2012 Fall Algebra I Final

Ali Nesin

22 Ocak 2012

1. *Find* $\mathrm{Aut}(\mathbb{Q}^\star)$*.* (10 pts.)

Solution: Let $\phi \in \mathrm{Aut}(\mathbb{Q}^\star)$. It is easy to show that $\phi(1) = 1$ and $\phi(-1) = -1$. Since $\phi(xy) = \phi(x)\phi(y)$, and since every element of $\mathbb{Q}^\star$ can be written uniquely as

$$\epsilon \prod_{i=1}^{k} p_i^{n_i}$$

for some unique $\epsilon = \pm 1$, $k \in \mathbb{N}$, distinct positive primes p_i and $n_i \in \mathbb{Z} \setminus \{0\}$, it is enough to find the values of ϕ at the positive primes p. Since ϕ is a bijection, the image of a prime can only be a prime. Thus ϕ permutes the primes among each other. (But be aware that the image of a positive prime can be a negative prime).

Thus let P be the set of positive primes. For each $f \in \mathrm{Sym}\, P$ and each $\alpha \in \mathrm{Func}(P, \{1, -1\}) \simeq \prod_P \{1, -1\}$ we obtain an automorphism $\phi_{f,\alpha}$ of $\mathbb{Q}^\star$ by

$$\phi_{f,\alpha}\left(\epsilon \prod_{i=1}^{k} p_i^{n_i}\right) = \epsilon \prod_{i=1}^{k} \alpha(p_i)^{n_i} f(p_i)^{n_i}.$$

It is also clear from the discussion above that each $\phi \in \mathrm{Aut}(\mathbb{Q}^\star)$ is obtained this way.

One can check that

$$\phi_{f,\alpha} \circ \phi_{g,\beta} = \phi_{f\circ g, \alpha\beta}.$$

Hence

$$Aut(\mathbb{Q}^\star) \simeq \mathrm{Sym}\, P \times \prod_P \{1, -1\}.$$

2. *Find all ideals of the ring* $\mathbb{Z}_p$ *of* p*-adic integers.* (10 pts.)

Solution: We know that an element of $\mathbb{Z}_p$ can be uniquely written (or represented) as $\sum_i a_i p^i$ for $a_i \in \{0, 1, \ldots, p-1\}$ and that such an element is invertible iff $a_0 \neq 0$. Let $0 \neq I \trianglelefteq \mathbb{Z}_p$. Let $n = \min\{\mathrm{val}_p(x) : x \in I\}$. Let $a \in I$ be such that $\mathrm{val}_p(a) = n$. Then $a = p^n \sum_i a_i p^i$ with $a_0 \neq 0$. Thus $\sum_i a_i p^i$ is invertible in $\mathbb{Z}_p$. It follows that $p^n \in I$. Now it is easy to show that $I = p^n \mathbb{Z}_p$.

3. *Find a domain that contains* $\mathbb{Z}_p$ *as a subring and also a square root of* p*.* (6 pts.)

Solution: The ring $\mathbb{Z}_p[X]/\langle X^2 - p\rangle$ is a ring that contains a squareroot of p. Since $X^2 - p$ is irreducible in $\mathbb{Z}_p[X]$, this ring is a domain.

4a. *Let* G *be a finite group and* $A \leq \mathrm{Aut}\, G$*. For* $g \in G$ *show that* $|Ag|$ *divides* $|A|$*.* (10 pts.)

4b. *Let everything be as above. Show that for* $g, h \in G$ *either* $Ag = Ah$ *or* $Ag \cap Ah = \emptyset$*.* (5 pts.)

4c. *Let* p *be a prime,* G *be a finite* p*-group and* $A \subset \mathrm{Aut}\, G$*, alsop a* p*-group. Show that there is an element* $1 \neq g \in G$ *which is fixed by all the elements of* A*.* (6 pts.)

Proofs: a. Let $B = \{\alpha \in A : \alpha(g) = g\}$. Then $B \subseteq A$. Let A/B denote the left coset space. The rule $\alpha B \mapsto \alpha(g)$ gives rise to a well-defined map (to be checked) from A/B into Ag. Furthermore this map is 1-1 and onto. Hence $|Ag| = |A/B|$ and so $|Ag|$ divides $|A|$.

b. Let $\alpha(g) = \beta(h) \in Ag \cap Ah$. Then $Ag = (A\alpha)g = A(\alpha g) = A(\beta h) = (A\beta)h = Ah$.

c. By part b, G is a union of the disjoint orbits Ag for some $g \in G$. By part a, Ag is a power of p, including $p^0 = 1$, because $A1 = \{1\}$ has only one element. Thus $\{g \in G : |Ag| = 1\}$ must have a nonzero multiple of p many elements.

