به نام خدا

امتحان میان ترم جبر کار بسته ۱

(۲۲ اردیبهشت ماه ۱۳۸۹)

۱. (الف) گروه دوری را تعریف کنید. یک گروه دوری و یک گروه غیر دوری مثال بزنید (با اثبات ادعاها).

(ب) فرض کنید a عضوی از گروه G با مرتبه‌ی n باشد، نشان دهید $\langle a\rangle = \{e, a, a^2, \ldots, a^{n-1}\}$.

(۱۵ نمره)

۲. نشان دهید هر زیر گروه یک گروه دوری مجددا دوری است.

(۱۰ نمره)

۳. (قضیه‌ی لاگرانژ) فرض کنید H زیر گروهی از گروه متناهی G باشد. در این صورت $|G : H| = \frac{|G|}{|H|}$.

(۱۰ نمره)

۴. (الف) فرض کنید H زیرگروه نرمالی از گروه G باشد. نشان دهید زیرگروه‌های G/H به صورت K/H هستند، که در آن K زیرگروهی از G شامل H است.

(ب) نشان دهید $H = \{1, \rho^2\}$ زیرگروه نرمالی از D_8 است و زیرگروه‌های D_8/H را بیابید.

(۲۰ نمره)

۵. دستگاه رمز قالبی با طول قالب ۲، که قالب P_1P_2 از متن اصلی را به قالب متن رمز C_1C_2 تبدیل می‌کند، به صورت زیر در اختیار است

$$\begin{cases} C_1 = 3P_1 + 4P_2 \\ C_2 = P_1 + 7P_2. \end{cases}$$

(الف) متن BE CAREFUL را رمزگذاری کنید

(ب) با استفاده از آلگوریتم اقلیدسی وارون ۱۷ در $\mathbb{Z}_{26}$ را بیابید.

(ب) متن رمز WACJJVUU را رمزگشایی کنید.

(۲۵ نمره)

موفق باشید

وقت: ۹۰ دقیقه

ارزش امتحان: ۸۰ نمره (از ۲۰۰ نمره)

به نام خدا

امتحان پایان ترم جبر کار بسته

(۱۲ دی ماه ۱۳۹۰)

۱. فرض کنید G یک گروه متناهی باشد و $H \leq G$. ثابت کنید

(آ) $\left|\bigcup_{g \in G} g^{-1} H g\right| \leq 1 + |G| + |G : H|$.

(ب) اگر H از هر رده‌ی G حداقل یک عضو داشته باشد، آن‌گاه $G = H$.

(۲۰ نمره)

۲. فرض کنید N یک زیرگروه نرمال از گروه G باشد. نشان دهید که هر زیرگروه G/N به صورت K/N است، که در آن $N \leq K \leq G$.

(۱۵ نمره)

۳. همه‌ی چندجمله‌ای‌های تحویل‌ناپذیر از درجه‌های ۳ و ۴ روی $\mathbb{Z}_2$ را بیابید.

(۱۵ نمره)

۴. یک میدان متناهی از مرتبه‌ی ۸ بسازید جدول ضرب آن‌را بنویسید. مولد گروه ضربی آن‌را بیابید.

(۲۰ نمره)

۵. فرض کنید M یک ایدآل از حلقه‌ی جابجایی و یکدار R باشد. نشان دهید M ایدآل ماکسیمال است اگر و تنها اگر R/M یک میدان باشد.

(۱۵ نمره)

۶. فرض کنید ماتریس

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

ماتریس امتحان توازن کد خطی C روی $\mathbb{Z}_2$ باشد. فاصله‌ی می‌نیمم C، ماتریس مولد، پیشروی هم‌مجموعه‌ها و سندرم‌هارا بیابید. واژه‌ی $u = 111001$ را کدگشایی کنید.

(۲۰ نمره)

۷. (الف) فرض کنید C یک کد خطی روی $\mathbb{F}_q$ به طول n و فاصله‌ی می‌نیمم d باشد. نشان دهید که C یک کد t-یابنده‌ی خطا است اگر و تنها اگر $t + 1 \leq d$. هم‌چنین C یک کد t-تصحیح کننده‌ی خطا است اگر و تنها اگر $2t + 1 \leq d$.

(۲۰ نمره)

موفق باشید

وقت: ۱۲۰ دقیقه

ارزش امتحان: ۱۲۵ نمره (از ۲۰۰ نمره)

به نام خدا

امتحان میان ترم جبر کار بسته ۱

(۲ آذر ماه ۱۳۹۰)

۱. دستگاه رمز قالبی با طول قالب ۲، که قالب $P_۱P_۲$ از متن اصلی را به قالب متن رمز $C_۱C_۲$ تبدیل می‌کند، به صورت زیر در اختیار است

$$\begin{cases} C_۱ = ۳P_۱ + ۴P_۲ \\ C_۲ = P_۱ + ۷P_۲. \end{cases}$$

(الف) متن SALAM را رمزگذاری کنید

(ب) متن رمز KCFRBD را رمزگشایی کنید.

(۲۰ نمره)

۲. دستگاه رمز کوله پشتی بر اساس دنباله‌ی $(۲, ۳, ۶, ۱۲)$ با پیمانه‌ی ۲۵ و ضرب‌گر $m = ۴$ را در نظر بگیرید.

(آ) متن رمز متناظر با REPLY را بیابید.

(ب) متن اصلی متناظر با متن رمز $(۸, ۱۲, ۱۸, ۱۹, ۲۰)$ را بیابید.

(۱۵ نمره)

۳. (الف) فرض کنید a عضوی از گروه G با مرتبه‌ی n باشد، نشان دهید $O(a^k) = \frac{n}{(n,k)}$.

