بسمه تعالی

دانشگاه صنعتی شریف
دانشکدهٔ علوم ریاضی

آزمون ورودی دورهٔ دکتری ریاضی

تاریخ امتحان: **۸۱٫۳٫۴**

موضوع امتحان: **نظریهٔ اعداد**

۱ـ اگر K میدانی با مشخصهٔ p باشد و $a \in K$ توان pـام هیچ عنصری از K نباشد، نشان دهید چندجمله‌ای $x^{p^n} - a$ روی K تحویل‌ناپذیر است ($n \geq ۱$).

۲ـ اگر E/F یک گسترش میدانها باشد با $E = F(\alpha)$ و $\alpha^n \in F$ (و n کوچکترین عددی باشد که α^n به F متعلق است)، آنگاه

الف) اگر E/F جدایی‌پذیر باشد، نشان دهید مشخصهٔ F، n را نمی‌شمارد.

ب) اگر هر ریشهٔ واحد واقع در E، به F نیز متعلق باشد، نشان دهید $[E : F] = n$.

۳ـ $(\frac{۷}{p})$ را برحسب p محاسبه کنید ($(\frac{a}{p})$ نماد لژاندر است).

۴ـ حلقهٔ عناصر صحیح میدان $\mathbb{Q}(\sqrt{-۳})$ را D می‌نامیم.

الف) پایه‌ای برای D روی $\mathbb{Z}$ بیابید.

ب) ایده‌آلهای $۵D$ و $۷D$ را به ایده‌آلهای اول تجزیه کنید.

۵ـ عدد رده‌ای میدان $\mathbb{Q}(\sqrt{۶})$ را بیابید.

۶ـ اگر a, b اعداد صحیح بزرگتر از ۱ و a فرد باشد و $c = a^b - ۱$ خالی از مربع باشد، نشان دهید در گروه رده‌های ایده‌آلی میدان $\mathbb{Q}(\sqrt{-c})$ عنصری از مرتبهٔ b وجود دارد.

Number Theory

1) Let K be a field of characteristic p and let $a \in K$ be an element which is not p-th power of any element of K. For any $n \geq 1$, show that the polynomial $x^{p^n} - a$ is irreducible over K.

2) Let E/F be an extension of fields, with $E = F(\alpha)$, and $\alpha^n \in F$ (with n the smallest integer such that $\alpha^n \in F$).

a) If E/F is seperable, show that the characteristic of F does not divide n.

b) If every root of unity in E, belongs to F, show that $[E : F] = n$.

3) Compute $(\frac{7}{p})$ in terms of p. ($(\frac{a}{p})$ is the Legendre symbol.)

4) Let D be the ring of integers of the quadratic field $\mathbb{Q}(\sqrt{-3})$.

a) Find a basis for D over $\mathbb{Z}$.

b) Factorize the ideals $5D$ and $7D$ into prime ideals.

5) Compute the class number of the quadratic field $\mathbb{Q}(\sqrt{6})$.

6) Let a, b be integers greater than 1 with a odd, such that $c = a^b - 1$ is squarefree. Show that the ideal class group of the field $\mathbb{Q}(\sqrt{-c})$ contains an elements of order b.