Algebra Comprehensive Exam

Spring 2018

Brookfield, Demeke, Krebs*, Shaheen

Answer five (5) questions only. You must answer *at least one* from each of groups, rings, and fields. Indicate CLEARLY which problems you want us to grade; otherwise, we will select which ones to grade, and they may not be the ones that you want us to grade. Be sure to show enough work that your answers are adequately supported. Tip: When a question has multiple parts, the later parts often (but not always) make use of the earlier parts.

Notation: Unless otherwise stated, $\mathbb{Q}, \mathbb{Z}, \mathbb{Z}_n, \mathbb{C}$, and $\mathbb{R}$ denote the sets of rational numbers, integers, integers modulo n, complex numbers, and real numbers respectively, regarded as groups or rings in the usual way.

Groups

(1) Let G be a group with identity element e. Let $x \in G$ be an element of finite order n. Prove that $x^m = e$ if and only if n divides m.

`Answer:` By definition, n is the least natural number such that $x^n = e$. Now suppose that $x^m = e$ for some $m \in \mathbb{Z}$. Then $m = qn + r$ for some integers q and r such that $0 \leq r < n$, and

$$e = x^m = x^{qn+r} = e^{qn}e^r = (e^n)^q e^r = e^q x^r = x^r.$$

Because $r < n$ and $x^r = e$, r is not a natural number. Since also $0 \leq r$, this implies $r = 0$. Thus finally, $m = qn$, that is, n divides m.

Conversely, if n divides m, then $m = qn$ for some $n \in \mathbb{Z}$, and $x^m = x^{qn} = (x^n)^q = e^q = e$.

(2) A positive integer n is called *squarefree* if its prime decomposition contains no repeated factors. In other words, to say that n is squarefree means that whenever p is a prime number, then p^2 does not divide n. Let n be a squarefree positive integer. Prove that every abelian group of order n is cyclic.

`Answer:` Suppose, to the contrary, that G is an abelian group of order n that is not cyclic. Let a be an element of G with largest possible order. Then $|a|$ divides n, but, since G is not cyclic, $|a|$ is less than n. Since n is squarefree, there is some prime number p that divides n, but does not divide $|a|$.

By Cauchy's Theorem, there is some $b \in G$ with $|b| = p$. Since G is abelian and the orders of a and b are relatively prime, the order of ab is $|a|\,|b| = |a|\,p > |a|$. This contradicts our choice of a.

OR

By the Classification Theorem of Finite Abelian Groups a finite abelian group of order n is isomorphic to a direct product of the form

$$\mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_2^{a_2}} \times \mathbb{Z}_{p_3^{a_3}} \times \cdots \times \mathbb{Z}_{p_k^{a_k}}$$

where $p_1, p_2, \ldots p_k$ are primes, $a_1, a_2, \ldots, a_k$ are natural numbers, and $n = p_1^{a_1}p_2^{a_2}p_3^{a_3}\cdots p_k^{a_k}$. Since n is square free, all the primes are distinct and $a_1 = a_2 = a_3 = \cdots = a_k = 1$:

$$G \cong \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \mathbb{Z}_{p_3} \times \cdots \times \mathbb{Z}_{p_k}$$

The fact that G is abelian now follows by induction from the fact that $\mathbb{Z}_m \times \mathbb{Z}_k \cong \mathbb{Z}_{mk}$ whenever $\gcd(m, k) = 1$.

(3) Prove that no group of order 56 is simple.
`Answer:` See S11 and F14

Rings

(1) Let $\phi\colon R \to S$ be a ring homomorphism, where R and S are integral domains. Let P be an ideal of S.

(i) Prove that $\phi^{-1}(P)$ is an ideal of R.
`Answer:` Suppose that $a, b \in \phi^{-1}(P)$. Then $\phi(a), \phi(b) \in P$, and $\phi(a-b) = \phi(a) - \phi(b) \in P$ since P is an ideal. This shows that $a - b \in \phi^{-1}(P)$.

