Journal of Number Theory **97**, 1–9 (2002)
doi:10.1006/jnth.2002.2793

A Generalization of an Addition Theorem of Kneser

Xiang-Dong Hou

Department of Mathematics and Statistics, Wright State University, Dayton, Ohio 45435

Ka Hin Leung[1]

Department of Mathematics, National University of Singapore, Kent Ridge, Singapore, 119260
E-mail: matllkh@nus.edu.sg

and

Qing Xiang

Department of Mathematical Sciences, University of Delaware, Newark, Delaware 19716

Communicated by A. Granville

Received March 6, 2000; revised March 24, 2001

A theorem of Kneser states that in an abelian group G, if A and B are finite subsets in G and $AB = \{ab : a \in A, b \in B\}$, then $|AB| \geqslant |A| + |B| - |H(AB)|$ where $H(AB) = \{g \in G : g(AB) = AB\}$. Motivated by the study of a problem in finite fields, we prove an analogous result for vector spaces over a field E in an extension field K of E. Our proof is algebraic and it gives an immediate proof of Kneser's Theorem. © 2002 Elsevier Science (USA)

Key Words: finite field; Kneser's theorem; the Cauchy–Davenport theorem; the Dyson e-transform.

1. INTRODUCTION

Let G be an abelian group, written multiplicatively, and let A, B and S be nonempty subsets of G. By AB we denote the set $\{ab \mid a \in A,\ b \in B\}$. The *stabilizer* of S, denoted by $H(S)$, is defined as the set $\{g \in G \mid gS = S\}$. It is clear that $H(S)$ is the largest subgroup of G such that $H(S)S = S$ and that S is a union of $H(S)$-cosets. In 1953, Kneser [3] proved the following beautiful theorem about sums of finite subsets of an abelian group.

[1] To whom correspondence should be addressed.

0022-314X/02 $35.00

THEOREM 1.1 (Kneser). *Let G be an abelian group and let A, B be nonempty, finite subsets of G. Then*

$$|AB| \geqslant |A| + |B| - |H(AB)|,$$

where $AB = \{ab \mid a \in A, b \in B\}$, and $H(AB)$ is the stabilizer of AB.

In the special case where G is a finite cyclic group of prime order, Kneser's theorem implies the Cauchy–Davenport theorem which asserts that if p is prime, and A, B are nonempty subsets of $\mathbb{Z}/p\mathbb{Z}$, then $|A + B| \geqslant \min\{p, |A| + |B| - 1\}$, where $A + B = \{a + b \mid a \in A, b \in B\}$.

Theorem 1.1 has the following equivalent formulation.

THEOREM 1.2 (Kneser). *Let G be an abelian group, and let A, B be finite nonempty subsets of G. Let $H = H(AB)$ be the stabilizer of AB. If $|AB| < |A| + |B|$, then $|AB| = |AH| + |BH| - |H|$.*

For the proofs of Theorems 1.1 and 1.2, we refer the reader to [5, p. 115, 131] (see also [4]). For convenience, we will refer Theorem 1.1 as Kneser's theorem in this paper. Kneser's theorem has many applications in additive number theory (see [5, Sects. 4.3, 4.4]). While it is relatively easy to prove the Cauchy–Davenport theorem, the proof of Kneser's theorem is much more involved (cf. [5]). Motivated by a problem about subspaces in finite fields (for detailed statement of the problem, see Section 4), we prove a vector space analogue of Kneser's theorem (see Theorem 2.4). It turns out that the vector space analogue we proved implies the original Kneser's theorem, hence we may view this vector space analogue as a generalization of Kneser's theorem. Furthermore, except for the Dyson e-transform that we use, the original idea in the proof of Kneser's theorem cannot be generalized to give a proof for Theorem 2.4. Instead, we need to employ a technique to get around the problem. Even though our technique does not work in the most general situation, our result is good enough for many applications, especially for those who work only on finite fields. As an illustration, we use Theorem 2.4 to solve our problem about subspaces in finite fields. This gives a simpler proof for the main result in [2].

