thus $H \cap P$ is a subgroup of P, so it's also a p-group. And since P is normal, to any $h \in H$, $p \in P \cap H$, we have $hph^{-1} \in P, H$, thus $hph^{-1} \in P \cap H$, i.e. $P \cap H$ is a normal subgroup of H. To any Sylow-p subgroup of H, say K, observe that K is a p-subgroup of G, we get K is contained in a Sylow-p subgroup of G, i.e. P, hence $K = P \cap H$, which proves $P \cap H$ is the Sylow-p subgroup of H, and recall we have proved it is normal, thus the uniqueness follows.

4.6 Problem 2
If N is a proper normal subgroup of S_n, $n \geq 5$, then $N \cap A_n$ is a normal subgroup of A_n. Since A_n is simple for $n \geq 5$, we have $N \cap A_n = A_n$, or $N \cap A_n = \{1\}$. If $N \cap A_n = A_n$, then $A_n < N$, by $[S_n : A_n] = 2$, thus $N = A_n$. If $N \cap A_n = \{1\}$, consider the projection $f : S_n \to S_n/A_n \cong \mathbb{Z}_2$. If any $x \in N$, s.t. $f(x) = 1$, then we have $x \in A_n$, then $x = 1$, thus the restriction $f|_N$ is injective, i.e. $N \cong f(N)$ is not trivial, thus $N \cong \mathbb{Z}_2$. So N is generated by an odd permutation (say x) with order 2, which can be expressed as odd transpositions and these transpositions are disjoint since x is with order 2. Now assume $x = (a_1a_2)(a_3a_4)...(a_{n-1}a_n)$, these a_i are distinct since these transpositions are disjoint. Then $(a_2a_3)x(a_2a_3) = (a_1a_3)(a_2a_4)...$, which is not x or identity, thus N is not normal, contradiction. Therefore the only proper normal subgroups of S_n $(n \geq 5)$, is A_n. So when $n \geq 5$, the normal subgroups of S_n are $\{1\}, A_n, S_n$.

5.1 Problem 2
(a) Assume $|I| = m$. Define the map $f : \prod_{i\in I} G_i \to G$ by: any $(g_1, ...g_m) \in \prod_{i\in I} G_i \mapsto g \in G$, where $g_i \in G_i$, s.t. g is defined that the corresponding tuple of G_i in G is g_i, and the rest $n - m$ tuples of g are just 1 for each tuple. Then it's easy to see it's an injective homomorphism with image G_I, thus by the first isomorphism theorem, $\prod_{i\in I} G_i \cong G_I$.

(b) By (a), without losing generality, we may assume $G_I = G_1 \times G_2 \times ... \times G_m \times \{1\} \times ... \times \{1\}$. And to any $(g_1 \times g_2 \times ... \times g_m \times 1 \times ... \times 1) \in G_I, (h_1, ...h_n) \in G$, we have $hgh^{-1} = (h_1g_1h_1^{-1} \times h_2g_2h_2^{-1} \times ... \times h_mg_mh_m^{-1} \times h_{m+1} \cdot 1 \cdot h_{m+1}^{-1} \times ... \times h_n \cdot 1 \cdot h_n^{-1}) = (h_1g_1h_1^{-1} \times h_2g_2h_2^{-1} \times ... \times h_mg_mh_m^{-1} \times 1 \times ... \times 1)$. Observe $h_ig_ih_i^{-1} \in G_i$, thus $hgh^{-1} = (h_1g_1h_1^{-1} \times h_2g_2h_2^{-1} \times ... \times h_mg_mh_m^{-1} \times 1 \times ... \times 1 \in G_I$, i.e. G_I is normal. It's easy to see that $G/G_I = \{1\} \times \{1\} \times ...\{1\} \times G_{m+1} \times ... \times G_n = G_J$.

(c) By (a) $G_I \cong \prod_{i\in I} G_i$, similarly, $G_J \cong \prod_{i\in J} G_i$, thus $G_I \times G_J \cong \prod_{i\in I} G_i \times \prod_{j\in J} G_J \cong G$.

5.1 Problem 11
By p.155, $E_{p^n} = \mathbb{Z}_p \times ... \times \mathbb{Z}_p$ (n factors). We may define $\mathbb{Z}_p \times ... \times \mathbb{Z}_p = < a_1 > \times ... \times < a_n >$, where each a_i is of order p. Also we have $a_ia_j = a_ja_i$ and $ord(a_i^m) = p$ if $m \neq p$, thus any non-trivial element $a_1^{N_1}a_2^{N_2}...a_n^{N_n}$ is of order n, since $(a_1^{N_1}a_2^{N_2}...a_n^{N_n})^m = a_1^{mN_1}a_2^{mN_2}...a_n^{mN_n}$, which equals to 1 iff each $a_i^{mN_i} = 1$, while which equals to 1 iff $m = 1$. Observe any sub-

group of order p is generated by an element in E_{p^n} and each non-trivial element generates a subgroup with order p. Also $< g >=< g^j >$, where $g \in E_{p^n}, j \neq p$, thus there are $\frac{p^n-1}{p-1} = \sum_{i=0}^{n-1} p^i$ subgroups of order p.

5.4 Problem 8

First note $[x, y] = [y, x]^{-1}$, and by $x[x, y] = [x, y]x$, we get $[x, y]^{-1}x[x, y] = x$, $[x, y]^{-1}x = x[x, y]^{-1}$, i.e. $x[y, x] = [y, x]x$. Similarly, we have $y[y, x] = [y, x]y$.

We can prove the result by induction, when $n = 1$, $(xy)^n = xy = x^n y^n [y, x]^{\frac{n(n-1)}{2}}$, so it's true for $n = 1$. Now we assume the equality is true for $n = k - 1$, and we consider the case for $n = k$, we know $(xy)^k = (xy)^{k-1}(xy) = x^{k-1}y^{k-1}[y, x]^{\frac{(k-1)(k-2)}{2}}(xy) = x^{k-1}y^{k-1}(xy)[y, x]^{\frac{(k-1)(k-2)}{2}}$.

By $y[y, x] = [y, x]y$, we can get $x^{-1}yx = y^{-1}x^{-1}yxy$, thus $yx = xy^{-1}x^{-1}yxy$. So $y^{k-1}xy = y^{k-2}(yx)y = y^{k-2}xy^{-1}x^{-1}yxyy = y^{k-2}x[y, x]y^2 = y^{k-2}xy^2[y, x]$. Similarly, we have $y^{k-1}xy = y^{k-2}xy^2[y, x] = y^{k-3}xy^3[y, x]^2$, keep doing this we can get:$y^{k-1}xy = xy^k[y, x]^{k-1}$ So $x^{k-1}y^{k-1}(xy)[y, x]^{\frac{(k-1)(k-2)}{2}} = x^{k-1}(xy^k[y, x]^{k-1})[y, x]^{\frac{(k-1)(k-2)}{2}} = x^k y^k [y, x]^{\frac{(k-1)k}{2}}$. So we proved, when $n = k$, $(xy)^k = x^k y^k [y, x]^{\frac{(k-1)k}{2}}$, i.e. we have finished the induction, which shows we finished the proof.

5.4 Problem 10

By the fundamental theorem of finitely generated abelian group, a finite abelian group is isomorphic to $\mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_{p_2^{n_2}} \times \mathbb{Z}_{p_m{}^{n_m}}$, where each p_i is a distinct prime number. And the subgroup $\{1\} \times ...\{1\} \times \mathbb{Z}_{p_i{}^{n_i}} \times \{1\}... \times \{1\}$ is a Sylow p_i subgroup, by 5.1 Problem 2, we know the whole group is the direct product of all the $\{1\} \times ...\{1\} \times \mathbb{Z}_{p_i{}^{n_i}} \times \{1\}... \times \{1\}$, i.e. the whole group is the direct product of its Sylow subgroups.

5.4 Problem 16

To any $x = [a_1, b_1]...[a_n, b_n] \in K'$, where $a_i, b_i \in K$, and any $g \in G$,

$$gxg^{-1} = g[a_1, b_1]...[a_n, b_n]g^{-1} = (g[a_1, b_1]g^{-1})(g[a_2, b_2]g^{-1})...(g[a_{n-1}, b_{n-1}]g^{-1})(g[a_n, b_n]g^{-1}),$$

where $g[a_i, b_i]g^{-1} = ga_i^{-1}g^{-1}gb_i^{-1}g^{-1}ga_ig^{-1}gb_ig^{-1} = (ga_ig^{-1})^{-1}(gb_ig^{-1})^{-1}ga_ig^{-1}gb_ig^{-1}$. Since $a_i, b_i \in K$, K is normal, thus $ga_ig^{-1}, gb_ig^{-1} \in K$, hence we have $g[a_i, b_i]g^{-1} \in K'$, therefore K' is a normal subgroup of G.

5.5 Problem 10

(a) $\mathbb{Z}_{147}$ and $\mathbb{Z}_{21} \times \mathbb{Z}_7$ are two abelian groups of order 147. They are not isomorphic because $gcd(21, 7) \neq 1$.

(b) $147 = 7^2 \times 3$, By Sylow theorem, $n_7 = 1 \mod 7$, and $n_7|3$, thus n_7 has to be 1. Therefore the unique Sylow 7-subgroup is normal.

