Matroid Theory

Alec Zabel-Mena
Text - Welsh, Dominic J. Matroid Theory

Chapter 1

Fundamental of Matroid Theory.

1.1 Definitions

We go over some fundamental definitions and theorems for matroids.

Definition 1.1.1 (The Independence Axioms)**.** We define a **matroid** M to be a set S, called the **ground set**, together with a collection $\mathcal{I} \subseteq 2^S$ of subsets of S which we call **independent sets** to such that;

(I1) $\emptyset \in \mathcal{I}$.

(I2) If $X \in \mathcal{I}$ and $Y \subseteq X$, then $Y \in \mathcal{I}$. (Inheretence)

(I2) If $X, Y \in \mathcal{I}$ such that $|Y| < |X|$, then ther is an $x \in X \backslash Y$ such that $Y \cup x \in \mathcal{I}$. (Augmentation)

There is one immediate example for a matroid.

Example 1.1.1. Let V be a finite vector space and let $\mathcal{I}$ be the collection of all linearly independent subsets of vectors of V. Clearly $\emptyset \in V$, and if X is linearly independent, and $Y \subseteq X$, then Y is also linearly independent; so inheretence is satisfied.

Now let X be linearly independent, then $\operatorname{span} S$ must also be linearly independent. Now take $\beta \in V \backslash \operatorname{span} S$ and for $\alpha_1, \ldots, \alpha_m \in S$ take

$$c_1\alpha_1 + \cdots + c_2\alpha_2 + b\beta = 0$$

If $b \neq 0$, then

$$\beta = (-\frac{c_1}{b})\alpha_1 + \cdots + (-\frac{c_m}{b})\alpha_m$$

putting $\beta \in \operatorname{span} S$, a contradiction, hence $b = 0$, and so $S \cup \beta$ is also linearly independent. Thus the augmentation axiom is satisfied and V is a matroid together with $\mathcal{I}$.

We define some additional concepts, all of which can be used in the definition of a matroid.

Definition 1.1.2. A **base** of a matroid M is a maximally independent subset of S. We denote the collection of bases of M by $\mathcal{B}$. We say a subset of S is **spanning** in M if it contains a base.

Definition 1.1.3. We define the **rank function** of a matroid to be the map $\operatorname{rank} : 2^S \to \mathbb{Z}$ defined by

$$\operatorname{rank} A = \max\{|X| : X \in \mathcal{I} \text{ and } X \subseteq A\} \tag{1.1}$$

We define the **rank** of the matroid to be $\operatorname{rank} M = \operatorname{rank} S$. We say $A \subseteq S$ is **closed**, or a **flat**, or a **subspace** of M if for all $x \in S \backslash A$, $\operatorname{rank} A \cup x = \operatorname{rank} A + 1$, and we say x **depends** on A.

Definition 1.1.4. We define the **closure operator** of a matroid to be the map $\operatorname{cl} : 2^S \to 2^S$ defined such that $\operatorname{cl} A$is the set of all elements which depend on A; that is

$$\operatorname{cl} A = \{x \in S \backslash A : \operatorname{rank} A \cup x = \operatorname{rank} A + 1\}. \tag{1.2}$$

Definition 1.1.5. A **dependent set** of a matroid is a subset $D \subseteq S$ which is not independent; this is $D \notin \mathcal{I}$. A **circuit** of a matroid is a minimally dependent set, and we denote the collection of all circuits as $\mathcal{C}$.

Now one thing that makes matroids so interesting, is that they can be axiomatically defined in various ways. We can not only define them in terms of independence, bu also in terms of bases, circuits, rank, and closure. We give the theorems below that establish the axioms.

Theorem 1.1.1 (The Base Axioms)**.** *A nonempty collection $\mathcal{B}$ of subsesets of a set S forms a set of bases of a matroid M on S if, and only if for:*

(B1) $B_1, B_2 \in \mathcal{B}$*, and* $x \in B_1 \backslash B_2$*, there is a* $y \in B_2 \backslash B_1$ *such that* $(B_1 \cup y) \backslash x \in \mathcal{B}$.