2. A VECTOR SPACE ANALOGUE OF KNESER'S THEOREM

Let $E \subset K$ be fields, and let A, B be two E-subspaces of K. By AB we denote the E-subspace of K spanned by $\{ab \mid a \in A, b \in B\}$. In this section, we consider the following problem. Given the dimensions of A and B over E, what can we say about $\dim_E AB$? Our result is presented in Theorem 2.4

which can be viewed as a vector space analogue of Kneser's theorem. We first prove the following lemma. The proof uses a tool analogous to the Dyson e-transform for a pair of subsets of an abelian group.

LEMMA 2.1. *Let $E \subset K$ be fields and let A, B be E-subspaces of K such that $0 < \dim_E A < \infty$ and $0 < \dim_E B < \infty$. Then for each nonzero $a \in A$, there exist a subfield H_a of K containing E and an H_a-vector space $V_a \subset AB$ such that $aB \subset V_a$ and*

$$\dim_E V_a + \dim_E H_a \geqslant \dim_E A + \dim_E B. \tag{2.1}$$

Proof. It suffices to prove the lemma in the case $a = 1$. For general $0 \neq a \in A$, we may replace A by $a^{-1}A$, and apply the result obtained in the case $a = 1$ to the E-spaces $a^{-1}A, B$. For the same reason, we may further assume that $1 \in B$.

We will use induction on $\dim_E A$. If $\dim_E A = 1$, take $V = B$ and $H = E$, the conclusion follows. Now assume $\dim_E A > 1$. For each $0 \neq e \in B$, let

$$A(e) = A \cap Be^{-1} \qquad \text{and} \qquad B(e) = B + Ae. \tag{2.2}$$

Note that $A(e)B(e) \subset AB$ and $\dim_E A(e) + \dim_E B(e) = \dim_E A + \dim_E B$. We consider the following two cases.

Case 1: *$A(e) = A$ for all $0 \neq e \in B$.* Then $A \subset Be^{-1}$ for all $0 \neq e \in B$, i.e., $AB \subset B$. Let H be the subfield of K generated by A and let $V = B$. Then V is an H-vector space and $B \subset V \subset AB$, and

$$\dim_E V + \dim_E H \geqslant \dim_E A + \dim_E B. \tag{2.3}$$

Case 2: *$A(e) \neq A$ for some $0 \neq e \in B$.* Then $0 < \dim_E A(e) < \dim_E A$ and $1 \in A(e)$, $1 \in B(e)$. By the induction hypothesis, there exist a subfield H of K containing E and an H-vector space $V \subset A(e)B(e) \subset AB$ such that $B \subset B(e) \subset V$ and

$$\begin{aligned}\dim_E V + \dim_E H &\geqslant \dim_E A(e) + \dim_E B(e)\\ &= \dim_E A + \dim_E B.\end{aligned} \tag{2.4}$$

This completes the proof. ∎

LEMMA 2.2. *Let V be an n-dimensional vector space over an infinite field E. Suppose that $x_1, x_2, \ldots, x_n$ form a basis of V over E. Then any n vectors in the set*

$$\{x_1 + \alpha x_2 + \cdots + \alpha^{n-1} x_n \mid \alpha \in E\}$$

form a basis of V over E.

Proof. This follows from the Vandermonde determinant. ∎

LEMMA 2.3. *Suppose E is a finite field and K is a field containing E. Let t be an indeterminate over K. Then every finite extension of $E((t))$ in $K((t))$ is of the form $F((t))$, where F is an intermediate field of $E \subset K$.*

Proof. Let $v : K((t)) \to \mathbb{Z}$ be the discrete valuation with $v(t) = 1$ and $v(K^*) = 0$. It is well known that $K((t))$ is complete with respect to v. Suppose M is a finite extension of $E((t))$ in $K((t))$. Then the residue field of M must be a finite extension of E, the residue field of $E((t))$. Therefore, the residue field of M is finite. By an exercise in [1, p. 81], it is known that $M = F((t))$ where F is a finite field in $K((t))$. Clearly, we have $F \subset K$. This completes the proof. ∎

We are now ready to prove our main result.