(c) Since any group of order 147, has a Sylow 3-subgroup of order 3, i.e. $\cong \mathbb{Z}_3$. Note $|\mathbb{Z}_3||\mathbb{Z}_{49}| = 147$, and $\mathbb{Z}_{49}$ is normal by (b). Thus any subgroup of order 147 with Sylow 7-subgroup cyclic is just $\mathbb{Z}_3\mathbb{Z}_{49}$, moreover it can be represented as $\mathbb{Z}_{49} \rtimes_\phi \mathbb{Z}_3$, for some homomorphism from $\mathbb{Z}_3$ to $Aut(\mathbb{Z}_{49}) = \mathbb{Z}_{49}^* \cong \mathbb{Z}_{42}$.

Consider $\mathbb{Z}_{49} \rtimes_\phi \mathbb{Z}_3$, note $Aut(\mathbb{Z}_{49}) = \mathbb{Z}_{49}^* \cong \mathbb{Z}_{42}$. Observe, $(1,0)(0,1) = (1,1), (0,1)(1,0) = (0+\phi(1)\cdot 1, 0+1) = (\phi(1)\cdot 1, 1)$, note if ϕ is non-trivial, then $\phi(1)\cdot 1$ is not 1 and relatively prime to 49, so if $\phi \in Aut((\mathbb{Z}_{49})$ is not trivial, then $(1,0)(0,1) \neq (0,1)(1,0)$. (such a non-trivial homomorphism exists since the homomorphisms from $\mathbb{Z}_3$ to $\mathbb{Z}_{42}$ are not always trivial.) Also $|\mathbb{Z}_{49} \rtimes_\phi \mathbb{Z}_3| = |\mathbb{Z}_{49}| \times |\mathbb{Z}_3| = 147$. So this is an abelian group of order 147 with Sylow 7-subgroup cyclic.

First note that if N, H, with $\phi \in Hom(H, Aut(N))$, $\beta \in Aut(H)$, then $N \rtimes_\phi H \cong N \rtimes_{\phi\circ\beta} H$ by sending (n, h) to $(n, \beta^{-1}(h))$.
Now, in our case, if ϕ is non-trivial, then $\phi(1)\cdot 1 = 18, 30$, since $\phi \in Hom(\mathbb{Z}_3, \mathbb{Z}_{49}^*) \cong \mathbb{Z}_3$ and only $18, 30$ in $\mathbb{Z}_{49}^*$ are of order 3. Define $\phi_1(1) = 18$, $\phi_2(1) = 30$, which implies that $\phi_1(2) = 30$. Note to the nontrivial $\beta \in Aut(\mathbb{Z}_3)$, $\phi_1 \circ \beta(1) = \phi_1(2) = 30 = \phi_2(1)$. Thus by above $N \rtimes_{\phi_1} H \cong N \rtimes_{\phi_2} H$, in other words, these two possible groups are isomorphic, thus there is only one non-abelian group with order 147, whose Sylow 7-subgroup is cyclic.

(d) $|GL_2(\mathbb{F}_7)| = (7^2-1)(7^2-7) = 48 \times 42 = 3^2 \times 2^5 \times 7$. So the Sylow 3-subgroup of $GL_2(\mathbb{F}_7)$ is of order 9. It's easy to see that $t_1, t_2 \in GL_2(\mathbb{F}_7)$ thus $< t_1, t_2 > \subset GL_2(\mathbb{F}_7)$, and $t_i^2 \neq id$, but $t_i^3 = id$, where $i = 1, 2$. Also $t_1t_2 = 2\cdot id = t_2t_1$, thus $< t_1, t_2 > \cong < t_1 > \times < t_2 > = \mathbb{Z}_3 \times \mathbb{Z}_3$.

So $< t_1, t_2 >$ is a subgroup of order 9 of $GL_2(\mathbb{F}_7)$ so it's a Sylow-3 subgroup of $GL_2(\mathbb{F}_7)$ isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_3$. Any subgroup of order 3, say U, of $GL_2(\mathbb{F}_7)$, is contained in a Sylow 3-subgroup of $GL_2(\mathbb{F}_7)$, which is conjugate to P, i.e. there exists $g \in GL_2(\mathbb{F}_7)$, s.t. $h \subset gPg^{-1}$, hence $g^{-1}hg \subset P$ i.e. U is conjugate to a subgroup of P, i.e. any subgroup of order 3 is conjugate to a subgroup of P.

(e) By the isomorphism of the semi-direct product above, we may assume $\phi_i(1)(a,b) = t_i(a,b)$, so $((a_1,b_1),c_1)\cdot((a_2,b_2),c_2) = ((a_1,b_1)+t_i(c_1)(a_2,b_2), c_1+c_2)$. Define $x := ((1,0),0), y = ((0,1),0), z((0,0),1)$. It's easy to see that x, y, z generate G_i.

By computation, $x^2z = ((2,0),1) = zx$, $zy = ((0,1),1) = yx$, thus

$$G_1 =< x, y, z | x^7 = y^7 = z^3, xy = yx, zy = yz, zx = x^2z > .$$

Similarly,

$$G_2 =< x, y, z | x^7 = y^7 = z^3, xy = yx, zy = yz, zx = x^2 z > .$$

Thus $G_1 \cong G_2$.
Similarly

$$G_3 =< x, y, z | x^7 = y^7 = z^3, xy = yx, zy = y^2 z, zx = x^2 z > .$$

Similarly

$$G_4 =< x, y, z | x^7 = y^7 = z^3, xy = yx, zy = y^4 z, zx = x^2 z > .$$

(f) By the presentation of G_1, we know $yx = xy, yz = zy$, thus $< y > \subset Z(G_1)$, thus $Z(G_1)$ is non-trivial, while by the presentations of G_3, G_4, we can see the centres are trivial. Thus G_1 is not isomorphic to G_3 or G_4.

(g) By Sylow theorem, any 7-subgroup is contained in a Sylow 7-subgroup, so any 7-subgroup is contained in $\mathbb{Z}_7 \times \mathbb{Z}_7$, which is $< x > \times < y >$, thus the subgroups of order 7 are $< x >$, $< y >$, $< xy^i >, i = 1, ..., 6$.

By the presentation of G_3, $yxy^{-1} = x, zxz^{-1} = x^2$, thus $< x >$ is normal. And $y(xy^i)y^{-1} = (yxy^{-1}y^i = xy^i$. And by $zy = y^2 z$, we have that $yz^{-1} = z^{-1}y^2$, $z(xy^i)z^{-1} = zxz^{-1}y^{2i} = x^2y^{2i} = (xy^i)^2 \in < xy^i >$, thus each $< xy^i >$ is normal, i.e. each subgroup of order 7 in G_3 is normal.

Similarly to the case of G_3, we can get in G_4: $z(xy^i)z^{-1} = x^2y^{4i}$ which is not always in $< xy^i >$, for example, when $i = 1$, $zxyz^{-1} = x^2y^4 \in < xy^2 >$, but $< xy > \cap < xy^2 > = \{1\}$, thus $< xy >$ is not normal. In other words, there is a subgroup of order 7 in G_4 not normal, thus $G_3 \ncong G_4$.

(h) If the group, say G, is abelian, then the only two choices are $\mathbb{Z}_{147}$ and $\mathbb{Z}_{21} \times \mathbb{Z}_7$ since $147 = 7^2 \times 3$ and by the fundamental theorem of finitely generated group. If the group, say G, is not abelian, then by and (b), (c), its Sylow 7-subgroup is normal and cyclic, thus $G = \mathbb{Z}_{49} \rtimes \mathbb{Z}_3$. And (d),(e),(f),(g) determine the four possible cases up to isomorphisms, thus there are only 6 cases for the group G of order 147.

5.5 Problem 16

Note $Aut(\mathbb{Z}_8) = \mathbb{Z}_8{}^* = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, i.e. there are 3 elements with order 2, say a, b, c, and there are 4 choices of mapping the generator of $\mathbb{Z}_2$ to $Aut(\mathbb{Z}_8)$. And if mapping the generator of $\mathbb{Z}_2$ to a, b, c respectively, we get 3 injective homomorphisms and if mapping the generator of $\mathbb{Z}_2$ to the identity of $Aut(\mathbb{Z}_8)$, we get a trivial homomorphism. So, we can conclude that there are 4 homomorphisms in total.

Now we consider the four $\mathbb{Z}_8 \rtimes_{\phi_i} \mathbb{Z}_2$, where each ϕ_i is among the 4 homomorphisms described above.
First, note, for any i, $(1,0) \in \mathbb{Z}_8 \rtimes_{\phi_i} \mathbb{Z}_2$, we have $(j,0)(1,0) = (j+\phi_i(0)\cdot 1, 0+0) = (j+1,0)$, i.e. $(1,0)^8 = id$. And $(0,i)(0,j) = (0+\phi_i(0)\cdot 0, i+j) = (0,i+j)$, thus $(0,1)^2 = (0,0) = id$.
Second by $Aut(\mathbb{Z}_8) = \mathbb{Z}_8{}^* = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$, we can get each $\phi_i(1) = 1,3,5,7 \in \mathbb{Z}_8$.