Theorem 1.1.2 (The Circuit Axioms)**.** *A nonempty collection $\mathcal{C}$ of subsesets of a set S forms a set of circuits of a matroid M on S if, and only if:*

(C1) If $Y \in \mathcal{C}$ *and* $X \neq Y$*, then* $X \nsubseteq Y$.

(C2) If $C_1, C_2 \in \mathcal{C}$ *are distinct, and* $z \in C_1 \cap C_2$*, then there is a circuit* $C_3 \in \mathcal{C}$ *such that* $C_3 \subseteq (C_1 \cup C_2) \backslash z$.

Theorem 1.1.3 (The First Rank Axioms)**.** *Let S be a set. A map* $\operatorname{rank} : 2^S \to \mathbb{Z}$ *is the rank function of a matroid on S if and only if for $X \subseteq S$ and $y, z \in S$*

(R1) $\operatorname{rank} \emptyset = 1$.

(R2) $\operatorname{rank} X \leq \operatorname{rank} X \cup y \leq \operatorname{rank} X + 1$.

(R3) If $\operatorname{rank} X \cup y = \operatorname{rank} X \cup z = \operatorname{rank} X$*, then* $x \cup y \cup z = \operatorname{rank} X$.

Theorem 1.1.4 (The Second Rank Axioms)**.** *Let S be a set. A map* $\operatorname{rank} : 2^S \to \mathbb{Z}$ *is the rank function of a matroid on S if and only if for $X, Y \subseteq S$*

(R′1) $0 \leq \operatorname{rank} X \leq |X|$.

(R′2) If XY*, then* $\operatorname{rank} X \leq \operatorname{rank} Y$

(R3̀) $\operatorname{rank} X \cup Y + \operatorname{rank} X \cap Y \leq \operatorname{rank} X + \operatorname{rank} Y$.

Theorem 1.1.5 (The Closure Axioms)**.** *Let S be a set. A map $\operatorname{cl} : 2^S \to 2^S$ is the closure operator of a matroid on S if and only if for $X, Y \subseteq S$, and $x, y \in S$*

(S1) $X \subseteq \operatorname{cl} X$.

(S2) *If* $Y \subseteq X$, *then* $\operatorname{cl} Y \subseteq \operatorname{cl} X$.

(S3) $\operatorname{cl} X = \operatorname{cl}(\operatorname{cl} X)$.

1. *If* $y \notin \operatorname{cl} X$ *and* $y \in \operatorname{cl}(X \cup x)$, *then* $x \in \operatorname{cl}(X cupy)$.

We defer their proofs to the relevant sections.
We can already provea fact about matroids.

Proposition 1.1.6. *If an element of a matroid belongs to every base, then it can belong to no circuit of the matroid.*

Proof. Let M be a matroid and let $\mathcal{B}$ be the collection of all bases of M, $\mathcal{C}$ the collection of all circuits of M, and $\mathcal{I}$ the collection of all independent sets of M. Take $x \in X = \bigcap_{B \in \mathcal{B}} B$ and suppose that $x \in C$ for $C \in \mathcal{C}$. By theorem 1.1.1, we have that $X \neq \emptyset$, moreover since $x \in C$, $C \subseteq X$, i.e $C \in \mathcal{B}$. mow notice that since C is a circuit, it is dependent, so $C \notin \mathcal{I}$, but we have that $C \in \mathcal{B}$ which makes it a base, and hence independent; so $C \in \mathcal{I}$, a contradiction. □

Definition 1.1.6. We say that two matroids M_1 and M_2 on S_1 and S_2 respectively are **isomorphic** if there is a $1-1$ map $\phi : S_1 \to S_2$ of S_1 onto S_2 such that if $X \subseteq S_1$ is independent in M_1, then $\phi(X) \subseteq S_2$ is independent in M_2. We write $M_1 \simeq M_2$ to denote isomorphism.