THEOREM 2.4. *Let $E \subset K$ be fields and let A, B be finite-dimensional E-subspaces of K such that $A \neq \{0\}$, $B \neq \{0\}$. Suppose that every algebraic element in K is separable over E. Then*

$$\dim_E AB \geqslant \dim_E A + \dim_E B - \dim_E H(AB), \tag{2.5}$$

where $H(AB) = \{x \in K \mid xAB \subseteq AB\}$ is the stabilizer of AB in K.

Proof. It suffices to prove the theorem when $H(AB) = E$. In the general case, let $F = H(AB)$, $A' = FA$, $B' = FB$. Then $A'B' = AB$ and (2.5) will follow from $\dim_F A'B' \geqslant \dim_F A' + \dim_F B' - 1$. Thus we assume that $H(AB) = E$.

First, we assume that $|E|$ is infinite. Let $\{x_1, x_2, \ldots, x_n\}$ be a basis of A over E. For any $\alpha \in E$, we let $x_\alpha = x_1 + \alpha x_2 + \cdots + \alpha^{n-1} x_n$. By Lemma 2.1, there exist a subfield H_α of K containing E and an H_α-vector space $V_\alpha \subset AB$ such that $x_\alpha B \subset V_\alpha$ and $\dim_E V_\alpha + \dim_E H_\alpha \geqslant \dim_E A + \dim_E B$. In particular, we are done if $H_\alpha = E$ for some α.

Clearly, $\dim_E AB$ is finite. Let $E(AB)$ be the subfield of K generated by E and AB, and let F be the algebraic closure of E in $E(AB)$. Observe that as $V_\alpha \neq \{0\}$, we have $H_\alpha x \subset AB$ for some nonzero $x \in AB$. Therefore $H_\alpha \subset E(AB)$.

As $\dim_E V_\alpha$ is finite, $[H_\alpha : E]$ is also finite. Hence

$$H_\alpha \subset F \qquad \text{for every } \alpha \in E.$$

Next we prove that $[F : E]$ is finite. As $\dim_E AB$ is finite, $E(AB)$ is finitely generated over E. If $E(AB) = F$, then F is then a finite extension of E. Otherwise, there exists a field $K' = E(y_1, \ldots, y_r)$ such that K' is purely transcendental over E and $E(AB)$ is algebraic over K'. As $E(AB)$ is finitely generated over E, $[E(AB):K']$ is then finite.

Thus $[F:E] = [F(y_1, \dots, y_r):K'] \leqslant [E(AB):K'] < \infty$.

As F is separable over E, the set $\{H_\alpha \mid \alpha \in E\}$ is finite since $[F:E]$ is finite. In particular, there exist n distinct elements $\alpha_1, \alpha_2, \dots, \alpha_n$ in E such that

$$H_{\alpha_1} = H_{\alpha_2} = \cdots = H_{\alpha_n} = H.$$

By Lemma 2.2, $x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_n}$ form a basis of A. Hence, $AB = V_{\alpha_1} + V_{\alpha_2} + \cdots + V_{\alpha_n}$ is an H-space. If $H \neq E$, then it contradicts to our assumption that $H(AB) = E$. Therefore, $H = E$ and (2.5) follows.

Now, suppose $|E|$ is finite. Let t be an indeterminate. We define $A' = A \otimes E((t))$ and $B' = B \otimes E((t))$. Note that $E((t)), A'$, and B' are all embedded in $K((t))$. It is clear that $\dim_E A = \dim_{E((t))} A'$, $\dim_E B = \dim_{E((t))} B'$ and $A'B' = (AB) \otimes E((t))$. Also by Lemma 2.3, every algebraic element in $K((t))$ over $E((t))$ is separable over $E((t))$. Now $|E((t))|$ is infinite, we may apply the previous argument to deduce that

$$\dim_{E((t))} A'B' \geqslant \dim_{E((t))} A' + \dim_{E((t))} B' - \dim_{E((t))} H(A'B').$$