Assume ϕ_1 is the trivial homomorphism, then $\mathbb{Z}_8 \rtimes_{\phi_1} \mathbb{Z}_2 = \mathbb{Z}_8 \times \mathbb{Z}_2$.

Assume ϕ_2 is the homomorphism mapping $1 \in \mathbb{Z}_8 \mapsto 3 \in \mathbb{Z}_8$, then to $(1,0),(0,1) \in \mathbb{Z}_8 \rtimes_{\phi_2} \mathbb{Z}_2$, we have $(1,0)(0,1) = (1+\phi_2(0)\cdot 1, 0+1) = (1,1)$ and $(0,1)(1,0) = (0+\phi_2(1)\cdot(1), 1+0) = (3,1)$, $(3,1)(1,0) = (3+\phi_2(1)\cdot(1), 1+0) = (6,1)$, $(6,1)(1,0) = (6+\phi_2(1)\cdot(1), 1+0) = (9,1) = (1,1) = (1,0)(0,1)$. Similarly, we have $(0,1)(1,0)^n = (0+n\phi_2(1)\cdot(1), 1+0) = (3n,1)$ and $(0,1)(1,1)^n = (0+n\phi_2^{(}1)\cdot(1), 1+1) = (3n,2) = (3n,0)$, and as n changes, $3n$ can be any element in $\mathbb{Z}_8$ so $(0,1),(1,0)$ generate $\mathbb{Z}_8 \rtimes_{\phi_2} \mathbb{Z}_2$.
So we can conclude that $\mathbb{Z}_8 \rtimes_{\phi_2} \mathbb{Z}_2 =< (1,0),(0,1) | (1,0)^8 = (0,1)^2 = id, (0,1)(1,0)^3 = (1,0)(0,1) >= QD_{16}$.

Assume ϕ_3 is the homomorphism mapping $1 \in \mathbb{Z}_8 \mapsto 5 \in \mathbb{Z}_8$, similarly, we can get $(1,0)(0,1) = (1+\phi_3(0)\cdot 1, 0+1) = (1,1)$ and $(0,1)(1,0)^n = (0+n\phi_3(1)\cdot(1), 1+0) = (5n,1)$, $(0,1)(1,1)^n = (0+n\phi_3(1)\cdot(1), 1+1) = (5n,0)$, and as n changes, $5n$ can be any element in $\mathbb{Z}_8$, so $(0,1),(1,0)$ generate $\mathbb{Z}_8 \rtimes_{\phi_3} \mathbb{Z}_2$. Moreover, $(1,0)(0,1) = (1,1) = (25,1) = (0,1)(1,0)^5$. So we can conclude that $\mathbb{Z}_8 \rtimes_{\phi_3} \mathbb{Z}_2 =< (1,0),(0,1) | (1,0)^8 = (0,1)^2 = id, (0,1)(1,0)^5 = (1,0)(0,1) >= M$.

Assume ϕ_4 is the homomorphism mapping $1 \in \mathbb{Z}_8 \mapsto 7 \in \mathbb{Z}_8$, similarly, we can get $(1,0)(0,1) = (1+\phi_3(0)\cdot 1, 0+1) = (1,1)$ and $(0,1)(1,0)^n = (0+n\phi_4(1)\cdot(1), 1+0) = (7n,1)$, $(0,1)(1,1)^n = (0+n\phi_4(1)\cdot(1), 1+1) = (7n,0)$, and as n changes, $7n$ can be any element in $\mathbb{Z}_8$, so $(0,1),(1,0)$ generate $\mathbb{Z}_8 \rtimes_{\phi_4} \mathbb{Z}_2$. Moverover, $(1,0)(0,1) = (1,1) = (49,1) = (0,1)(1,0)^7 = (1,1)$, in other words, $(1,0)(0,1) = (1,1) = (0,1)(1,0)^{-1}$ (observe $(1,0)^{-1} = (1,0)^7$). So we can conclude that $\mathbb{Z}_8 \rtimes_{\phi_4} \mathbb{Z}_2 =< (1,0),(0,1) | (1,0)^8 = (0,1)^2 = id, (0,1)(1,0)^{-1} = (1,0)(0,1) >= D_{16}$.

7.1 Problem 23

(a) First, $1 = 1 + 0f\omega \in O_f$. Also, for $z_1 = a_1 + b_1 f\omega$ and $z_2 = a_2 + b_2 f\omega$, we have that $z_1 + z_2 = (a_1+a_2) + f\omega(b_1+b_2) \in O_f$. $z_1 z_2 = a_1 b_1 + b_1 b_2 f_2 \omega^2 + f\omega(b_1 a_2 + a_1 b_2)$. And if $D \not\equiv 1 \mod 4$, $z_1 z_2 = a_1 b_1 + D b_1 b_2 f^2 + f\sqrt{D}(b_1 a_2 + a_1 b_2) \in O_f$; if $D \equiv 1 \mod 4$, $z_1 z_2 = a_1 b_1 + \frac{D-1}{4} b_1 b_2 f^2 + f\omega(b_1 a_2 + a_2 b_1 + f b_1 b_2) \in O_f$. So we get O_f is a subring of O.

(b) Let $z = a + b\omega \in O$, and write $b = fq + r$, with $0 \le r \le f$. Then $z = a + b\omega = a + (fq + r)\omega = r\omega + (a + fq\omega) = r\omega O_f$, thus the representatives of O/O_f are $\{0, \omega, 2\omega, ..., (f-1)\omega\}$. Thus $[O : O_f] = f$.

(c) Let R be a subring of O containing 1 such that the quotient group O/R has index f. Since $1 \in R$, $\mathbb{Z} \in R$. To any $a + b\omega \in O$, we have $fa + fb\omega \in R$, hence $fb\omega \in R$, thus $O_f \in R$. Since both quotients have index f, this implies $R = O_f$.

7.1 Problem 25

(a) $\alpha\bar{\alpha} = (a + bi + cj + dk)(a - bi - cj - dk) = a^2 + b^2 + c^2 + d^2 - bcij + bdki + cbij - cdjk - dbki + cdjk = a^2 + b^2 + c^2 + d^2$. Thus $N(\alpha) = \alpha\bar{\alpha}$.

(b) $N(\alpha\beta) = N((a+bi+cj+dk)(x+yi+zj+wk)) = N((ax-by-cz-dw)+(ay+bx+cw-dz)i+(az-bw+cw+dy)j+(aw+bz-cy+dx)k)) = (ax-by-cz-dw)^2+(ay+bx+cw-dz)^2+(az-bw+cw+dy)^2+(aw+bz-cy+dx)^2 = (a^2+b^2+c^2+d^2)(x^2+y^2+z^2+w^2)$. $N(\alpha\beta) = N(\alpha)N(\beta)$.

(c) If α is a unit with inverse β, by $1 = N(1) = N(\alpha\beta) = N(\alpha)N(\beta)$ and $N(\alpha), N(\beta) \in \mathbb{Z}$, we get $N(\alpha) = N(\beta) = 1$. Conversely, if $N(\alpha) = 1$, then $1 = N(\alpha) = \alpha\bar{\alpha}$, by definition, $\bar{\alpha} \in I$, thus α is a unit.
To any $\alpha = a + bi + cj + dk =\in I^\times$, thus $N(a + bi + cj + dk) = a^2 + b^2 + c^2 + d^2 = 1$, hence $a, b, c, d = 0, \pm 1$ and 3 of them must be 0. Thus $|I^\times| = 8$. Since $I^\times$ is not abelian with 4 elements of order 2, we have $I^\times \cong Q_8$.

7.1 Problem 26

(a) By $V(1) = V(1 \cdot 1) = V(1) + V(1)$, we have $V(1) = 0$, thus $1 \in R$. It remains to show that R is closed under subtraction and multiplication. Note $0 = v(1) = v(-1)V(-1) = 2V(-1)$, thus $-1 \in R$, thus if $a \in R$, then so is $-a$.
If $a, b \in R$, then $V(a - b) \ge min\{V(a), V(-b)\} \ge 0$, hence R is closed under subtraction. By V is a homomorphism we can conclude that R is closed under multiplication. Thus R is a subring.

(b) We have $0 = v(1) = v(xx^{-1}) = v(x) + v(x^{-1})$, so either $v(x) \ge 0$ or $v(x^{-1}) \ge 0$, and the result follows.

(c) Suppose that $x \in R$ is a unit. Then $x^{-1} \in R$, hence $V(x), V(x^{-1}) \ge 0$. By $0 = v(xx^{-1}) = v(x) + v(x^{-1})$, we have $V(x) = 0$. Now suppose that $V(x) = 0$. Then $0 = v(x) + v(x^{-1})$, $v(x^{-1}) = 0$ thus $x^{-1} \in R$, which implies that x is a unit.

7.2 Problem 3

(a) Obviously, $1 = 1 + \sum_{n=1}^{\infty} 0 \cdot x^n \in R[[x]]$. Let $\alpha = \sum_{n=0}^{\infty} a_n x^n, \beta = \sum_{n=0}^{\infty} b_n x^n$, then $\alpha\beta = (\sum_{n=0}^{\infty} a_n x^n)(\sum_{n=0}^{\infty} b_n x^n) = \sum_{n=0}^{\infty}(\sum_{j+i=n}^{\infty} b_j a_i)x^n = \sum_{n=0}^{\infty}(\sum_{i+j=n}^{\infty} a_i b_j)x^n = (\sum_{n=0}^{\infty} b_n x^n)(\sum_{n=0}^{\infty} a_n x^n) = \beta\alpha$. So $R[[x]]$ is a oommutative ring with 1.