Example 1.1.2. We list all nonisomorphic matroids on a set of n elements for $n = 1, 2, 3$.

$\underline{n=1}$ For $S = \{1\}$, we have $M_1 = \emptyset$ and $M_2 = 2^S$. There are $2^1 = 2$ matroids on S.

$\underline{n=2}$ On $S = \{1, 2\}$we have

$$\begin{aligned} M_1 &= \emptyset \\ M_2 &= \{\emptyset, \{1\}\} \\ M_3 &= \{\emptyset\{1\}, \{2\}\} \\ M_4 &= \{\emptyset, \{1\}, \{2\}, \{1, 2\}\} = 2^S \end{aligned}$$

there are $2^2 = 4$ matroids on S

<u>$n = 3$</u> For $S = \{1, 2, 3\}$ we have

$$
\begin{aligned}
&M_1 = \emptyset\\
&M_2 = \{\emptyset, \{1\}\}\\
&M_3 = \{\emptyset\{1\}, \{2\}\}\\
&M_4 = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}\\
&M_5 = \{\emptyset, \{1\}, \{2\}, \{3\}\}\\
&M_6 = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}\}\\
&M_7 = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}\}\\
&M_8 = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\} = 2^S
\end{aligned}
$$

There are $2^3 = 8$ matroids on S.

Now one might be tempted to generalize that there are a total of 2^n matroids on a given n element set, however a quick check for $n = 4$ concludes that that is not the case.

<u>$n = 4$</u> For $S = \{1, 2, 3, 4\}$ we have

$$
\begin{aligned}
M_1 &= \emptyset\\
M_2 &= \{\emptyset, \{1\}\}\\
M_3 &= \{\emptyset\{1\}, \{2\}\}\\
M_4 &= \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}\\
M_5 &= \{\emptyset, \{1\}, \{2\}, \{3\}\}\\
M_6 &= \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}\}\\
M_7 &= \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}\}\\
M_8 &= \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}\\
M_9 &= \{\emptyset, \{1\}, \{2\}, \{3\}, \{4\}\}\\
M_{10} &= \{\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{1, 2\}, \{1, 3\}, \{1, 4\}\}\\
M_{11} &= \{\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}\}\\
M_{12} &= \{\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}\}\\
M_{13} &= \{\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}, \{1, 2, 3\}\}\\
M_{14} &= \{\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}, \{1, 2, 3\}, \{1, 2, 4\}\}\\
M_{15} &= \{\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}, \{1, 2, 3\}, \{1, 2, 4\}\{1, 3, 4\}\}\\
M_{16} &= \{\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}, \{1, 2, 3\}, \{1, 2, 4\}\{1, 3, 4\},\\
&\quad \{2, 3, 4\}\}\\
M_{17} &= \{\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}, \{1, 2, 3\}, \{1, 2, 4\}\{1, 3, 4\},\\
&\quad \{2, 3, 4\}, \{1, 2, 3, 4\}\} = 2^S
\end{aligned}
$$

Notice that $S = \{1, 2, 3, 4\}$ has $17 = 2^4 + 1$ matroids.

We conclude the section with an additional axiomatic definition for a matroid. This definition relies on the concept of an "independence function", which was postulated and shown by Rado.

Definition 1.1.7 (The Independence Function Axioms)**.** A map $f : 2^S \to \mathbb{Z}/2\mathbb{Z}$ on the set of finite sequences of elements of S is an **independence function** if for any $n \in \mathbb{Z}^+$ and sequences $\{x_i\}_{i=1}^n, \{y_i\}_{i=1}^{n+1}$ of S the folowing hold:

(IF1) $f(\emptyset) = 1$

(IF2) f is decreasing.

(IF3) f is commutative, i.e. for any permutation $i \to \alpha i$ of $\{1, \dots, n\}$

$$f(\{x_i\}) = f(\{x_{\alpha i}\}) \tag{1.3}$$

(IF4) f is non reflexive, i.e. $f(x, x) = 0$ for all $x \in S$.