We are done if we can show that $H(A'B') = H(AB) \otimes E((t))$. The proof of this equality goes as follows. First, it follows from the definitions of $H(AB)$ and $H(A'B')$ that $H(AB) \otimes E((t)) \subset H(A'B')$. Next, by Lemma 2.3, $H(A'B') = F((t))$ where F is a subfield of K. Note that $AB = A'B' \cap K$ is an F-space, we deduce that $F \subset H(AB)$. Consequently, we obtain $F = H(AB)$ and $H(A'B') = H(AB) \otimes E((t))$. This completes the proof. ∎

Remark. (1) Clearly, Theorem 2.4 holds when E is perfect, and in particular, when $\operatorname{char} E = 0$ or $|E|$ is finite.

(2) In the proof of Theorem 2.4, the separability assumption is to ensure that $\{H_\alpha \mid \alpha \in E\}$ is a finite set. From the proof of Lemma 2.1, it is clear that $H_\alpha \subset E(A)$, where $E(A)$ is the subfield of K generated by A over E. Thus, the separability assumption in Theorem 2.4 can be replaced with a weaker assumption that the algebraic closure of E in $E(A)$ is a simple extension over E.

(3) As we will see in Section 3, Theorem 2.4 implies Kneser's theorem. Therefore, we may view Theorem 2.4 as a generalization of Kneser's theorem.

For our later application, we record the following when $|E|$ is finite.

Corollary 2.5. *Let $E \subset K$ be finite fields and let A, B be E-subspaces of K such that $A \neq \{0\}$, $B \neq \{0\}$.*

Then

$$\dim_E AB \geqslant \dim_E A + \dim_E B - \dim_E H(AB),$$

where $H(AB) = \{x \in K \mid xAB \subseteq AB\}$ *is the stabilizer of* AB *in* K.

For completeness, we also prove the following analogue of Theorem 1.2.

THEOREM 2.6. *Let* $E \subset K$ *be fields and let* A, B *be finite-dimensional* E*-subspaces of* K *such that* $A \neq \{0\}$, $B \neq \{0\}$.

Suppose that every algebraic element in K *is separable over* E. *Let* $H = H(AB)$ *be the stabilizer of* AB. *If* $\dim_E AB < \dim_E A + \dim_E B$, *then* $\dim_E AB = \dim_E HA + \dim_E HB - \dim_E H$.

Proof. We apply Theorem 2.4 to the E-subspaces HA, HB in K. Then

$$\dim_E AB \geqslant \dim_E HA + \dim_E HB - \dim_E H. \tag{2.6}$$

Since AB, HA, and HB are all H-spaces, we see that $\dim_E AB$, $\dim_E HA$ and $\dim_E HB$ are multiples of $\dim_E H$. If inequality (2.6) is strict, then $\dim_E AB > \dim_E HA + \dim_E HB \geqslant \dim_E A + \dim_E B$. This contradicts to our assumption that $\dim_E AB < \dim_E A + \dim_E B$. This completes the proof. ∎

Remark. We mention that Theorem 2.6 also implies Theorem 2.4. Hence the two theorems are equivalent. To show that Theorem 2.6 implies Theorem 2.4, we observe that if $\dim_E AB \geqslant \dim_E A + \dim_E B$, then (2.5) of course follows. Otherwise, we apply Theorem 2.6 to the E-subspaces HA, HB in K. Then $\dim_E AB \geqslant \dim_E HA + \dim_E HB - \dim_E H \geqslant \dim_E A + \dim_E B - \dim_E H$.

3. A NEW PROOF OF KNESER'S THEOREM

Let G be as defined in Theorem 1.1. In proving Kneser's theorem, we may assume G is finitely generated. Thus, we may assume

$$G = \langle y_1 \rangle \times \cdots \times \langle y_r \rangle \times \langle z_1 \rangle \times \cdots \times \langle z_k \rangle$$

such that the order of y_i is t_i for each $1 \leqslant i \leqslant r$ and z_j $(1 \leqslant j \leqslant k)$ are torsion free. In other words, $G \cong (\mathbb{Z}/t_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/t_r\mathbb{Z}) \times \mathbb{Z} \times \cdots \times \mathbb{Z}$. Let $x_1, \ldots, x_r$ be algebraically independent over $\mathbb{C}$ and define

$$E = \mathbb{C}(x_1, \ldots, x_r), \qquad F = E[\sqrt[t_1]{x_1}, \ldots, \sqrt[t_r]{x_r}].$$