(b) We define $a_0 = 1, a_1 = -1, a_i = 0, i \geq 2$, and $b_i = 1$, any i, thus $(1-x)(1+x+x^2+...) = (\sum_{n=0}^{\infty} a_n x^n)(\sum_{n=0}^{\infty} b_n x^n) = \sum_{n=0}^{\infty}(\sum_{k=0}^{n} a_k b_{n-k})x^n = a_0(b_0x^0+b_1x+b_2x^2+...)+a_1(b_0x^1+b_1x^2+...) = (1+x+x^2+...) - (x+x^2+x^3+...) = 1$, thus $1-x$ is a unit.

(c) Assume $(\sum_{n=0}^{\infty} a_n x^n)$ is a unit, then there exists $\sum_{n=0}^{\infty} b_n x^n$, s.t.$(\sum_{n=0}^{\infty} a_n x^n)(\sum_{n=0}^{\infty} b_n x^n) = \sum_{n=0}^{\infty}(\sum_{k=0}^{n} a_k b_{n-k})x^n = 1$. So $a_0 b_0 = 1$, i.e. a_0 is a unit in R.
Conversely, if a_0 is a unit in R, Define $b_0 = a_0^{-1}, b_{n+1} = -a_0^{-1}\sum_{j=1}^{n+1} a_j b_{n+1-j}$, It is easy to see that for $n \geq 1$, $\sum_{j=0}^{n} a_j b_{n-j} = 0$, Now let $g = \sum_{i=0}^{\infty} b_i x^i$, we get $(\sum_{i=0}^{\infty} a_i x^i)(g) = 1$.

7.2 Problem 6
(a) Define $E_{ij}A = (r_{pq})$, note $r_{pq} = \sum_{k=1}^{n} e_{pk}a_{kq}$, and if $p \neq i$, then $e_{pk} = 0$, hence $r_{pq} = 0$. And if $p = i$, then $r_{pq} = a_{jq}$, that finishes the proof.

(b) Define $AE_{ij} = (r_{pq})$, note $r_{pq} = \sum_{k=1}^{n} a_{pk}e_{kq}$, and if $q \neq j$, then $e_{kq} = 0$, hence $r_{pq} = 0$. And if $q = j$, then $r_{pq} = a_{pi}$, that finishes the proof.

(c) $E_{pq}AE_{rs}$, by (a) $E_{pq}A$ whose pth row equals the qth row of A and all other rows are zero; by (b) $E_{pq}AE_{rs}$ whose sth column equals the rth column of AE_{ij} and all other columns are zero, thus whose p, s entry is a_{qr} and all other entries are zero.

7.2 Problem 7
To any $r \in \mathbb{R}$, define rI to be the diagonal matrix with d along the diagonal. To any $A = (a_{ij}) \in M_n(\mathbb{R})$, then we can get $rI \cdot A = A \cdot rI = (ra_{ij})$, thus $rI \in$ the centre.
And to any $A = (a_{ij}) \in$ the centre, consider $H = \sum_{i=1}^{n} E_{i1}AE_{1i}$. By last one, H is a diagonal matrix all of whose diagonal entries equal a_{11}. By A is from the center, $H = \sum_{i=1}^{n} AE_{i1}E_{1i} = A\sum_{i=1}^{n} E_{i1}E_{1i} = A$, thus A is a diagonal matrix all of whose diagonal entries equal a_{11}, that finishes the proof.

7.2 Problem 13
(a) Note the conjugating by g permutes the elements of $\mathcal{K}$, thus $gKg^{-1} = K, thusgK = Kg$. So, to any $\sum_{i=1}^{n} r_i g_i$, $(\sum_{i=1}^{n} r_i g_i)K = \sum_{i=1}^{n} r_i g_i K = \sum_{i=1}^{n} r_i K g_i = \sum_{i=1}^{n} K r_i g_i = K(\sum_{i=1}^{n} r_i g_i)$, thus K is in the centre.

(b) To any $\sum_{i=1}^{n} r_i g_i \in RG$ and α, $\sum_{i=1}^{n} r_i g_i \alpha = \sum_{j=1}^{r}(\sum_{i=1}^{n} r_i g_i)(a_j K_j)$ by (a),
$= \sum_{j=1}^{r}(a_j K_j)(\sum_{i=1}^{n} r_i g_i) = (\sum_{j=1}^{r} a_j K_j)(\sum_{i=1}^{n} r_i g_i) = \alpha(\sum_{i=1}^{n} r_i g_i)$. Thus α is in the center.

Conversely, assume α is in the centre. Since $G = \cup \mathcal{K}_i$, α is in the form of $\sum ak$, where

$k \in \mathcal{K}_i$ for some i and $a \in R$. If $a_i k$ is a sum element of α, where $k \in \mathcal{K}_i$, $a_i \in R$, then since the conjugation permutes the elements of $\mathcal{K}_i$, all the other elements of $\mathcal{K}_i$ times a should also be a sum element since α is fixed under conjugation, thus α is in the form of $\sum_{i=1}^n a_i K_i$.

7.3 Problem 10
(a) Yes (b) No (c) Yes (d) No (e) Yes (f) No.

7.3 Problem 29
To any $x, y \in$ that set and $z \in R$, assume $x^n = 1 = y^m$. Since R is commutative, thus $(xz)^n = x^n z^n = 0z^n = 0$. And $(x-y)^{n+m} = \sum C_{n+m}^i x^i (-y)^{n+m-i}$ Since $i + (n+m-i) = n+m$, either $i \geq n$ or $n+m-i \geq m$, in either case we get $x^i y^{n+m-i} = 0$, thus $(x+y)^{n+m} = 0$. So we get the set is an ideal.

7.3 Problem 33
(a) If $a_1, ...a_n$ are nilpotent and a_0 is a unit, then by 7.1 problem 14 and the sum nilpotent elements is nilpotent, we get it's a unit, since the polynomial is a sum of a nilpotent element and a unit.
Conversely, if the poly is a unit, assume $q(x) = b_m x^m + ...b_0$ and $p(x)q(x) = 1$, then $b_0 a_0 = 1$ thus a_0 is a unit. Now we have $a_n b_m = 0$, $a_{n-1} b_m + a_n b_{m-1} = 0, ..., a_n b_0 + a_{n-1} b_1 + ...a_0 b_n = 0$. By multiplying proper ${a_n}^k$ to each equation, we may conclude that ${a_n}^{m+1-j} b_j = 0$.Thus $(a^n)^{m+1} q(x) = 0$. However $q(x)$ is a unit, which can not be a zero-divisor, thus $(a^n)^{m+1} = 0$, i.e. a_n is a nilpotent, thus $p(x) - a_n x^n$ is a unit, therefore by repeating the last procedure we get a_{n-1} is nilpotent. Keep this procedure, we can conclude all the $a_i, i \neq 0$ are nilpotent.

(b) If each a_i is nilpotent, then each $a_i x^i$ is also a nilpotent element of $R[x]$, then $p(x)$ is a sum of nilpotent elements, thus it's nilpotent by last problem. If $p(x)$ is nilpotent.
Conversely, we can prove by induction. To degree 0, then a_0 is nilpotent by definition. Now we assume to any polynomial with degree $n-1$, if the polynomial is nilpotent then its coefficients are nilpotent. Now to any nilpotent poly with degree n, say $a_n x^n + ...a_1 x + a_0$, and assume $(a_n x^n + ...a_1 x + a_0)^m = 0$, s.t. $a_n^m x^{nm} = 0$, hence $a_n^m = 0$, i.e. a_n is nilpotent, and $a_n x^n$ is nilpotent. By last problem, $a_n x^n + ...a_1 x + a_0 - a_n x^n$ is nilpotent, which is a nilpotent poly with degree $n-1$ thus all its coefficients are nilpotent. Thus any n-degree nilpotent poly's coefficients are nilpotent. That finishes the proof.

7.4 Problem 11
If both I, J are not contained in P, then there exits $i \in I, j \in J$, s.t. $i, j \notin P$, but $ij \in IJ \subset P$, thus either i or j is contained in P, contradiction. Thus either I or J is contained in P.

7.4 Problem 19
To any prime ideal P of R, R/P is a finite integral domain which is a field, thus P is

maximal.

7.4 Problem 30
To any $x, y \in$ that rad$I$ and $z \in R$, assume $x^n, y^m \in I$. Since R is commutative, thus $(xz)^n = x^n z^n \in I$, since $x^n \in I$. And $(x-y)^{n+m} = \sum C^i_{n+m} x^i (-y)^{n+m-i}$ Since $i + (n+m-i) = n+m$, either $i \geq n$ or $n+m-i \geq m$, in either case we get $x^i y^{n+m-i} \in I$, thus $(x+y)^{n+m} \in I$. So we get the rad$I$ is an ideal.
To any $a \cdot I \in (\text{rad}I)/I$, there exits $n \in \mathbb{Z}^*$, s.t. $(a \cdot I)^n = 0$. And any $a \cdot I \in R/I$, s.t. $(a \cdot I)^n = 0$, then $a^n \in I$, so $a \cdot I \in (\text{rad}I)/I$. So by 7.3 exercise 29, $(\text{rad}I)/I = \mathcal{R}(R/I)$.