(IF5) f is distributive; that is

$$f(\{x_i\})f(\{y_i\}) \leq \sum_{i=1}^{n+1} f(\{x_i\}, y_i) \tag{1.4}$$

Theorem 1.1.7. *Let S be a set and $f : 2^S \to \mathbb{Z}/2\mathbb{Z}$ be an independence function. Define $\mathcal{I}$ to be the collection of sequences finite $\{x_i\}_{i=1}^n$ of S such that $f(\{x_i\}) = 1$. Then $\mathcal{I}$ forms a matroid on S. Conversely, if M is a matroid on S with independence set $\mathcal{I}$, then there is a map $f : 2^S \to \mathbb{Z}/2\mathbb{Z}$ satisfying the independence function axioms.*

1.2 Examples

We define some matroids, and observe the properties of a peculiar one.

Proposition 1.2.1. *Let S be a set with $|S| = n$ and define $\mathcal{I} = \{X \subseteq S : |X| \leq k\}$ for $k \leq n$. Then S is a matroid on S.*

Proof. Clearly $\emptyset \in \mathcal{I}$, and if X is independent, and $Y \subseteq X$, then $|Y| \leq |X| \leq k$, hence $Y \in \mathcal{I}$.

Now take $Y, X \in \mathcal{I}$ with $|Y| < |X|$. Now if $|Y| + 1 = |X| = k$, the result is clear. Otherwise, choose an $x \imath X \backslash Y$, then since $|Y| < k$, $|Y \cup x| \leq k$, and hence is independent. □

Definition 1.2.1. We call the matroids on a set S, generated by the collection $\mathcal{I} = \{X \subseteq S : |X| \leq\}$ the **uniform matroid** of rank k on S; and we denote it $U_{n,k}$.

We discuss some properties of the uniform matroid.

Corollary. $\mathcal{B}(U_{n,k}) = \{X \subseteq S : |X| = k\}$ *and* $\mathcal{C}(U_{n,k}) = \{X \subseteq S : |X| = k + 1\}$

Proof. If $B \in \mathcal{I}(U_{n,k})$ is a base, then $|B| \leq k$ and by the maximality of B for any $x \in S \backslash B$, $B \cup x \notin \mathcal{I}$, i.e. $|B \cup x| = |B| + 1 > k$. It follows that $|B| = k$. Likewise by the same reasoning we see by the minimality of any circuit $C \in \mathcal{C}$ that $|C| = k + 1$ □

Remark. Since any base, and any dependent set in $U_{n,k}$ has size $\geq k$, it is easy to see that any set A with $|A| \geq k$ is spanning in $U_{n,k}$.

Corollary. *For any* $A \subseteq U_{n,k}$ $\operatorname{rank} A = \begin{cases} |A|, & \text{if } |A| \leq k \\ k, & \text{if } |A| > k \end{cases}$ *and* $\operatorname{cl} A = \begin{cases} A, & \text{if } |A| < k \\ S, & \text{if } |A| \geq k \end{cases}$

Proof. By definition, we have that $\operatorname{rank} A = \max\{|X| : X \subseteq A, |X| \leq k\}$. Now if A is independent, then $\operatorname{rank} A = A$. If A is dependent, well since every dependent set of $U_{n,k}$ is spanning, choose a base $B \subseteq A$. Then $\operatorname{rank} A = \operatorname{rank} B = k$.

Now by the closure axioms, $A \subseteq \operatorname{cl} A \subseteq S$. Suppose that $|A| < k$, and take $x \in \operatorname{cl} A$, then $\operatorname{rank} A \cup x = \operatorname{rank} A + 1 = |A| + 1$, hence $\operatorname{rank} A = |A|$, thus $x \in A$, so $\operatorname{cl} A = A$. Now if $|A| \geq k$, then for any $x \in S \backslash A$, $\operatorname{rank} A \cup x = \operatorname{rank} A + 1 \geq k + 1 > |A| + 1$, this puts $x \in \operatorname{cl} A$, and bu consequence $S \subseteq \operatorname{cl} A$. Therefore $\operatorname{cl} A = S$. □

Corollary. $\operatorname{rank} U_{n,k} = k$.