(۱۰ نمره)

۴. فرض کنید که G یک گروه دوری متناهی از مرتبه‌ی n باشد. نشان دهید به ازای هر شمارنده‌ی s از n یک و تنها یک زیرگروه از مرتبه‌ی s در G وجود دارد.

(۱۰ نمره)

۵. (الف) فرض کنید H زیر گروهی از گروه G باشد. نشان دهید رابطه‌ی $a \equiv b$ اگر و تنها اگر $a^{-۱}b \in H$ یک رابطه‌ی هم‌ارزی روی G است و رده‌های هم‌ارزی را بیابید.

(ب) اگر G متناهی باشد، نشان دهید $|G| = |G : H||H|$.

(۱۵ نمره)

۶. نشان دهید اگر F یک میدان متناهی باشد، $F \setminus \{۰\}$ یک گروه دوری است.

(۱۰ نمره)

موفق باشید

وقت: ۹۰ دقیقه

ارزش امتحان: ۸۰ نمره (از ۲۰۰ نمره)

حرف	معادل دهدهی	معادل دودویی	حرف	معادل دهده‌ی	معادل دودویی
A	۰۰	۰۰۰۰۰	N	۱۳	۰۱۱۰۱
B	۰۱	۰۰۰۰۱	O	۱۴	۰۱۱۱۰
C	۰۲	۰۰۰۱۰	P	۱۵	۰۱۱۱۱
D	۰۳	۰۰۰۱۱	Q	۱۶	۱۰۰۰۰
E	۰۴	۰۰۱۰۰	R	۱۷	۱۰۰۰۱
F	۰۵	۰۰۱۰۱	S	۱۸	۱۰۰۱۰
G	۰۶	۰۰۱۱۰	T	۱۹	۱۰۰۱۱
H	۰۷	۰۰۱۱۱	U	۲۰	۱۰۱۰۰
I	۰۸	۰۱۰۰۰	V	۲۱	۱۰۱۰۱
J	۱۹	۰۱۰۰۱	W	۲۲	۱۰۱۱۰
K	۱۰	۰۱۰۱۰	X	۲۳	۱۰۱۱۱
L	۱۱	۰۱۰۱۱	Y	۲۴	۱۱۰۰۰
M	۱۲	۰۱۱۰۰	Z	۲۵	۱۱۰۰۱

به نام خدا

امتحان پایان ترم جبر کار بسته ۱

(۱۷ خرداد ماه ۱۳۸۹)

۱. چندجمله‌ای‌های $f(x)=x^{۷}+۲x^{۵}+۲x^{۴}+۲x^{۳}+x+۱$ و $g(x)=x^{۴}+x^{۳}+۲x^{۲}+x+۱$ در $\mathbb{Z}_{۳}[x]$ مفروض هستند. بزرگترین مقسوم‌علیه مشترک $f(x)$ و $g(x)$ را بیابید و آن‌را برحسب ترکیب خطی $f(x)$ و $g(x)$ بنویسید.

(۲۰ نمره)

۲. فرض کنید ماتریس

$$G=\begin{bmatrix} ۰ & ۱ & ۰ & ۰ & ۱ \\ ۰ & ۰ & ۱ & ۰ & ۱ \\ ۱ & ۰ & ۱ & ۱ & ۱ \end{bmatrix}$$

ماتریس مولد کد خطی C به طول ۵ روی $\mathbb{Z}_{۲}$ باشد. فاصله‌ی می‌نیمم C، ماتریس امتحان توازن و همه‌ی کد واژه‌های C را بیابید. هم‌مجموعه‌های C در $\mathbb{Z}_{۲}^{۵}$، پیشروی هم‌مجموعه‌ها، سندرم‌هارا بیابید و واژه‌ی $u=۰۱۰۰۱$ را کدگشایی کنید.

(۳۰ نمره)

۳. (الف) اگر C یک کد خطی t-تصحیح کننده‌ی خطا به طول n روی $\mathbb{F}_q$ باشد، آن‌گاه

$$|C|\sum_{j=۰}^{t}\binom{n}{j}(q-۱)^{j}\leq q^{n},$$

و تساوی برقرار است اگر و تنها اگر C کامل باشد.

(ب) آیا $[۱۲,۷,۵]$ کد خطی دوتایی وجود دارد؟

(۳۰ نمره)

۴. نشان دهید اگر F یک میدان متناهی باشد، $F\setminus\{۰\}$ یک گروه دوری است.

(۲۰ نمره)

۵. (الف) نشان دهید چند جمله‌ای‌های $f(x)=x^{۳}+x^{۲}+۱$ و $g(x)=x^{۳}+x+۱$ روی $\mathbb{Z}_{۲}$ تحویل‌ناپذیر هستند و با استفاده از آن‌ها دو میدان F و K با مرتبه‌ی ۸ بسازید.

(ب) جدول‌های جمع و ضرب در F و K را بنویسید و نشان دهید F و K دو میدان یکریخت هستد.

(۲۰ نمره)

موفق باشید

وقت: ۱۲۰ دقیقه

ارزش امتحان: ۱۲۰ نمره (از ۲۰۰ نمره)

حرف	A	B	C	D	E	F	G	H	I	J	K	L	M
عدد متناظر	۰۰	۰۱	۰۲	۰۳	۰۴	۰۵	۰۶	۰۷	۰۸	۰۹	۱۰	۱۱	۱۲
حرف	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
عدد متناظر	۱۳	۱۴	۱۵	۱۶	۱۷	۱۸	۱۹	۲۰	۲۱	۲۲	۲۳	۲۴	۲۵