7.4 Problem 32
(a) Intersections of ideals are ideals so Jac I is an ideal. Since it is the intersection of ideals all of which contain I, then it contains I.

(b) To any maximal ideal M containing $I, R/M$ is a field. If $r \in R, r^n \in I$, then $(r \cdot M)^n \in I \cdot M = M$, so $r^n \in M$, since M is prime, we get $r \in M$. So rad$I \subset$ Jac$I$.

(c) Let $n = p_1^{a_1} p_2^{a_2} ... p_k^{a_k}$, where p_is are distinct prime numbers. Then Jac $n\mathbb{Z} = (p_1) \cap (p_2) \cap ... \cap (p_k) = (p_1 p_2 ... p_k)$.

7.4 Problem 37
To any $r \in R - M$, consider the ideal $< r >$, which is contained in a maximal ideal if $< r > \neq R$. Since R is local, if $< r > \neq R$, $r \in < r > \subset M$, which is a contradiction. Thus $< r > = R$, hence $1 \in < r >$, thus r is a unit.

Conversely, any maximal ideal doesn't contain any units, otherwise it contains 1, which is a contradiction. Thus any maximal ideal is contained in M, hence it equals to M by maximality. Thus there is only one maximal ideal.

7.4 Problem 41
(a) Note $\mathbb{Z}$ is a PID, thus the ideals are in the form of $< x >$, where $x \in \mathbb{Z}$. If $x = p_1^{n_1} ... p_m^{n_m}$, where p_is are distinct prime numbers. Then $p_1 \cdot (p_1^{n_1 - 1} ... p_m^{n_m}) \in < x >$. Obviously, if $m \neq 1$, then to any n, $(p_1^{n_1-1} ... p_m^{n_m})^n, p_1^n \notin < x >$. Thus primary ideals are in the form of $< p^n >$, where p is prime. And obviously, $< p^n >$ and 0 are primary. That finishes the proof.

(b) To a prime ideal P, if $ab \in P$, then either a or b is contained in P, thus every prime ideal is primary.

(c) To any zero divisor of R/Q, say $r + Q$, there exits $s \in R, \notin Q$ s.t. $rs \in Q$, so by the explanation in the question, a positive power of r and a positive power of s both lie in Q, which means there exists $n \in \mathbb{Z}^*$, s.t. $r^n \in Q$, thus $(r+Q)^n = r^n + Q = Q$, i.e. $r+Q$ is a nilpotent element.

(d) To any $ab \in$rad(Q), then there exists $n \in \mathbb{Z}^*$, s.t. $(ab)^n = a^n b^n \in Q$ if either a^n or b^n is contained in Q, then we are done, otherwise we have neither a^n nor b^n is in Q, we have a positive power of a^n and a positive power of b^n both lie in Q, thus either a or b is on rad(Q), which finishes the proof.

7.6 Problem 5

(a) It suffices to show that if $(m,n)=1$ then the ideals (m) and (n) are comaximal. Because, if we knew that this is the case then we know that (n_i) and (n_j) were comaximal, and thus that the Chinese Remainder Theorem applies to the ideals $(n_1),...,(n_k)$. The intersection of these ideals is exactly $(n_1...n_k)$. The equivalences specify an element in $Z/n_1 \times ...Z/n_k$; the fact that there is a unique solutions follows from the fact that this is isomorphic to $Z/n_1...n_k$.
If $(m,n)=1$ then there exist integers a,b such that $am+bn=1$; thus the ideal $(m,n)=\mathbb{Z}$, and (m) and (n) are comaximal, as desired.

(b) Since x is unique it suffices to show that this x satisfies the above equivalences. For any $i, n_i | n'_j$ for $j \neq i$, so

$$x \equiv a_i t_i n'_i \equiv a_i \mod n_i,$$

that finishes the proof.

(c) We have $n'_1 = 2025 \equiv 1 \mod 8$, $n'_2 = 648 \equiv -2 \mod 25$, $n'_3 = 200 \equiv 81 \mod 38$ and $t_1 = 1, t_2 = 12, t_3 = 32$. Thus $x \equiv 1 \cdot 1 \cdot 1 + 2 \cdot 12 \cdot (-2) + 3 \cdot 32 \cdot 38 \equiv 3601 \mod 16200$, and $y \equiv 5 \cdot 1 \cdot 1 + 12 \cdot 12 \cdot (-2) + 47 \cdot 32 \cdot 38 \equiv 8269 \mod 16200$.

7.6 Problem 8

(a) $a \sim a$ since $\rho_{11}(a) = \rho_{11}(a)$. If $a \sim b$, then $\rho_{ik}(a) = \rho_{jk}(b)$, thus $\rho_{jk}(b) = \rho_{ik}(a)$, hence $b \sim a$. If $a \sim b, b \sim c$, then $\rho_{ik}(a) = \rho_{jk}(b)$, $\rho_{kp}(b) = \rho_{tp}(c)$, thus $\rho_{kp} \circ \rho_{ik}(a) = \rho_{tp}(c)$. Thus $a \sim c$. That finishes the proof.

(b) If $\rho_i(a) = \rho_i(b) = \bar{a}$, which implies $\rho_{ij}(a) = d = \rho_{ij}(a)$ for some $d \in A_j$ and some j, which is impossible since ρ_{ij} is injective.

(c) Suppose that $c \in A_q, d \in A_w$, with $\rho_{qt}(c) = \rho_{it}(a), \rho_{ws}(d) = \rho_{js}(b)$. Then $\bar{c} + \bar{d} = \overline{\rho_{tk} \circ \rho_{qt}(c) + \rho_{sk} \circ \rho_{ws}(d)} = \overline{\rho_{qt}(c)} + \overline{\rho_{ws}(d)} = \overline{\rho_{it}(a)} + \overline{\rho_{js}(b)} = \bar{a} + \bar{b}$. Thus it's well-defined. Note to $a \in A_i$, $\bar{a} + \bar{-a} = \overline{\rho_{ii}(a) + \rho_{ii}(-a)} = \overline{a-a} = \bar{0}$. Thus it has inverse. It's easy to see the associativity, thus it's a group, and ρ_i is a group homomorphism since $\rho_i(a+b) = \overline{a+b} = \overline{\rho_{ii}(a) + \rho_{ii}(b)} = \bar{a} + \bar{b} = \rho_i(a) + \rho_i(b)$.

(d) Define the multiplicity by $\bar{a} \cdot \bar{b} = \overline{\rho_{ik}(a) \cdot \rho_{jk}(b)}$, where $a \in A_i, b \in A_j$. Similarly to (b), it's well-defined. Since each A_k is a commutative ring, it's immediate that $\bar{a} \cdot \bar{b} = \overline{\rho_{ik}(a) \cdot \rho_{jk}(b)} = \overline{\rho_{jk}(b) \cdot \rho_{ik}(a)} = \bar{b} \cdot \bar{a}$. Thus A is a commutative ring, and the 1 is defined as $\bar{1}$ (note $\rho_{ik}(1) = \rho_{jk}(1)$).

(e) Define $\phi(\bar{a}) = \phi_i(a)$, where $a \in A_i$. It's easy to see it's well-defined. If there is an alternative homomorphism $\psi : A \to C$, then to any $a \in A_i$, $\psi(\bar{a}) = \psi \circ \rho_i(a) = \phi_i(a) = \phi \circ \rho_i(a) = \phi(\bar{a})$, thus $\psi = \phi$.

7.6 Problem 11

(a) We can identify $(a_1, a_2, ...a_n) \in \varprojlim Z/p^iZ$ as $b_0 + b_1 p + ...b_{n-1}p^{n-1}$, where $b_{i-1} = (a_i \mod p^{i-2})/p^{i-1}$. It's easy to see this satisfies the μ_{ij}. If $(a_1, a_2, ...a_n) \in \varprojlim Z/p^iZ$, $= c_0 + c_1 p + ...c_{m-1}p^{m-1}$. By μ_{ij}, $b_0 + b_1 p + ...b_{n-1}p^{n-1} = c_0 + c_1 p + ...c_{m-1}p^{m-1}$, which shows the uniqueness. We can use the pullback of the addition and multiplication in $\{b_0 + b_1 p + ...b_{n-1}p^{n-1}\}$ to define the addition and multiplication in Z_p.

(b) Let's prove by induction, first note $0 = 0$, we assume $n \in Z, = b_0 + b_1 p + ...b_{n-1}p^{n-1}$, then $n+1$, if $b_0 < p-1$, then $n + 1 = (b_0 + 1) + b_1 p + ...b_{n-1}p^{n-1}$, otherwise, $n + 1 = 0 + (b_1 + 1)p + ...b_{n-1}p^{n-1} = (b_1 + 1)p + ...b_{n-1}p^{n-1}$, and we can repeat what we just did to $b_1, ...b_{n-1}$, in particular, if $n + 1 = (b_{n-1} + 1)p^{n-1}$ and $b_{n-1} + 1 = p$, then $n + 1 = p^n$. Thus we have any $n \in Z$ is contained in Z_p.