In the example 1.1.1 of section 1.1, we showed that a collection of linearlt independent subsets of vectors of a vector space forms a matroid over that vector space.

Definition 1.2.2. Let V be a finite vector space, and let M be the matroid on V formed by taking all linearly independent subsets of vectors of V. We call a matroid isomorphic to M **vectorial**.

Proposition 1.2.2. *The rank of a vectorial matroid is the dimension of the vector space that it is isomorphic to.*

Proof. Since $\dim V = |B|$, where B is a basis of linearly independent vectors of V, it is easy to see that $\operatorname{rank} M = \dim V$. □

Definition 1.2.3. Let G be a graph with edge set E, and let $X \in \mathcal{I}$ if and only if X contains no cycle of G. Then $\mathcal{I}$ is a collection of independent sets of a matroid, which we call the **cycle matroid** on G and denote it $M(G)$.

We defer the proof that the cycle is indeed a matroid for when we talk about matroids on graphs.

Example 1.2.1. The complete graph K_3 has as it's cycle matroid the matroid $U_{3,2}$ see figure 1.1.

We now talk about matroids arising from algebra. we give some proofs, but these matroids will be discussed when approrpiate.

Definition 1.2.4. Let F be a field and K be an extension of F. We call a subset $\{x_1, \ldots, x_k\} \subseteq K$ of K **algebraically dependent** if there is a polynomial f with coefficients in F such that $f(x_1, dots, x_k) = 0$. Otherwise we say they are **algebraically independent**.

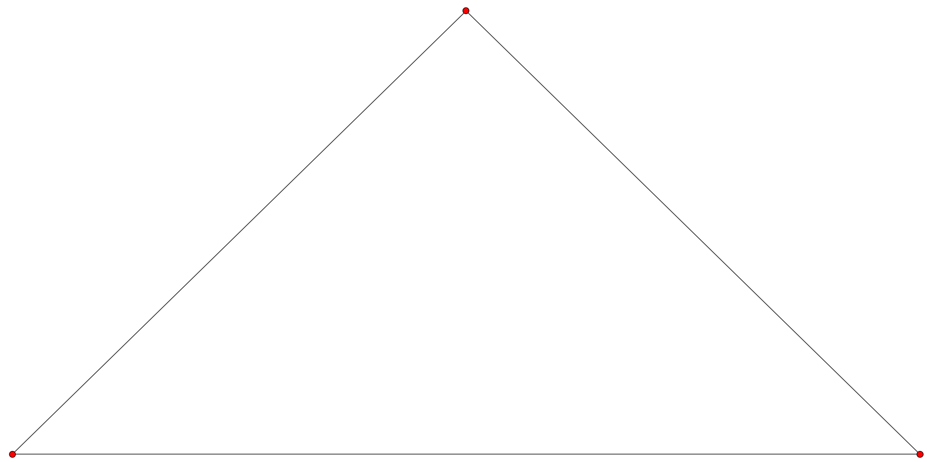

Figure 1.1: The complete graph K_3.

Theorem 1.2.3. *Let F be a field, K an extension of F, and let $S \subseteq K$ be finite. For any $X \subseteq S$, let $X \in \mathcal{I}$ if and only if X is algebraically independent. Then $\mathcal{I}$ forms a matroid over S..*

Proof. Clearly $\emptyset$ is algebraically independent. Now suppose that X is algebraically independent, and that YX. Then for every polynomial in X, $f \neq 0$. We have then there is a polyomial $g \in Y$ with $g \neq 0$ for which $f = g + h$ hence Y is algebraically independent.