Let $c_1, \ldots, c_k$ be algebraically independent over F and put $K = F(c_1, \ldots, c_k)$. Obviously, F is the algebraic closure of E in K. Define

$$\begin{array}{llcl} \eta: & G & \rightarrow & K \\ & y_1^{n_1}\cdots y_r^{n_r}z_1^{m_1}\cdots z_k^{m_k} & \mapsto & (\sqrt[t_1]{x_1})^{n_1}\cdots(\sqrt[t_r]{x_r})^{n_r}c_1^{m_1}\cdots c_k^{m_k}, \\ & 0\leqslant n_i\leqslant t_i,\ m_j\in\mathbb{Z}. & & \end{array}$$

Note that $\eta(G)$ is linearly independent over E. For any subset C in G, we define $\Phi(C)=\sum_{g\in C}E\eta(g)$, the E-subspace generated by $\eta(C)$. Observe that $\Phi(CC')=\Phi(C)\Phi(C')$ for any subsets C, C' in G. In particular, when C is a subgroup in G, $\Phi(C)$ is closed under multiplication; if furthermore C is finite, then $\dim_E\Phi(C)$ is also finite, hence $\Phi(C)$ is a subfield in F.

Let $G'=\langle y_1\rangle\times\cdots\times\langle y_r\rangle$. It is now clear that Φ induces a mapping,

$$\begin{array}{lccc} \Phi^*: & \{H\,|\,H \text{ is a subgroup of } G'\} & \rightarrow & \{L\,|\,L \text{ is a field and } E\subset L\subset F\} \\ & H & \mapsto & \Phi(H) \end{array}$$

Obviously, Φ^* is injective.

On the other hand, $\mathrm{Gal}(F/E)\cong G'$. Therefore, the number of subgroups in G' is the same as the number of intermediate subfields in $E\subset F$. This proves that Φ^* is surjective and hence bijective.

Now we are ready to prove Kneser's theorem.

By Theorem 2.4, we obtain

$$\dim_E\Phi(A)\Phi(B)\geqslant\dim_E\Phi(A)+\dim_E\Phi(B)-\dim_E H(\Phi(A)\Phi(B)).$$

As $\dim_E\Phi(A)=|A|$, $\dim_E\Phi(B)=|B|$ and $\dim_E(\Phi(A)\Phi(B))=|AB|$, to finish the proof of Kneser's theorem, it suffice to show that $H(\Phi(A)\Phi(B))=\Phi(H(AB))$, i.e., $H(\Phi(AB))=\Phi(H(AB))$.

First observe that $H(\Phi(AB))\supset\Phi(H(AB))$.

Since $\dim_E H(\Phi(AB))\leqslant\dim_E\Phi(AB)=|AB|<\infty$ and F is the algebraic closure of E in K, we have $H(\Phi(AB))\subset F$. Since Φ^* is surjective, $H(\Phi(AB))=\Phi(H')$ for some subgroup H' of G'. Therefore, $\Phi(H')\Phi(AB)=\Phi(H'(AB))=\Phi(AB)$. Hence, $H'(AB)=AB$. It follows that $H'\subset H(AB)$. This proves that $H(\Phi(AB))=\Phi(H(AB))$.

4. A PROBLEM ABOUT SUBSPACES IN FINITE FIELDS

In a previous paper [2], in the process of determining the range of the parameters of a family of partial difference sets constructed by using Galois rings, we are led to the following problem about subspaces in finite fields. Let $E\subset L$ be finite fields, and let r be a positive integer. What is the maximum dimension of an E-subspace W in L such that $W^r\neq L$? Here W^r is the E-subspace of L spanned by $\{w_1w_2\cdots w_r\,|\,w_i\in W,\ 1\leqslant i\leqslant r\}$. This is actually the problem which motivated much of the research in this paper. In [2], using somewhat lengthy arguments, we prove the following theorem.