(c) If $(b_0 + b_1 p + ...b_{n-1}p^{n-1}) \cdot c_0 + c_1 p + ...c_{m-1}p^{m-1} = 1$, thus $(b_0 + b_1 p + ...b_{n-1}p^{n-1}) \cdot (c_0 + c_1 p + ...c_{m-1}p^{m-1}) \mod p = 1$, thus $b_0 \cdot c_0 \mod p = 1$, thus $b_0 \neq 0$.
If $b_0 + b_1 p + ...b_{n-1}p^{n-1})$ is with $b_0 \neq 0$, then by 7.2 problem $3-(c)$, it is a unit.

(d) By problem (a), we identify each $(a_1, a_2, ...a_n, ...) \in Z_p$ as $b_0 + b_1 p + ...b_{n-1}p^{n-1} + ...$, then $p(a_1, a_2, ...a_n, ...) = b_0 p + b_1 p^2 + ...b_{n-1}p^n + ...$, thus $Z_p/pZ_p = \{0, 1, ...p\} = Z/pZ$.
To any non-zero ideal I, let p^k is the largest p^i dividing all the elements in I. Thus $I \subset (p^k)$
Assume $a \in I$, s.t. $a = bp^k$, where $p \not| b$, then by (c), b is a unit. Thus $p^k = b^{-1}a \in I$, thus $I = (p^k)$.
Since $Z_p/(p^k Z_p) = Z/p^k Z$ is a field iff $k = 1$, thus pZ_p is the unique maximal ideal.

(e) Define $a = (a_1, a_2, ...a_n, ...)$. Obviously, a_i satisfies the requirement by Fermat's little theorem. Assume $a_{i-1}^{p-1} \equiv 1 \mod p^{i-1}$. There is always some $\bar{b_i} \in Z/p^iZ$ s.t. $\mu_{i,i-1}(\bar{b_i}) = a_{i-1}$. We consider the $\bar{b_i}^p$ in Z/p^iZ. And define $a_i := \overline{b_i}^p$. Note $\mu_{i,1}(a_i) = \mu_{i-1,1} \circ \mu_{i,i-1}(a_i) = \mu_{i-1,1} \circ \mu_{i,i-1}(\overline{b_i}^p) = \mu_{i-1,1}(a_{i-1}{}^p)$ by the homomorphism property, and note in $\mod p^{i-1}$, by $a_{i-1}^{p-1} \equiv 1 \mod p^{i-1}$, we have $a_{i-1}^p \equiv a_{i-1} \mod p^{i-1}$, thus $\mu_{i,1}(a_i) = \mu_{i-1,1}(a_{i-1}{}^p) = \mu_{i-1,1}(a_{i-1})$. So $\mu_{i,1}(a_i) = a_1$.

Now we need to show that $a_i^{p-1} \equiv 1 \mod p^i$. Note $a_i^{p-1} = (\overline{b_i}^p)^{p-1}$ and by the definition of $\bar{b_i}$, we have $\bar{b_i} = a_{i-1} + qp^i$ for some q, thus $a_i^{p-1} = (a_{i-1} + qp^i)^{p^{p-1}}$. Note in Z/p^iZ, $(a_{i-1} + qp^i)^p \equiv a_{i-1}^p$. So $a_i^{p-1} \equiv (a_{i-1}^p)^{p-1}$. And by assumption $a_{i-1}^{p-1} \equiv 1 \mod p^{i-1}$, $a_{i-1}^{p-1} = 1 + kp^{i-1}$, for some k. So $a_i^{p-1} \equiv (a_{i-1}^p)^{p-1} = (1 + kp^{i-1})^p$, where $(1 + kp^{i-1})^p \equiv 1 \mod p^i$. Therefore $a_i^{p-1} \equiv 1 \mod p^i$. That finishes the induction, i.e. we found such an $a = (a_1, a_2, ...a_n, ...)$.

To each $n \in Z/nZ$ with $n \neq 0$, we can construct an A_n as we did above. Note, they are different, since each a_1 is different. And to any such $a = (a_1, a_2, ...a_i, ...)$, we have $a^{p-1} = (a_i^{p-1}) = (1)$. So there are $n - 1$ roots of $x^{n-1} = 1$.

8.1 Problem 8

(a) For $D = -1$ the proof is in the text. First, suppose that $D = -3, -7, -11$; then $O = Z[\frac{1+\sqrt{D}}{2}]$; we can write this as the set of numbers $\frac{a}{2} + \frac{b}{2}\sqrt{D}$, where $a, b \in \mathbb{Z}$ and $a \equiv b \mod 2$. Let $\alpha = a + b\sqrt{D}$ and let $\beta = c + d\sqrt{D}$. Write $\gamma = \alpha/\beta = r + s\sqrt{D}$. Let n be an integer, which is closest to the rational number s, and let m be an integer that minimizes $|r - m - n/2|$. We let $\delta = m + n\frac{1+\sqrt{D}}{2} \in O$. We claim that $N(\alpha - \beta\delta) < N(\beta)$, which gives us the Euclidean algorithm. $N(\alpha - \beta\delta) = N(\beta)N(\gamma - \delta)$, so it suffices to check that $N(\gamma - \delta) < 1$. We have
$N(\gamma - \delta) = N((r - m - n/2) + (s - n/2)\sqrt{D}) = (r - m - n/2)^2 + |D|(s - n/2)^2 \leq 1/4 + |D|/16 = \frac{4+|D|}{16} < 1$.
Now if $D = -2$. We do the same process as above to define γ, but then we choose m and n so that $|s - n|$ and $|r - m|$ are minimized. Then again we just need to check that $N(\gamma - \delta) < 1$. But $N(\gamma - \delta) = (r - m)^2 + 2(s - n)^2 \leq \frac{1}{4} + \frac{2}{4} < 1$. That finishes the proof.

8.1 Problem 9

First of all, it is clear that $Z[\sqrt{2}]$ is an integral domain since it is contained in R. For each element $a + \sqrt{2}b \in Z[\sqrt{2}]$, define $N(a + \sqrt{2}b) = |a^2 - 2b^2|$ to be a norm. Also, it is multiplicative: $N(xy) = N(x)N(y)$. Now we can show the existence of a Division Algorithm as follows. Let $x = a + b\sqrt{2}$ and $y = c + d\sqrt{2}$ be arbitrary elements in $Z[\sqrt{2}]$, where $a, b, c, d \in Z$. We have:
$\frac{x}{y} = \frac{a+b\sqrt{2}}{c+d\sqrt{2}} = \frac{(ac-2bd)+(bc-ad)\sqrt{2}}{c^2-2d^2} = r + s\sqrt{2}$, where $r = \frac{ac-2bd}{c^2-2d^2}$ and $s = \frac{bc-ad}{c^2-2d^2}$. Let m be an integer closest to the rational number r and let n be an integer closest to the rational number s, so that

$$|r - m| \leq \frac{1}{2} \text{ and } |s - n| \leq \frac{1}{2}.$$

Let $t := r - n + (s - m)\sqrt{2}$. Then we have $t = r + s\sqrt{2} - (n + m\sqrt{2}) = \frac{x}{y} - (n + m\sqrt{2})y$.
$yt = x - (n + m\sqrt{2})y \in Z[\sqrt{2}]$.
Thus we have $x = (n + m\sqrt{2})y + yt$ $(*)$, with $n + m\sqrt{2}, yt \in Z[\sqrt{2}]$.

We have $N(t) = |(r-n)^2 - 2(s-m)^2| \leq |r-n|^2 + 2|s-m|^2 \leq \frac{1}{4} + 2 \cdot \frac{1}{4} = \frac{3}{4}$.It follows from the multiplicativity of the norm N that $N(yt) = N(y)N(t) \leq \frac{3}{4}N(y) < N(y)$. Thus the expression $(*)$ gives a Division Algorithm with quotient $n + m\sqrt{2}$ and remainder yt.

8.2 Problem 6

(a) Let S be the set of all ideals of R that are not principal, and let $C_{k k\in I}$ be a totally ordered set (under inclusion) in S. The chain $C_{k k\in I}$ has as upper bound $\cup_{s_k \in I} C_k$, which is a ideal by the union of ideals is an ideal. If this union is principal, then we assume it is $< d >$ but d would have to stay in some C_k for some k, implying $C_k =< d >$, a contradiction, thus the union is not principal. Thus every totally ordered set in S has an upper bound, a maximal element of S exists by Zorn's Lemma.

(b) Note $I \subset I_a$ but $I \neq I_a$, thus by maximality, I_a has to be principal. Similarly I_b is principal, say $= (\alpha)$. And by definition of J we have $I \subset J$, and by $bI_a \subset I$, we have $b \in J$, thus $I \subsetneq I_b \subset J$, so by maximality, J is principal, say $= (\beta)$.

Now we have $I_a J = (\alpha)(\beta) = (\alpha\beta)$, and by the definition of J, we have $I_a J \subset I$.

(c) Note $I \subset I_a = (\alpha)$, thus any $x \in I$, we have $x = s\alpha$, by the definition of J, $s \in J$. Thus $I \subset I_a J$. Thus $I = I_a J = (\alpha\beta)$, contradiction. Thus R is a PID.