Now suppose that $X = \{x_1, \ldots, x_k\}$ and $Y = \{y_1, \ldots, y_m\}$ are algebraically independent, with $m < k$, so that $|Y| < |X|$. Now for every polynomial in X, f, $f(x_1, \ldots, x_k) \neq 0$, and for every polynomial g in Y, $g(y_1, \ldots, y_m) \neq 0$. Now we can find a polynomial f_1 in X such that $f = f_1(x_i) + f_2(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_k)$, where $f_1(x_i) \neq 0$, for $x_i \in X \backslash Y$ (if $X \cap Y = \emptyset$, then choose any x_i), then $f_1 \neq 0$ and $g \neq 0$ implies that $f(x_i) + g(y_1, \ldots, y_m) \neq 0$, then we see that $Y \cup x_i$ is also algebraically independent, whc=ich completes the proof. $\square$

Definition 1.2.5. Let F be a field, K a field extension of F, and $S \subseteq K$ be finite. The collection of all algebraically independent subsets of S form a matroid on S. We call these matroids **algebraic**.

Definition 1.2.6. We call an element of Euclidean d-space, $x \in \mathbb{R}^d$ **affinely dependent** on a subset $\{x_1, \ldots, x_r\} \subseteq \mathbb{R}^d$ if there exist real numbers λ_i for $1 \leq i \leq r$ such that:

$$\sum \lambda_i = 1 \tag{1.5}$$

and

$$x = \sum \lambda_i x_i \tag{1.6}$$

We call a subset $X \subseteq \mathbb{R}^d$ **affinely independent** if no element $x \in X$ is affinely dependent on $X \backslash x$.

Theorem 1.2.4. *Let $S \subseteq \mathbb{R}^d$. Then the collection of all affinely independent subsets of S form a matroid on S.*

Proof. Clearly $\emptyset$ is affinely indipendent, trivially. Let X be affinely independent, and let $Y \subseteq X$. Then for $x \in X$ and $\{x_1, \dots, x_r\} \subseteq X$ with $x \neq x_i$ for $1 \leq i \leq r$, there are no real nubers λ_i for which $\sum \lambda_i = 1$ and $x = \sum \lambda_i x_i$. Now if $x \in Y$, take $\{y_1, \dots, y_s\} \subseteq \{x_1, \dots, x_r\}$ and we are done. Now take $y \neq x \in Y$, and again take $\{y_1, \dots, y_s\} \subseteq \{x_1, \dots, x_r\}$ and where $y \neq y_j$ for $1 \leq j \leq s$. Now if there are realnumbers γ_j for which $\sum \gamma_j = 1$ and $y = \sum \gamma_j y_j$, then by inclusion, we can find addition γ_i for which $x = \sum \gamma_i x_i$, a contradiction; so Y must also be affinely independent.

Now let X and Y be affinely independent with $|Y| < |X|$, then for $y \in Y$ and $x \in X$ and $\{x_1, \dots, x_r\}$, $\{y_1, \dots, y_s\}$ (not necessarily disjoint) with $x_i \neq x$ and $y_j \neq y$ for $1 \leq i \leq r$ and $1]leqj \leq s$, there are no real numbers λ_i and γ_j for which $\sum \lambda_i = \sum \gamma_j = 1$ and $x = \sum \lambda_i x_i$ and $y = \sum \gamma_j y_j$. Now if there is indeed a λ_i and $x_i \notin \{y_1, \dots, y_s\}$ for which $y = \lambda_i x_i + \sum \gamma_i y_i$, that would imply that we can find real numbers λ_i for which $x = \sum \lambda_i$ which cannot happen. Thus $Y \cup x_i$ must be affinely independent. $\square$

Definition 1.2.7. Let J be an abelian torsion group. An element $g \in J$ is called **dependent** if for elements $g_1, \dots, g_n \in J$ and integers $m \neq 0, k_1, \dots, k_m$ we have

$$mg = k_1 g_1 + \cdots + k_n g_n. \tag{1.7}$$

A subset $Y \subseteq J$ is **independent** if there is no $y \in Y$ for which y is dependent on $Y \backslash y$.

We defer the proof of this theorem.

1.3 Loops and Parallel elements.