THEOREM 4.1. *Let $E \subset L$ be finite fields with $[L:E] = t$ and let r be a positive integer. Let*

$$s(r,t) = \max\{\dim_E W : W \text{ is an } E\text{-subspace of } L \text{ such that } W^r \neq L\},$$

where W^r is the E-subspace of L generated by $\{w_1 w_2 \cdots w_r \mid w_i \in W, 1 \leqslant i \leqslant r\}$. Then

$$s(r,t) = \max_{k|t} k\left(\left\lfloor \frac{\frac{t}{k} - 2}{r} \right\rfloor + 1\right).$$

Here we use Corollary 2.5 to give a much simpler proof.

Proof of Theorem 4.1. For convenience, we define $M(r,t) = \max_{k|t} k(\lfloor \frac{\frac{t}{k}-2}{r} \rfloor + 1)$. For completeness, we first recall the proof that $s(r,t) \geqslant M(r,t)$.

Let F be the field such that $E \subset F \subset L$ and $[F:E] = k$. Write $L = F[x]$, where $x \in L$. Let $n = \lfloor \frac{(t/k)-2}{r} \rfloor$, and let W be the F-subspace of L generated by $\{1, x, \ldots, x^n\}$. Then W^r is the F-subspace generated by $\{1, x, \ldots, x^{nr}\}$, and

$$\dim_E W^r = k(nr+1) = k\left(r\left\lfloor \frac{\frac{t}{k} - 2}{r} \right\rfloor + 1\right) < t. \tag{4.1}$$

Hence, $W^r \neq L$. Therefore $\dim_E W = k(n+1) \leqslant s(r,t)$. Consequently, $M(r,t) \leqslant s(r,t)$.

To prove $s(r,t) \leqslant M(r,t)$, we shall show that if $\dim_E W \geqslant M(r,t) + 1$, then $W^r = L$. Let $K = H(W^r)$ be the stabilizer of W^r. Clearly, K is a subfield in L and $W^r = (KW)^r$. Note also that $H(W^i)W^{r-i} = W^r$ for all $i \leqslant r$. Hence, $H(W^i) \subset K$ for all $i \leqslant r$. It follows that $H((KW)^i) = K$ for all $i \leqslant r$. Thus by Corollary 2.5, we obtain

$$\dim_K (KW)^{i+1} \geqslant \dim_K KW + \dim_K (KW)^i - 1$$

for all $i \leqslant r-1$. Therefore, $\dim_K (KW)^r \geqslant r \cdot \dim_K KW - (r-1)$. Let $k = \dim_E K$. As $\dim_E W \geqslant M(r,t) + 1$ and $\dim_E KW$ is a multiple of k, $\dim_K KW \geqslant (\lfloor \frac{\frac{t}{k}-2}{r} \rfloor + 2)$.

Hence

$$\dim_K (KW)^r \geqslant r \left\lfloor \frac{\frac{t}{k} - 2}{r} \right\rfloor + (r+1) \geqslant r \left(\frac{\frac{t}{k} - 2}{r} - \frac{r-1}{r} \right) + (r+1) = \frac{t}{k}.$$

Therefore, $W^r = (KW)^r = L$. ▮

REFERENCES

1. J. W. S. Cassels, "Local Fields," London Mathematical Society Students Texts, Vol. 3, Cambridge Univ. Press, Cambridge, New York, 1986.
2. X. D. Hou, K. H. Leung, and Q. Xiang, New partial difference sets in $Z_{p^2}^t$ and a related problem about Galois rings, *Finite Fields Appl.*, **7** (2001), 165–188.
3. M. Kneser, Abschätzung der asymptotischen Dichte von Summenmengen, *Math. Zeit.* **58** (1953), 459–484.
4. H. B. Mann, "Addition Theorems," Wiley, New York, 1965.
5. M. B. Nathanson, "Additive Number Theory, Inverse Problems and the Geometry of Sumsets," Springer, New York, 1996.