8.3 Problem 6

(a) To any $a + bi \in Z[i]/(1+i)$, $a + bi = a - b$. Thus any element can be represented by an integer. Note $1 = 1 \cdot 1 = (-i) \cdot (-i) = -1$, i.e. $2 = 0$, Thus every even integer is 0 and every odd integer equals to 1. Thus we can get every element is either 1 or 0. Thus $Z[i]/(1+i)$ is a field of order 2.

(b) Note (q) is prime (since q is prime and the ideal generated by prime element is prime), thus $Z[i]/(q)$ is an integral domain. Also note $a + bi \in Z[i]/(q)$, $a, b \mod q$, thus there are $q \times q = q^2$ elements in $Z[i]/(q)$. Therefore $Z[i]/(q)$ is a finite integral domain, which is hence a field.

(c) With the same reason as (b), $Z[i]/(p)$ has order p^2. Since $\pi, \bar{\pi}$ are coprime ($\pi, \bar{\pi}$ are irreducible by proposition 18), and $Z[i]$ is a PID, there exists $a, b \in Z[i]$, s.t. $a\pi + b\bar{\pi} = 1$, thus comaximal. Thus by Chinese remainder theorem, $Z[i]/(p) \cong Z[i]/(\pi) \times Z[i]/(\bar{\pi})$. Note $Z[i]/(\pi), Z[i]/(\bar{\pi})$ are symmetrical, thus $|Z[i]/(\pi)| = |Z[i]/(\bar{\pi})| = p$.

9.1: Problems 5

$Z[x,y]/ < x, y > \cong Z$, which is a domain and hence $< x, y >$ is a prime ideal.
$Z[x,y]/ < 2, x, y > \cong Z/2Z$, which is a field and hence $< 2, x, y >$ is a maximal ideal. That finishes the proof.

9.1: Problems 17

If I is a homogeneous ideal, consider the generating set A, and B as the set of the homogeneous components of the elements in A. By definition, $B \subset I$, so $(B) \subset I$. But $I = (A) \subset (B)$, so $(B) = I$, hence I is generated by homogeneous polynomials.

Conversely, if I is generated by homogeneous polynomials, say $\{a_i\}_{i \in T}$. To any poly $p(x)$ in I, we can express as $\sum(g_{i,1} + g_{i,m_i})a_i$, where each g_{i,m_j} is homogeneous, and recall each a_i is also homogeneous, thus each $g_{i,m_j}a_l$ is homogeneous. assume the minimum degree of polys in I is k. Then if $p \in I$ is of degree k, its homogeneous component is itself, so its homogeneous component is in I. Now assume any poly in I with degree n is with each homogeneous component is also in I. Now to any poly in I with degree $n+1$, we can express $\sum h_i a_i + \sum k_i a_i$, where $\sum h_i a_i$ is the part of degree at most n, and the $\sum k_i a_i$ is the homogeneous component of degree $n+1$. Note $\sum h_i a_i \in I$, by induction its each homogeneous component is in I and $\sum k_i a_i \in I$, thus we finished the induction, i.e. I is homogeneous.

9.2: Problems 5

By the Fourth Isomorphism Theorem for rings, $I/(p(x))$ is an ideal of $F[x]/(p(x))$ if and only if I is an ideal of $F[x]$ containing $p(x)$. Since $F[x]$ is a PID, we get $I = (f(x))$ for some $f(x) \in F[x]$. Since $(p(x)) \subset (f(x))$, we have $f(x)|p(x)$. Note $F[x]$ is a UFD, thus we can factorise $p(x) = p_1(x)...p_n(x)$. Then any ideal $I/(p(x))$ is in the form of $(g_1(x), ...g_m(x))/(p(x))$, where $g_i(x)s$ are distinct elements of $\{p_1(x), ...p_n(x)\}$.

10.1: Problems 19

Since the $F[x]$-submodules of V are precisely the T-invariant subspace of V. We see that $T(0) = 0 \in V$, $T(V) \subset V, T(x\text{-axis}) = 0 \subset x\text{-axis}$ and $T(y\text{-axis}) = y\text{-axis} \subset y\text{-axis}$. Hence, these are $F[x]$-modules.

To a submodule W, if $(t, z) \in W$ with $t, z \neq 0$, then $x \cdot (t, z) = (t, 0)$, thus x-axis is in W. And by $(t, z) + (n, 0)$ for any $n \in R$, we have $y = z$ is in W, to any $m \in R$, $\frac{m}{z} \cdot (t, z) = (\frac{m}{z}t, m) \in W$, thus by above $y = m$ is in W. Thus $W = V$.

Now if W doesn't contain $(t, z) \in W$ with $t, z \neq 0$, then it's easy to see $W = 0$ or y-axis or x-axis by F-action.

10.2: Problems 13

Since I is nilpotent, we assume $I^r = 0$. By $\bar{\psi}$ is onto, any $n + IN \in N/IN$, we have $m \in M$, s.t. $\bar{\psi}(m + IM) = n + IN$. Thus $n + IN \in \psi(M) + IN$. By $N = \cup n + IN, n \in N$, we have $N = \psi(M) + IN$. Thus $N = \psi(M) + I(\psi(M) + IN) = \psi(M) + I^2N$. Keep doing this, we get $N = \psi(M) + I^rN = \psi(M)$. That finishes the proof.

10.3: Problems 23

Let $\{M_i\}_{i\in I}$ be a collection of free R-modules, each with basis A_i. We claim that $\bigoplus_{i\in I} M_i$ is free over $\cup_{i\in I} A_i$. Letting $m \bigoplus_{i\in I} M_i$ we know we can write m as a finite sum $m = m_{i1} + ... + m_{ik}$ with $m_{ij} \in M_{ij}$. Furthermore this expression of m is unique since the coordinates in a direct sum are independent. But each m_{ij} has a unique representation over the basis A_{ij}. Hence we can express m over the basis $\cup_{i\in I} A_i$, and furthermore this representation of m is unique. This proves the result.

10.3: Problems 27

(a) $\varphi_1\psi_1(a_1, a_2, ...) = \varphi_1(a_1, 0, a_2, 0, ...) = (a_1, a_2, ...)$, i.e. $\varphi_1\psi_1 = 1$. Similarly, $\varphi_2\psi_2 = 1$. $\varphi_1\psi_2(a_1, a_2, ...) = \varphi_1(0, a_1, 0, a_2, 0, ...) = (0, 0, ...)$, thus $\varphi_1\psi_2 = 0$, similarly, $\varphi_2\psi_1 = 0$. And $(\psi_1\varphi_1 + \psi_2\varphi_2)(a_1, a_2, ...) = (a_1, 0, a_3, 0...) + (0, a_2, 0, a_4, ...) = (a_1, a_2, a_3, ...)$, thus $\psi_1\varphi_1 + \psi_2\varphi_2 = 1$.

Now if $a_1, a_2 \in R$, we assume $a_1\varphi_1 + a_2\varphi_2 = 0$, then $a_1 = (a_1\varphi_1 + a_2\varphi_2)\psi_1 = 0$, similarly, $a_2 = (a_1\varphi_1 + a_2\varphi_2)\psi_2 = 0$, thus φ_1, φ_2 are independent. Note to any $x \in R$, we have $(x\psi_1)\varphi_1 + (x\psi_2)\varphi_2 = x$. Thus φ_1, φ_2 generate R.

(b) By part (a), we have $R \cong R^2$, and by induction, to any n, we have $R \cong R^n$.

10.4: Problems 1

First it's easy to see $s \cdot t \in S$ for any $s \in S, t \in R$. Note $s \cdot 1 = s \times f(1) = s \times 1 = s$. And $s \cdot (xy) = sf(xy) = sf(x)f(y) = (s \cdot x) \cdot y$. So $s \cdot r = sf(r)$ defines a right R-action on S. And there is a canonical left S-action on S by multiplication. Thus S is a (S, R)-bimodule.

10.4: Problems 7

Any $\frac{m}{d} \otimes t \in Q \otimes_R N$, since Q is also an R-module, we have $\frac{m}{d} \otimes t = m(\frac{1}{d} \otimes t) = \frac{1}{d} \otimes m \cdot t$. And $d \in R, m \cdot t \in N$. That finishes the proof.

10.4: Problems 25

Define $f : S \otimes_R R[x] \to S[x]$ by $f(s, p(x)) \mapsto sp(x)$. Note by $f((s_1 \otimes p_1(x))(s_2 \otimes p_2(x)) = f(s_1s_2 \otimes p_1(x)p_2(x)) = s_1s_2p_1(x)p_2(x) = f(s_1 \otimes p_1(x))f(s_2 \otimes p_2(x))$. And it's easy to see that $f(a(s \otimes p(x)) = af(s \otimes p(x))$. Thus f is an algebra-homomorphism.

f is onto, since any $p(x) \in S[x]$ is in the form of $\sum_{i=1}^n a_i x^i$, then $f(\sum_{i=1}^n a_i \otimes x^i) = \sum_{i=1}^n a_i x^i = p(x)$.

If $f(\sum a_i \otimes x^i) = 0$, then $\sum a_i x^i = 0$, thus $a_i = 0$ for each i, thus $\sum a_i \otimes x^i = 0$, hence f is injective, thus f is an isomorphism.