5. *Let V be a vector space and U and W subspaces of V. Show that* $\dim(U+W) = \dim U + \dim W - \dim(U \cap V)$*.* (15 pts.)

Proof: Consider the map $U \times V \longrightarrow U + W$ given by $(u, w) \mapsto u + w$. This is a linear map which is onto and whose kernel is

$$\{(u, w) \in U \times W : u + w = 0\} = \{(u, -u) : u \in U \cap W\} \simeq U \cap W.$$

The result follows.

6. *An ordered ring is a ring R together with a total order $<$ such that*

ORD1. $x < y \implies x + z < y + z$.

ORD2. $x < y$ *and* $0 < z \implies xz < yz$.

a. *Show that in an ordered ring if $x < y$ then $-y < -x$.* (2 pts.)

b. *Show that in an ordered ring for all x, $0 \leq x^2$.* (4 pts.)

c. *Show that an ordered ring is a domain of characteristic 0 and that -1 cannot be a sum of squares.* (10 pts.)

d. *Given an ordered ring R, let $P = \{x \in R : 0 < x\}$ (the positive cone). Show that P is closed under addition and multiplication, that it does not contain 0 and that $R = (-P) \cup \{0\} \cup P$. Show that if R is a field then P is also closed under inversion.* (2 + 4 pts.)

e. *Let R be a ring and $P \subseteq R$ be a subset that satisfies the properties listed above. Define $x < y$ by $y - x \in P$. Show that R becomes an ordered ring.* (4 pts.)

f. *Let R be a domain and S be the set of finite sums of squares of R excluding 0. Show that S is closed under addition and multiplication.* (2 pts.)

g. *Let $K = R$ be a ring in which -1 is not a sum of squares. Let S be as above. Show that S can be extended to a set P which is closed under addition and multiplication, which does not contain 0 and for which $R = (-P) \cup \{0\} \cup P$.* (10 pts.)

Proofs: a. It is enough to add $-x - y$ to both sides of the inequality $x < y$.

b. If $0 < x$ or $0 = x$ that is clear by ORD2. Assume $x < 0$. By the first part $0 < -x$. So $0 < (-x)^2 = x^2$.

c. By part b, $0 < 1^2 = 1$. So by ORD 1, $1 < 2$ and $2 < 3$ etc. So for no natural number $n \neq 0$ (in $\mathbb{N}$) can ve have $n = 0$ in the ring because otherwise we would have

$$0 < 1 < 2 < \ldots < n - 1 < n = 0$$

and $0 < 0$ by transitivity of the order. Thus $\mathbb{R}$ had characteristic 0.

No nonzero zerodivisors: If x and y are > 0 then $xy > 0$. The other cases are similar by considering $\pm x$ and $\pm y$.

Since $1 > 0$ we must have $-1 < 0$, so by part b, -1 cannot be a sum of squares.

d. The first part is clear. For the second part. Assuma $a \in P$. Then $a^{-1} = a \cdot (a^{-1})^2 \in P$ because squares are in P.

e. We first show that we have a total order. $x \not< x$ because $0 \notin P$. Transitivity follows from the fact that P is closed under addition. The order is total because $R = (-P) \cup \{0\} \cup P$.

ORD1 is clear. ORD2 follows from the fact that P is closed under multiplication.

f. Clear.

g. Let $Z = \{P \subseteq R : S \subset P,\ S$ is closed under addtion and multiplication and $0 \notin S\}$. Order Z by inclusion. Z is obviously closed under the union of chains. Thus by Zorn's Lemma Z has a maximal element, say P. We proceed to show that $R = (-P) \cup \{0\} \cup P$. Assume not. Let $x \in R$ be an element not in this union. Let

$$P_1 = P + xP.$$

Then $P \subset P_1$ and P_1 is closed under addition and multiplication because $x^2 \in S \subset P$. Furthermore $0 \notin P_1$ because otherwise by part d, $-x$ would be in P, i.e. x would be in $-P$, a contradiction.