Suppose that $a \in \phi^{-1}(P)$ and $r \in R$. Then $\phi(a) \in P$, and $\phi(ra) = \phi(r)\phi(a) \in P$ since P is an ideal. This shows that $ra \in \phi^{-1}(P)$.

Together the above two closure properties mean that $\phi^{-1}(P)$ is an ideal.

(ii) Prove that if P is a prime ideal, then $\phi^{-1}(P)$ is also a prime ideal.
`Answer:` Suppose that $a, b \in R$ satisfy $ab \in \phi^{-1}(P)$. Then $\phi(a)\phi(b) = \phi(ab) \in P$. Since P is prime, either $\phi(a) \in P$ or $\phi(b) \in P$, that is, $a \in \phi^{-1}(P)$ or $b \in \phi^{-1}(P)$. This property means that P is a prime ideal.

(2) Consider the ring $\mathbb{Z}[x]$ of polynomials with integer coefficients. Let I be the set of polynomials in $\mathbb{Z}[x]$ whose constant term is even.

(i) Prove that I is an ideal of $\mathbb{Z}[x]$.
`Answer:` Let $\phi : \mathbb{Z}[x] \to \mathbb{Z}_2$ be the composition of the evaluation-at-zero homomorphism $\mathbb{Z}[x] \to \mathbb{Z}$ composed with the obvious homomorphism $\mathbb{Z} \to \mathbb{Z}_2$. Then $I = \ker \phi$ and so I is an ideal.

(ii) Prove that I is not a principal ideal.
`Answer:` See F09.

(iii) Prove that $\mathbb{Z}[x]$ is not a Euclidean domain.
`Answer:` If, to the contrary, $\mathbb{Z}[x]$ were a Euclidean domain, then it would also be a PID. This obviously cannot be true since I is not principal.

(3) Let p be a prime number. Suppose that R is a ring and that $\psi\colon R \to \mathbb{Z}_p$ is a ring homomorphism. Let $M = \{x \in R \mid \psi(x)^{p-1} \neq 1\}$. Prove that $M = R$ or M is a maximal ideal of R.
`Answer:` First we notice that $\mathbb{Z}_p$ is a field and so the nonzero elements form a group of order $p-1$ under multiplication. In particular, $a^{p-1} = 1$ for all nonzero element of $\mathbb{Z}_p$. Thus the only element of $\mathbb{Z}_p$ satisfying $a^{p-1} \neq 1$ is $a = 0$.

Thus $M = \{x \in R \mid \psi(x) = 0\}$ is the kernel of the homomorphism ψ, and $R/M \cong \psi(R)$. $\mathbb{Z}_p$ is a field and so either $\psi(R) = \{0\}$ and $M = R$, or $\psi(R) = \mathbb{Z}_p$ in which case R/M is a field and M is maximal.

Fields

(1) Let F be a finite field. Prove that the group of units of F is a cyclic group.
`Answer:` See Fraleigh Corollary 23.6.

(2) Let $\sigma = e^{2\pi i/5} \in \mathbb{C}$, and let $F = \mathbb{Q}(\sigma)$. Describe the Galois group of F over $\mathbb{Q}$. Explain what theorems you are using.
`Answer:` See S12 (and F11 and F12).

(3) Let K be a finite field extension of F with $[K : F] = 47$. Let $a \in K \setminus F$. Prove that $F(a) = K$.

`Answer:` Since, by assumption, $a \notin F$ we have $F(a) \neq F$ and $[F(a) : F] \neq 1$.

We also have $F \subseteq F(a) \subseteq K$ with $[K : F] = 47$ and so $[F(a) : F]$ divides 47. Since 47 is prime and $[F(a) : F] \neq 1$, we have $[F(a) : F] = 47$. This implies that $[K : F(a)] = 1$ and $F(a) = K$.