10.5: Problems 12

(a) There is a canonical injection $I_i : B_i \to \bigoplus_{i\in I} B_i$. Then it induces a map

$$\varphi_i : Hom_R(\bigoplus_{i\in I} B_i, A) \to Hom_R(B_i, A)$$

by sending $\alpha \mapsto \alpha \circ I_i$. Note $Hom_R(\bigoplus_{i\in I} B_i, A)$ and $\prod_i Hom_R(B_i, A)$ are abelian groups, by the universal property of the direct product of abelian groups, there is a homomorphism

$$\Phi : Hom_R(\bigoplus_{i\in I} B_i, A) \to \prod_i Hom_R(B_i, A),$$

s.t. $\pi_i \circ \Phi = \varphi_i$, where π_i is the i^{th} natural projection from the direct product.
If $\Phi(a) = 0$, then $a \circ I_i = \varphi_i(a) = \pi_i \circ \Phi(a) = 0$, thus $a = 0$, thus Φ is injective.
To $\phi = \prod_i \phi_i \in \prod_i Hom_R(B_i, A)$. Define $a_\phi : \oplus_I B_i \to A$ by $a_\phi(b_i) = \sum \phi_i(b_i)$. It's easy to see $a_\phi \in Hom_R(\bigoplus_{i\in I} B_i, A)$. Now $\pi_i(\Phi(a_\phi))(b) = \varphi_i(a_\phi)(b) = a_\phi(I_i(b)) = \phi_i(b)$, thus $\Phi(a_\phi) = \phi$, thus Φ is onto.
Now to any $r \in R$, $\Phi(ra) = \prod_i((ra) \circ I_i) = \prod_i(ra \circ I_i) = r\prod_i(a \circ I_i) = r\Phi(a)$, thus Φ is an R-module homomorphism, hence R-module isomorphism.

(b) We define $\varphi_i : Hom_R(A, \prod_i B_i) \to Hom_R(A, B_i)$ by $\varphi_i(a) = \pi_i \circ a$. Now by the universal property of the direct product of abelian groups, there is a homomorphism

$$\Phi : Hom_R(A, \prod_i B_i) \to \prod_i Hom_R(A, B_i)$$

s.t. $\pi_i \circ \Phi = \varphi_i$. Similar to part (a), we have Φ is injective and also a R-module homomorphism.
Now consider $\phi = \prod_i \phi_i \in \prod_i Hom_R(A, B_i)$. Define $a_\phi : A \prod_i B_i$ as $\pi_i a_\phi(b) = \phi_i(b)$. Clearly, a_ϕ is a homomorphism. $\pi_i\Phi(a_\phi)(b) = \varphi_i a_\phi(b) = \pi_i a_\phi(b) = \phi_i(b)$.Therefore $\pi_i\Phi(a_\phi) = \phi_i$, thus $\Phi(a_\phi) = \phi$. Thus Φ is onto, that finishes the proof.

10.5: Problems 16
(a) Since M is an abelian group, thus M is a Z-module, by Corollary 37, M is contained in an injective Z-module Q.

(b) Since $M \subset Q$, there is an inclusion $i : M \to Q$, which induces a map $i^* : Hom_Z(R, M) \to Hom_Z(R, Q)$ by composition any $\phi \in Hom_Z(R, M)$ to $i \circ \phi \in Hom_Z(R, Q)$.
Any $f \in Hom_R(R, M)$, is also an abelian group homomorphism since R, M are abelian groups, and an abelian group homomorphism is a $Z-$ module homomorphism, thus $f \in Hom_Z(R, M)$, thus $Hom_R(R, M) \subset Hom_Z(R, M)$. That finishes the proof.

(c) If M is an R-module, by exercise 10.5.10(b) we have $M \cong Hom_R(R, M)$. By (b), we have $M \subset Hom_Z(R, Q)$. But 10.5.15(c) says that if Q in an injective Z-module, $Hom_Z(R, Q)$ is an injective R-module. Hence, we proved that M is contained in an injective R-module.

10.5: Problems 21
If $0 \to A \to B \to C \to 0$ is an exact sequence of left S-modules, then by N is flat as an

S-module, we have:

$$0 \to N \otimes_S A \to N \otimes_S B \to N \otimes_S C \to 0,$$

which can be seen as an exact sequence of left R-modules.
By M is a right R-module, we have

$$0 \to M \otimes_R (N \otimes_S A) \to M \otimes_R (N \otimes_S B) \to M \otimes_R (N \otimes_S C) \to 0.$$

By tensor product associativity, we have:

$$0 \to (M \otimes_R N) \otimes_S A \to (M \otimes_R N) \otimes_S B \to (M \otimes_R N) \otimes_S C \to 0.$$

Therefore $M \otimes_R N$ is flar as a right S-module.

10.5: Problems 25
(a) There is an exact sequence $0 \to I \to R \to R/I \to 0$. If A is flat, then $0 \to A \otimes_R I \to A \otimes_R R \to A \otimes_R R/I \to 0$ is exact, thus $A \otimes_R I \to A \otimes_R R$ is injective.

(b) (1) Suppose now that the element $\sum a_i \otimes_R I_i \in A \otimes_R I$ is mapped to 0 by $1 \otimes \psi$. This means that the element $\sum a_i \otimes_R \psi(I_i)$, can be written as a sum of generators. Since this sum of elements is finite, all of the second coordinates of the resulting equation lie in some finitely generated submodule I' of I. Then this equation implies that $\sum a_i \otimes_R I_i \in A \otimes_R I'$ is mapped to 0 in $A \otimes_R R$. Since I' is a finitely generated module, the injectivity by assumption shows that $\sum a_i \otimes_R I_i$ is 0 in $A \otimes_R I'$ and also in in $A \otimes_R I$.

(2) Assume $F \cong R^n$, then $K \cong R^n/I$, by $A \otimes F \cong A^n$, and $K \cong A^n/A \otimes I$, it's easy to see $K \cong A^n/A \otimes I \to A^n \cong A \otimes F$ is injective. (Note by $A \otimes R \cong A$, the map $A \otimes I \to AI$ is onto, so now it's an isomorphism.)

(3) Similar to (1), if the element $\sum a_i \otimes_R k_i \in A \otimes_R K$ is mapped to 0, then by this sum of elements is finite, $\sum a_i \otimes_R k_i$ is contained in some $A \otimes_R K'$, where K' is a sub-module of a finitely generated free sub-module $F' \subset F$ ($K' := K \cap F'$, thus is also contained in K) and is mapped to $0 \in A \otimes_R F'$, and by (2), $\sum a_i \otimes_R k_i = 0$ in $0 \in A \otimes_R K'$ and also in in $A \otimes_R K$.

(c) For the first diagram, the map $g : J \to L$ can be defined as $\psi^{-1} \circ f$ (note ψ is injective), and note the image of K in F is just $ker f$, thus $K \subset f^{-1}(\psi(L) = J$, hence the map $p : K \to J$ (induced by $h : K \to F$) is the inclusion. Moreover since ϕ is injective, $ker \psi^{-1} \circ f = ker f$, which is just the image of K in J, thus the top sequence of the first diagram is exact. Note $\psi \circ g(a) = \psi \circ \psi^{-1} \circ f = f\iota(a)$, and $\iota \circ p(a) = \iota \circ f(a) = p(a) = p \circ id(a)$. Thus the first diagram is commutative.
For the second diagram, recall the tensor product is right exact, thus this diagram is commutative with exact rows.

Now by (b), $1 \otimes \iota$ is injective, and by part (d) of exercise 1, $1 \otimes \psi$ is injective, thus by the definition of flatness, A is flat.

(d) Since F is flat, by (a), $F \otimes_R I \to F \otimes_R R \cong F$ is injective, thus $F \otimes I \subset F \otimes R$ is mapped to FI by $f \otimes i \mapsto fi$, therefore K as a submodule of F, the image of $K \otimes I$ is just KI by the injectivity and $k \otimes i \mapsto ki$.
Tensor I with the exact sequence $0 \to K \to F \to A \to 0$, recall tensor product is right exact, thus we get the exact sequence $K \otimes I \xrightarrow{f} F \otimes I \xrightarrow{g} A \otimes I \to 0$. Note the image of $K \otimes I$ is just KI, thus by exactness $A \otimes I = F \otimes I / kerg = F \otimes I / Imf = F \otimes I / K \otimes I = FI/KI$.

(1) If $FI \cap K = KI$, then $A \otimes I = FI/KI = FI/(FI \cap K)$. Consider the quotient map $\phi : F \to A$ and the restriction to FI, which sends $\sum f_j i_j$ to $\phi(\sum f_j i_j) = \sum \phi(f_j) i_j \in AI$, it's easy to see $\phi(FI) = AI$. Since $ker\phi = K$, we have $ker\phi|_{FI} = K \cap FI$, thus $FI/(FI \cap K) \cong (F/K)I = AI$, thus $A \otimes I \cong AI$, thus A is flat.

(2) If A is flat, then $A \otimes I = AI$, thus $FI/KI = (F/K)I \cong FI/(FI \cap K)$, hence $FI/KI \cong FI/(FI \cap K)$, also note $KI \subset FI \cap K$, thus $FI \cap K = KI$.